Notices

The following acknowledgements pertain to this software license:

**OpenSSL/OpenSSL Project**

LMS includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit ([http://www.openssl.org/](http://www.openssl.org/)), and cryptographic software written by Eric Young (eay@cryptsoft.com), and software written by Tim Hudson (tjh@cryptsoft.com).

**License Issues**

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. The license texts are listed below. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

**OpenSSL License:**

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit ([http://www.openssl.org/](http://www.openssl.org/))”.

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:
Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”. The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].
Preface

Cisco Prime LAN Management Solution (LMS) provides you with powerful features that enable you to configure, monitor, troubleshoot, and administer Cisco networks.

Cisco Prime LMS 4.2 has a new menu layout that facilitates access to information and to tools required for managing your network.

Cisco Prime LMS 4.2 groups the options to the following underlying core functions in this release:

- Monitoring
- Inventory Management
- Configuration
- Reporting
- Administration
- Work Center Management

This guide provides you with information on the Configuration Management function in Cisco Prime LMS.

This preface lists related documents that support the Configuration Management function, and demonstrates the styles and conventions used in this guide. The preface contains the following sections:

- Audience
- Document Conventions
- Product Documentation

Audience

This guide is for users who are skilled at network administration and management, and for network operators who can use this guide to make configuration changes to devices, using LMS. The network administrators or the operators should be familiar with the following:

- Basic Network Administration and Management
- Basic Solaris and Soft Appliance System Administration
- Basic Windows System Administration
- Basic LMS Administration
Document Conventions

Table 1 describes the conventions followed in the user guide.

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands and keywords</td>
<td><strong>boldface font</strong></td>
</tr>
<tr>
<td>Variables for which you supply values</td>
<td><strong>italic font</strong></td>
</tr>
<tr>
<td>Displayed session and system information</td>
<td><strong>screen font</strong></td>
</tr>
<tr>
<td>Information you enter</td>
<td><strong>boldface screen font</strong></td>
</tr>
<tr>
<td>Variables you enter</td>
<td><strong>italic screen font</strong></td>
</tr>
<tr>
<td>Menu items and button names</td>
<td><strong>boldface font</strong></td>
</tr>
<tr>
<td>Selecting a menu item in paragraphs</td>
<td><strong>Option &gt; Network Preferences</strong></td>
</tr>
<tr>
<td>Selecting a menu item in tables</td>
<td><strong>Option &gt; Network Preferences</strong></td>
</tr>
</tbody>
</table>

Note: Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Product Documentation

Note: We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 2 describes on the product documentation that is available.

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting Started with Cisco Prime LAN Management Solution 4.2</td>
<td>PDF version part of Cisco Prime LMS 4.2 Product DVD.</td>
</tr>
<tr>
<td>Context-sensitive online help</td>
<td>Select an option from the navigation tree, then click Help.</td>
</tr>
<tr>
<td>Configuration Management with Cisco Prime LAN Management Solution 4.2 (This document)</td>
<td>PDF version part of Cisco Prime LMS 4.2 Product DVD.</td>
</tr>
<tr>
<td>Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.2</td>
<td>PDF version part of Cisco Prime LMS 4.2 Product DVD.</td>
</tr>
<tr>
<td>Inventory Management with Cisco Prime LAN Management Solution 4.2</td>
<td>PDF version part of Cisco Prime LMS 4.2 Product DVD.</td>
</tr>
<tr>
<td>Administration of Cisco Prime LAN Management Solution 4.2</td>
<td>PDF version part of Cisco Prime LMS 4.2 Product DVD.</td>
</tr>
</tbody>
</table>
Table 2  Product Documentation (continued)

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Work Centers in Cisco Prime LAN Management Solution 4.2</td>
<td>PDF version part of Cisco Prime LMS 4.2 Product DVD.</td>
</tr>
<tr>
<td>Reports Management with Cisco Prime LAN Management Solution 4.2</td>
<td>PDF version part of Cisco Prime LMS 4.2 Product DVD.</td>
</tr>
</tbody>
</table>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
Configuration Management in Cisco Prime LAN Management Solutions (LMS) allows you to manage, deploy, and modify the configuration files used by devices in your network. You can run tools that can compare configuration files and perform software image management tasks.

Configuration Dashboard in LMS provides information such as date of last configuration change, status of the configuration jobs, summary of inventory configuration protocol and Hardware and Software summary.

You can create configuration jobs and also manage configuration archive settings. You can define baseline configuration templates and determine the devices that are non-compliant in your network.

You can perform VLANs configurations and Virtual Switching System (VSS) conversions.

This chapter provides information on the organization of the Configuration Management user guide and an overview of Configuration Management tasks.

It explains:

- Organization
- Configuration Management Tasks
- Configuration Center
# Organization

The Configuration Management user guide is organized as follows:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Overview of Configuration Management” (This chapter)</td>
<td>Provides information on the organization of Configuration Management with Cisco Prime LMS user guide and an overview of the tasks in Configuration Management functionality.</td>
</tr>
<tr>
<td>Chapter 2, “About Configuration Dashboard”</td>
<td>Describes the Configuration Dashboard portlets in LMS.</td>
</tr>
<tr>
<td>Chapter 3, “Managing and Deploying Templates”</td>
<td>Describes how to manage configuration templates and deploy them on devices.</td>
</tr>
<tr>
<td>Chapter 4, “Using Compliance and Audit Manager Feature”</td>
<td>Describes how to manage policy groups, policy profiles, run compliance check and fix the violations shown in the report.</td>
</tr>
<tr>
<td>Chapter 5, “Making and Deploying Configuration Changes Using NetConfig”</td>
<td>Describes how to use the NetConfig feature in Configuration Management. NetConfig allows you to make configuration changes to your managed network devices whose configurations are archived in the Configuration Archive.</td>
</tr>
<tr>
<td>Chapter 6, “Archiving Configurations and Managing them using Configuration Archive”</td>
<td>Describes how to use the Configuration Management feature. Configuration Management gives you easy access to the configuration files for all devices or Cisco IOS-based Catalyst switches, Content Service Switches, Content Engines, and Cisco routers in the LMS inventory.</td>
</tr>
<tr>
<td>Chapter 7, “Using Baseline Templates to Check Configuration Compliance”</td>
<td>Describes how to use Compliance management task to create, deploy and manage baseline templates. It also describes how to check for configuration compliance.</td>
</tr>
<tr>
<td>Chapter 8, “Editing and Deploying Configurations Using Config Editor”</td>
<td>Describes how to use the Config Editor task. Config Editor allows you to edit a configuration file that exists in the configuration archive.</td>
</tr>
<tr>
<td>Chapter 9, “Managing Software Images Using Software Management”</td>
<td>Describes how to use the Software Image Management tool in LMS. To ensure rapid, reliable software upgrades, Software Management automates many steps associated with upgrade planning, scheduling, downloading, and monitoring.</td>
</tr>
<tr>
<td>Chapter 10, “Virtual Switching System Support”</td>
<td>Describes how to convert two standalone switches into a Virtual Switching System. It also describes how to convert a Virtual Switching System back to standalone switches.</td>
</tr>
<tr>
<td>Chapter 11, “Configuring VLAN”</td>
<td>Describes how to configure and manage a Virtual Local Area Network (VLAN) in your network. It also describes how to configure and manage a Private VLAN (PVLAN), Trunk, and also assign ports to VLANs.</td>
</tr>
</tbody>
</table>
Table 1-1  Configuration Management User Guide (continued)

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 12, “Configuring Virtual Routing and Forwarding (VRF)”</td>
<td>Describes how to perform end-to-end VRF configurations in an enterprise network using LMS.</td>
</tr>
<tr>
<td>Chapter 13, “Viewing Topology Services”</td>
<td>Describes how to view and monitor your network including the links and the ports of each link using Topology Services in LMS.</td>
</tr>
<tr>
<td>Appendix A, “CLI Utilities”</td>
<td>Describes how to use the CiscoWorks Command Line (CWCLI) utilities in LMS.</td>
</tr>
<tr>
<td>Appendix B, “Config Template XML Schema”</td>
<td>Describes how to create new configuration templates that can be deployed using the Template Center feature.</td>
</tr>
<tr>
<td>Appendix C, “Troubleshooting Tips and FAQs”</td>
<td>Describes the Troubleshooting tips and FAQs.</td>
</tr>
</tbody>
</table>

Configuration Management Tasks

This section provides an overview of the Configuration Management tasks supported in LMS. The information is organized as follows:

<table>
<thead>
<tr>
<th>Configuration Tasks</th>
<th>Menu Navigation Path</th>
<th>Description</th>
</tr>
</thead>
</table>
| Dashboard           | Configuration > Dashboard: Configuration | You can view and configure the following configuration dashboard portlets:  
  • Best Practices Deviation  
  • Discrepancies  
  • Job Information Status  
  • Device Change Audit  
  • Inventory Config Protocol Summary  
  • Hardware Summary  
  • Job Approval  
  • Software Summary  
  • Syslog Alerts |
## Configuration Management Tasks

<table>
<thead>
<tr>
<th>Configuration Tasks</th>
<th>Menu Navigation Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Templates</td>
<td>Configuration &gt; Compliance: Compliance Templates</td>
<td>You can perform the following compliance tasks:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Manage Baseline templates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run compliance check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deploy Baseline templates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run compliance check and deploy jobs</td>
</tr>
<tr>
<td>Out-of-Sync Summary</td>
<td>Configuration &gt; Compliance: Out-of-Sync Summary</td>
<td>You can generate an Out-of-Sync report for the group of devices for which running configurations are not synchronized with the startup configuration.</td>
</tr>
</tbody>
</table>

## Job Browsers

<table>
<thead>
<tr>
<th>Job Browsers</th>
<th>Menu Navigation Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>Configuration &gt; Job Browsers: Compliance</td>
<td>You can view the compliance check and deploy job status.</td>
</tr>
<tr>
<td>Configuration Archive</td>
<td>Configuration &gt; Job Browsers: Configuration Archive</td>
<td>You can manage archive management jobs.</td>
</tr>
<tr>
<td>Template Center</td>
<td>Configuration &gt; Job Browsers: Template Center</td>
<td>You can browse the template deployment jobs registered on the system. Using the Template Center, you can manage template jobs. That is, you can stop, delete, refresh, or filter jobs using this job browser. You can also view the template job details such as work order, device details, and job summary.</td>
</tr>
<tr>
<td>NetConfig</td>
<td>Configuration &gt; Job Browsers: NetConfig</td>
<td>Using the Job Browser, you can manage NetConfig jobs. That is, you can edit, stop, delete, or filter jobs using this job browser.</td>
</tr>
<tr>
<td>Software Image Management</td>
<td>Configuration &gt; Job Browsers: Software Image Management</td>
<td>You can view all your scheduled Software Image Management jobs. You can edit, stop, delete the jobs using the Software Image Management Job Browser.</td>
</tr>
<tr>
<td>Config Editor</td>
<td>Configuration &gt; Job Browsers: Config Editor</td>
<td>You can manage configuration editor jobs.</td>
</tr>
<tr>
<td>Job Approval</td>
<td>Configuration &gt; Job Browsers: Job Approval</td>
<td>You can approve configuration jobs.</td>
</tr>
</tbody>
</table>

## Tools
<table>
<thead>
<tr>
<th>Configuration Tasks</th>
<th>Menu Navigation Path</th>
<th>Description</th>
</tr>
</thead>
</table>
| Template Center     | Configuration > Tools: Template Center | Template Center in LMS provides you with a list of system-defined templates. These templates contain configuration commands that can be deployed on the devices in your network. You can perform the following tasks from Template Center:  
  • Deploying Templates  
  • Managing Templates  
  • Importing Templates  
  • Assigning Template to users  
  • Viewing and Managing Template Center Jobs |
| NetConfig           | Configuration > Tools: NetConfig | You can perform the following NetConfig tasks:  
  • Deploying NetConfig jobs  
  • Assigning Tasks to users  
  • User Defined Tasks |
| Config Editor       | Configuration > Tools: Config Editor | You can open a configuration file, edit it, save it in a private location or in public location using the following tasks:  
  • Open and edit config files  
  • Save config files as private  
  • Save config files as public |
| Software Image Management | Configuration > Tools: Software Image Management | You can perform the following Software Image Management tasks:  
  • Patch Distribution  
  • Software Distribution  
  • Software Repository  
  • Repository Synchronization  
  • Upgrade Analysis  
  • Software Management Jobs |

**Workflows**
## VLAN Configuration Tasks

<table>
<thead>
<tr>
<th>Configuration Tasks</th>
<th>Menu Navigation Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Configuration &gt; Workflows: VLAN</td>
<td>You perform the following VLAN tasks:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure VLAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Delete VLAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create Private VLAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Delete Private VLAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure Port Assignment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure Promiscuous Ports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create Trunk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Modify Trunk Attributes</td>
</tr>
</tbody>
</table>

## VRF-lite Configuration Tasks

<table>
<thead>
<tr>
<th>Configuration Tasks</th>
<th>Menu Navigation Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-lite</td>
<td>Configuration &gt; Workflows: VRF-lite</td>
<td>You can perform the following Virtual Routing and Forwarding (VRF) tasks:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create VRF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Edit VRF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Extend VRF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Delete VRF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Edge VLAN Configuration</td>
</tr>
</tbody>
</table>

## Virtual Switching System Configuration Tasks

<table>
<thead>
<tr>
<th>Configuration Tasks</th>
<th>Menu Navigation Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Switching</td>
<td>Configuration &gt; Workflows: Virtual</td>
<td>You can convert two standalone switches into a Virtual Switching System or convert Virtual Switching System back to standalone switches.</td>
</tr>
<tr>
<td>System</td>
<td>Switching System</td>
<td></td>
</tr>
</tbody>
</table>

## Configuration Center Configuration Tasks

<table>
<thead>
<tr>
<th>Configuration Tasks</th>
<th>Menu Navigation Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Center</td>
<td>Configuration Center</td>
<td>You can view all the launch points for all types of device or feature configurations supported in LMS.</td>
</tr>
<tr>
<td>Configuration Tasks</td>
<td>Menu Navigation Path</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Configuration Archive</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td>Configuration &gt; Configuration Archive: Summary</td>
<td>You can view the configuration archival status and summary.</td>
</tr>
</tbody>
</table>
| Views | Configuration > Configuration Archive: Views | You can search archives using version tree and version summary. Views list the following links:  
  • Custom Queries  
  • Search Archive  
  • Version Summary  
  • Version Tree |
| Synchronization | Configuration > Configuration Archive: Synchronization | You can schedule a job to update the configuration archive for selected group of devices. |
| Compare Configs | Configuration > Configuration Archive: Compare Configs | You can compare the following configurations:  
  • Startup vs Running  
  • Running vs Latest Archived  
  • Two Versions of the Same Device  
  • Two Versions of Different Devices  
  • Base Config vs Latest Version of Multiple Devices |
| Label Configs | Configuration > Configuration Archive: Label Configs | A label is a name given to a group of customized selection of configuration files. You can select configuration files from different devices, group and label them. |
| Protocol Usage Summary | Configuration > Configuration Archive: Protocol Usage Summary | You can view the configuration protocol usage details for successful configuration fetches. |
| **Topology** | | |
| Topology Services | Configuration > Topology | You can launch Topology Services to view and monitor your network. |
# Configuration Center

Configuration Center is a launch point for all types of device or feature configurations supported in LMS. The various device or feature configurations supported in LMS are

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technologies and Services</strong></td>
<td></td>
</tr>
<tr>
<td>Auto Smartport</td>
<td>Auto Smartports macros dynamically configure switch ports based on the</td>
</tr>
<tr>
<td></td>
<td>device type detected on the port.</td>
</tr>
<tr>
<td></td>
<td>You can:</td>
</tr>
<tr>
<td></td>
<td>• Assess Auto Smartports readiness of the network.</td>
</tr>
<tr>
<td></td>
<td>• Upgrade IOS, wherever required, to make the device ASP capable.</td>
</tr>
<tr>
<td></td>
<td>• Deploy Auto Smartports templates on selected devices.</td>
</tr>
<tr>
<td></td>
<td>• Add or edit macros, system-defined, user-defined, or remote macro,</td>
</tr>
<tr>
<td></td>
<td>associated to an event.</td>
</tr>
<tr>
<td></td>
<td>• Enable or disable Auto Smartports on selected interfaces of the selected</td>
</tr>
<tr>
<td></td>
<td>devices.</td>
</tr>
<tr>
<td></td>
<td>• Modify or disable Auto Smartports configuration on ASP enabled devices.</td>
</tr>
<tr>
<td>Credential</td>
<td>You can:</td>
</tr>
<tr>
<td></td>
<td>• Configure or change enable or secret password to enter in enable mode on</td>
</tr>
<tr>
<td></td>
<td>devices.</td>
</tr>
<tr>
<td></td>
<td>• Configure local username and password authentication on devices.</td>
</tr>
<tr>
<td></td>
<td>• Configure SSH.</td>
</tr>
<tr>
<td></td>
<td>• Add, remove, and edit Telnet passwords.</td>
</tr>
<tr>
<td>EEM</td>
<td>You can:</td>
</tr>
<tr>
<td></td>
<td>• Configure EEM scripts or applets on selected devices.</td>
</tr>
<tr>
<td></td>
<td>• Configure the EEM policy.</td>
</tr>
<tr>
<td></td>
<td>• Register or unregister a script or applet.</td>
</tr>
<tr>
<td></td>
<td>• Configure EEM environmental variables that are used by the TCL script.</td>
</tr>
<tr>
<td>EnergyWise</td>
<td>You can measure, monitor, and manage the way your devices consume energy.</td>
</tr>
<tr>
<td></td>
<td>You can:</td>
</tr>
<tr>
<td></td>
<td>• Assess EnergyWise readiness of the network.</td>
</tr>
<tr>
<td></td>
<td>• Upgrade IOS, wherever required, to make the device EnergyWise capable.</td>
</tr>
<tr>
<td></td>
<td>• Define EnergyWise domains.</td>
</tr>
<tr>
<td></td>
<td>• Associate devices to the EnergyWise domain.</td>
</tr>
<tr>
<td></td>
<td>• Define Endpoint group and configuring EnergyWise policies.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Gold          | You can configure Boot Level Diagnostic tests and configure GOLD Monitoring tests on devices. You can:  
• Configure Boot Level diagnostic tests.  
• Configure GOLD monitoring tests.  
• Configure Health Monitoring diagnostics.  
• Enable or disable Health Monitoring diagnostics test.  
• Configure Health Monitoring interval. |
| Identity      | Identity offers authentication, access control, and user policies to secure network resources and connectivity. You can:  
• Assess Identity readiness of the network.  
• Upgrade IOS, wherever required, to make the device Identity capable.  
•Configure RADIUS settings.  
• Configure security modes, authentication profile, and host mode.  
• Configure MACsec on capable devices. |
| MACsec        | You can configure MACsec to provide secure, encrypted communication on wired LANs.  
You can use this template to configure:  
• Security policy to be applied to the session after the supplicant passes 802.1x authentication.  
• Authentication Failure Policy.  
• MKA policy. |
| Performance Monitoring | You can configure the following for endpoints like Cisco Unified Video Advantage (CUVA), Cisco TelePresence Movi, Tandberg, and Webex Servers:  
• Configure a flow record to specify the fields you want to monitor.  
• Configure a policy to include one or more classes.  
• Reaction ID, jitter and threshold of lost packets.  
You can configure a flow record and specify how the collected data is aggregated and presented. |
| PfR           | Performance Routing provides best path optimization and load balancing of traffic over the WAN and to the Internet for enterprise networks with multiple paths. You can:  
• Configure traffic classes for performance routing.  
• Configure performance metrics of these individual traffic classes.  
• Control the traffic by applying suitable traffic class and link policies. |
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
</table>
| Port Macros   | You can configure Auto Smartport macros on devices.  
You can:  
• Enable or disable Auto Smartport at device level.  
• Apply or remove Auto Smartport policy definitions. |
| QoS           | This template provides QoS macros to switch ports upon detection of a Medianet endpoint.  
You can:  
• Select specific network traffic.  
• Prioritize it according to its relative importance.  
• Use QoS macros to provide preferential treatment of traffic in your network. |
| RSVP          | Resource Reservation Protocol (RSVP) signals the QoS needs of an application's traffic, along the devices, in the end-to-end path through the network.  
You can configure:  
• User or application that requires an RSVP request.  
• Bandwidth that has to be reserved.  
• Admission policy that the devices use to admit the RSVP message. |
| SCH           | You can use this template to enable Smart Call Home on MDS, Nexus, IOS and ASA platforms. |
| SGA           | You can propagate the Security Group Tags (SGT) across network devices that do not have hardware support for Cisco TrustSec.  
You can use this template to configure:  
• Default SGT Exchange Protocol (SXP) password.  
• SXP address connection.  
• Default SXP source IP address. |
| Smart Install | Smart Install is a configuration and image management feature that provides zero-touch deployment for new devices.  
You can:  
• Assess the readiness of your network for Smart Install capable directors.  
• Upgrade IOS, wherever required, to make the device Smart Install capable.  
• Discover and enable Smart Install on Smart Install capable directors.  
• Manage configuration files and images of clients in the Smart Install director.  
• Configure DHCP settings for Smart Install. |
<p>| SNMP          | You can configure SNMP community strings, SNMP security feature, and SNMP traps on devices. |</p>
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS</td>
<td>You can configure:</td>
</tr>
<tr>
<td></td>
<td>• TACACS authentication</td>
</tr>
<tr>
<td></td>
<td>• TACACS+ authentication</td>
</tr>
<tr>
<td></td>
<td>• RADIUS on devices</td>
</tr>
<tr>
<td>Video Conferencing</td>
<td>You can use this template to configure different video endpoints for video conferences.</td>
</tr>
<tr>
<td></td>
<td>You can configure three types of video profiles:</td>
</tr>
<tr>
<td></td>
<td>• Homogeneous Video Conference</td>
</tr>
<tr>
<td></td>
<td>• Heterogeneous Video Conference</td>
</tr>
<tr>
<td></td>
<td>• Guaranteed Audio Conference</td>
</tr>
<tr>
<td>Video Transcoding</td>
<td>You can use this template to configure video transcoding when the bit rate, frame rate, resolution, or codec is different between two endpoints.</td>
</tr>
<tr>
<td>VLAN</td>
<td>You can configure and manage VLAN, Private VLAN (PVLAN), Trunk, and also assign ports to VLANs.</td>
</tr>
<tr>
<td>VRF-Lite</td>
<td>You can select Layer 2 or Layer 3 devices and configure VRF on the selected devices.</td>
</tr>
<tr>
<td></td>
<td>You can:</td>
</tr>
<tr>
<td></td>
<td>• Select the Layer 2 or Layer 3 devices from the Distribution Layer or the Core Layer.</td>
</tr>
<tr>
<td></td>
<td>• Configure VRF on the selected devices.</td>
</tr>
<tr>
<td></td>
<td>• Configure details of the VRF like: VRF Name, Route Distinguisher, and description of VRF.</td>
</tr>
<tr>
<td></td>
<td>• Map an interface to a VRF.</td>
</tr>
<tr>
<td></td>
<td>• Configure the routing protocol to the selected devices on which VRF is configured.</td>
</tr>
<tr>
<td>VSS</td>
<td>You can convert VSS-capable standalone switches to a Virtual Switching System.</td>
</tr>
<tr>
<td></td>
<td>You can:</td>
</tr>
<tr>
<td></td>
<td>• Select devices for VSS configuration</td>
</tr>
<tr>
<td></td>
<td>• Perform hardware compatibility checks on the devices</td>
</tr>
<tr>
<td></td>
<td>• Perform software compatibility checks on the devices and generate compliance report</td>
</tr>
<tr>
<td></td>
<td>• Define configuration parameters</td>
</tr>
<tr>
<td></td>
<td>• Deploy commands on the devices to enable VSS mode</td>
</tr>
<tr>
<td>Validated Designs</td>
<td>You can use this template to configure QoS, rate limiting, ACLs, OSPF for routed access, and IPv6 on Access switches.</td>
</tr>
<tr>
<td>Access Switch</td>
<td>This template provides resilience, QoS, security, and, scalability for Cisco Smart Business Architecture (SBA) networks.</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Cisco Smart Business Architecture</td>
<td>You can use this template to configure QoS, rate limiting, ACLs, OSPF for routed access, and IPv6 on Access switches.</td>
</tr>
<tr>
<td></td>
<td>This template provides resilience, QoS, security, and, scalability for Cisco Smart Business Architecture (SBA) networks.</td>
</tr>
</tbody>
</table>
### Chapter 1  
Overview of Configuration Management

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small Branch Configuration</td>
<td>You can use this template to configure security features like GETVPN, DMVPN, Firewall, IPS and unified communications.</td>
</tr>
</tbody>
</table>

### Configuration Tools

<table>
<thead>
<tr>
<th>NetConfig Templates</th>
<th>You can configure:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• General Settings</td>
</tr>
<tr>
<td></td>
<td>NetConfig provides system-defined configuration tasks. You can create</td>
</tr>
<tr>
<td></td>
<td>configuration commands by using these tasks. All System-defined tasks</td>
</tr>
<tr>
<td></td>
<td>are categorized into various task groups in the Tasks Selector.</td>
</tr>
<tr>
<td></td>
<td>• User-defined tasks</td>
</tr>
<tr>
<td></td>
<td>You can create user-defined tasks and add one or more templates to each task.</td>
</tr>
<tr>
<td></td>
<td>The templates contain configuration commands and rollback commands. You can</td>
</tr>
<tr>
<td></td>
<td>enter the configuration commands either by typing them or by importing them</td>
</tr>
<tr>
<td></td>
<td>from a file. The template is associated with the MDF categories of devices,</td>
</tr>
<tr>
<td></td>
<td>for which these templates will be applicable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Template Center</th>
<th>You can deploy system-defined templates and user-defined templates on devices in your network.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You can configure the following types of templates:</td>
</tr>
<tr>
<td></td>
<td>• Custom Templates—Lists all the user-defined templates assigned to the current user.</td>
</tr>
<tr>
<td></td>
<td>• Cisco Best Practices Templates—Lists all the system-defined templates.</td>
</tr>
</tbody>
</table>

**Note** Some of the NetConfig Tasks will be listed as Cisco Best Practice templates from LMS 4.2.1 Release.
About Configuration Dashboard

This chapter provides information on the Configuration dashboard in LMS. Configuration dashboard in LMS provides information such as the date of last configuration change, status of the configuration jobs, summary of configuration protocol, Hardware and Software summary. The Configuration dashboard shows the following list of portlets:

- Best Practices Deviation
- Discrepancies
- Job Information Status
- Device Change Audit
- Config Protocol Summary
- Hardware Summary
- Job Approval
- Software Summary
- Syslog Alerts

Best Practices Deviation

You can view the deviation type and the number of deviations using the Best Practices Deviation portlet. The Best Practices Deviation portlet helps you to view deviations from normal or recommended practices in a network and provides information on each of the Best Practice deviations reported in LMS. These deviations do not have a serious impact on the functioning of the network.

This portlet gives a description of the Best Practice Deviation. It includes the impact, if any, that the deviation has on the network and ways to resolve the deviation.
Table 2-1 lists Best Practices Deviation portlet details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Brief description of the deviation from the Best Practice.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of deviations. Click the number corresponding to the deviation to</td>
</tr>
<tr>
<td></td>
<td>navigate to the Unacknowledged Best Practices Deviation Reports.</td>
</tr>
<tr>
<td></td>
<td>This page displays details such as the type, summary, first found and</td>
</tr>
<tr>
<td></td>
<td>remarks.</td>
</tr>
</tbody>
</table>

You can click the portlet name in the title bar to navigate directly to the Report Generator page. Select **Best Practices Deviations** from the Select a Report drop-down list to navigate to the Best Practices Deviations page.

**Discrepancies**

In the Discrepancies portlet, you can view the type and count of discrepancies, such as network inconsistencies and anomalies or misconfigurations in the discovered network.

The Discrepancy portlet gives a description of the discrepancy, the impact it has on the network, and ways to resolve it.

LMS provides reports on discrepancies in the discovered network, enabling identification of configuration errors such as link-speed mismatches on either end of a connection. Discrepancies are computed at the end of each data collection schedule.

Table 2-2 lists the Discrepancies portlet details.
You can click the portlet name in the title bar to navigate directly to the Report Generator page. Select Discrepancies from the Select a Report drop-down list to navigate to the Network Discrepancy page.

### Table 2-2 Discrepancy Portlet Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the discrepancies such as network inconsistencies, anomalies or misconfigurations in the network. The available types are:</td>
</tr>
<tr>
<td></td>
<td>• Port is in Error Disabled State—Count of switch ports in the discovered network have a status of errDisable.</td>
</tr>
<tr>
<td></td>
<td>• VTP Disconnected Domain—Count of devices that are part of the same VTP domain have different VTP configuration revision numbers.</td>
</tr>
<tr>
<td></td>
<td>• Link Duplex Mismatch—Count of discrepancies when there is a duplex mismatch between links.</td>
</tr>
<tr>
<td></td>
<td>• Devices with duplicate SysName—Count of discrepancies when LMS discovers two devices with the same SysName.</td>
</tr>
<tr>
<td></td>
<td>• Trunk VLANs Mismatch—Count of discrepancies when the list of active or allowed VLANs between the two ends of a trunk do not match.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of deviations. Click the number corresponding to the deviation to navigate to the Unacknowledged Discrepancy Report in the application.</td>
</tr>
</tbody>
</table>

You can click the portlet name in the title bar to navigate directly to the Report Generator page. Select Discrepancies from the Select a Report drop-down list to navigate to the Network Discrepancy page.

### Job Information Status

In the Job Information Status portlet, you can view the status of up to 20 jobs of the installed applications. You can click the portlet name in the title bar of the portlet to navigate to the Job Browser page.

Table 2-3 lists Job Information Status portlet details.

### Table 2-3 Job Information Status Portlet Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique ID assigned to the job by the system, when the job is created. The Job IDs are displayed in ID.No.of.Instances format in periodic jobs. For example, the Job ID 1002.11 indicates that this is the eleventh instance of the job whose ID is 1002. When you click the Job ID, the job details, if available, are displayed.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Type of the job. For example, Inventory Collection, SyslogDefaultPurge, and NetConfig Job.</td>
</tr>
</tbody>
</table>
In the Device Change Audit portlet, you can view the changes in the inventory and configuration information for all the devices after every Inventory or Configuration Collection. However, the VLAN config change details will not be displayed. The changes in the exception period are displayed in red.

Table 2-4 lists the Device Change Audit portlet details.

### Table 2-4  Device Change Audit Portlet Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device name as entered in the Device and Credential Repository. Click or hover the mouse over the device name to view device details.</td>
</tr>
<tr>
<td>User Name</td>
<td>Name of the user who performed the change. This is the name entered when the user logged in.</td>
</tr>
<tr>
<td>Creation Time</td>
<td>Date and the time at which the application communicated the network change or when Change Audit saw the change record.</td>
</tr>
<tr>
<td>Message</td>
<td>Brief summary of the changes in the network change. You can click the Message link to navigate to the 24-hour Inventory Change Report details page.</td>
</tr>
</tbody>
</table>

In the Device Change Audit portlet, you can view the changes in the inventory and configuration information for all the devices after every Inventory or Configuration Collection. However, the VLAN config change details will not be displayed. The changes in the exception period are displayed in red.
You can click the portlet name in the title bar to navigate directly to the Report Generator page.

To configure the Device Change Audit portlet:

**Step 1** Move the mouse over the title bar of the Device Change Audit portlet to view the icons.

**Step 2** Click the Configuration icon. You can:
- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed Refresh time.
- Select the Only Exception Period Report checkbox to view any of the special or extraordinary period report.

**Step 3** Click **Save** to view the configured portlet with the changed settings.

### Config Protocol Summary

In Config Protocol Summary portlet, you can view the configuration protocol usage details for successful configuration fetches.

Table 2-5 lists the Config Protocol Summary details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Protocols used by LMS for fetching the configuration.</td>
</tr>
<tr>
<td>Config Type</td>
<td>The Configuration types for the various protocols. The available types are:</td>
</tr>
<tr>
<td></td>
<td>• Running — Count of the successful running configuration fetched for each protocol.</td>
</tr>
<tr>
<td></td>
<td>• Startup — Count of the successful startup configuration fetched for each protocol.</td>
</tr>
<tr>
<td></td>
<td>• VLAN — Count of the successful VLAN configuration fetched for each protocol. This configuration fetch is supported by only Telnet and SSH protocols.</td>
</tr>
</tbody>
</table>

Click the Count link to view a detailed report for a protocol and corresponding Config Type. The detailed report shows the list of devices which are accessed using a particular protocol and for which successful Config Fetch has happened.

**Example:**

If you click on a Count link, 20, for Telnet protocol and Running Config Type, a detailed report is generated with the following fields:
- Device Name — Device Name of each device.
- Accessed At — Date and time at which each device was accessed for Config Fetch purpose.
- Config Type — Configuration type for each device.
- File Type — Configuration file type for each device.
- This detailed report shows only the devices for which Telnet has successfully fetched configurations.

You can use the export icon to export the list of devices from this detailed report to the device selector.
Chapter 2  About Configuration Dashboard

Table 2-5  Config Protocol Summary Details (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config NeverCollected</td>
<td>The count of devices for which configuration fetch has never happened. Click the Count link to launch the Configuration Never Collected Device page.</td>
</tr>
<tr>
<td>Edit Protocol Order</td>
<td>Click this button, if you want to change the transport protocol order.</td>
</tr>
</tbody>
</table>

Hardware Summary

In the Hardware Summary portlet, you can view a pie graph that displays the distribution of all managed Cisco devices in the inventory. The graph plots the percentage count of devices, based on Cisco MetaData Framework (MDF) categorization of devices.

Each section represents the device category, the device count and percentage of total devices.

The portlet has the following view options:
- View as Grid—Shows the information in a table format.
- View as Chart—Shows the information in a pie-chart format.

Table 2-6 lists Hardware Summary portlet details.

Table 2-6  Hardware Summary

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Management</td>
<td>Percentage of network management used.</td>
</tr>
<tr>
<td>DSL and Long Reach Ethernet</td>
<td>Percentage of Ethernet used.</td>
</tr>
<tr>
<td>Security and VPN</td>
<td>Percentage of security and VPN used.</td>
</tr>
<tr>
<td>Switches and Hubs</td>
<td>Percentage of switches and hubs used.</td>
</tr>
<tr>
<td>Routers</td>
<td>Percentage of routers used.</td>
</tr>
<tr>
<td>Count</td>
<td>Count of the devices.</td>
</tr>
<tr>
<td></td>
<td>For instance, you can click the number corresponding to Switches and Hubs to navigate to the Hardware Report details page.</td>
</tr>
</tbody>
</table>

You can click the portlet name in the title bar to navigate directly to the Report Generator page.

For more information on how to generate the report, see section “Generating a Hardware Report” in Reports Management with Cisco Prime LAN Management Solution 4.2.
Job Approval

In Job Approval portlet, you can view the list of all jobs. Table 2-7 lists Job Approval portlet details.

Table 2-7   Job Approval Portlet Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>ID of the job that has been given for approval.</td>
</tr>
<tr>
<td></td>
<td>ID is the unique number assigned to the job. For periodic jobs such as Daily, Weekly, and so on, the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3, indicates that this is the third instance of the job ID 1001. Click the Job ID hyperlink to view the job details.</td>
</tr>
<tr>
<td>Job Description</td>
<td>Description of the job.</td>
</tr>
<tr>
<td>Job Schedule</td>
<td>Date and time for which the job has been scheduled.</td>
</tr>
</tbody>
</table>

The Job Approval portlet allows you to approve or reject a job for which you are an approver. A job will run only if it is approved. If the job is not approved by its scheduled runtime, or if an approver rejects it, the job is moved to its rejected state and will not run.

For periodic jobs, only one instance of the job needs to be approved. If one instance is approved, all other instances are also considered as approved.

You are notified by e-mail, when a job that has to be approved by you is created.

This portlet enforces the approval process by sending job requests through e-mail to people on the approver list.

You can click the portlet name in the title bar to navigate directly to the Jobs Pending Approval details page in LMS.

In the Job Approval portlet, you can view the list of Job details.

You can configure the Job Approval portlet to set the number of records to be displayed in the portlet and refresh time both manually and automatically.

To configure the Job Approval portlet:

**Step 1** Move the mouse over the title bar of the Job Approval portlet to view the icons.

**Step 2** Click the Configuration icon.

**Step 3** You can:

- Select the minute and hour from the Refresh Every drop-down list to change the refresh time. The items in the portlet get refreshed at the changed Refresh time.

- Select the number of records to be displayed in the portlet from the Show Last Records drop-down list.

**Step 4** Click **Save** to view the portlet with the configured settings.
Software Summary

In the Software Summary portlet, you can view the software version information and count for selected devices such as Cisco Interfaces and Modules, Switches and Hubs, Universal Gateways and Access Servers, and Routers.

Table 2-8 lists the Software Summary portlet details.

Table 2-8  Software Summary Portlet Details

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Categories</td>
<td>Categories of devices used in the application.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Software version of the device categories.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of devices.</td>
</tr>
<tr>
<td></td>
<td>For instance, you can click on the number corresponding to Switches and Hubs to navigate to the Software Report details page.</td>
</tr>
</tbody>
</table>

You can click the portlet name in the title bar to navigate directly to the Report Generator page.

For more information on how to generate the report, see section “Generating a Software Report” in Reports Management with Cisco Prime LAN Management Solution 4.2.

Configuring Software Summary Portlet

To configure the Software Summary portlet:

Step 1  Move the mouse over the title bar of the Software Summary portlet to view the icons.
Step 2  Click the Configuration icon.

You can:

• Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed Refresh time.
• Select the number of rows to be displayed in the portlet from the No. of Rows to be Displayed drop-down list.

Step 3  Click Save to view the portlet with the configured settings.

Syslog Alerts

The Syslog Alerts portlet displays the 24-hour Syslog event distribution as a pie chart. It also displays the total number of Syslog counts.

The portlet displays the top ten syslog summary reports.

The portlet has the following view options:

• View as Grid—Shows the information in a table format.
• View as Chart—Shows the information in a pie-chart format.
To configure the Syslog Summary portlet:

**Step 1** Move the mouse over the title bar of the Syslog Summary portlet.
**Step 2** Click the configuration icon.
You can:
- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed refresh time.
- Select the number of rows to be displayed in the portlet from the No.of Rows to be Displayed drop-down list.
- Select the Show graph checkbox.
**Step 3** Click **Save** to view the portlet with the configured settings.
Chapter 2  About Configuration Dashboard

Syslog Alerts
Managing and Deploying Templates

This chapter guides you to manage and deploy configuration templates in LMS. It explains:

• Accessing Template Center
• Creating Configuration Templates
• Deploying Templates
• Managing Templates
• Importing Templates
• Assigning Templates to Users
• Understanding the Template Center Jobs Browser
• Guidelines for Creating Configuration Templates Using IF and FOREACH Statements
Accessing Template Center

The Template Center in LMS provides you with a list of both system-defined templates and user-defined templates. These templates contain configuration commands that can be deployed on the devices in your network. These templates are deployed using Deploy Template jobs in LMS.

You can make customized versions of these system-defined templates, by exporting them, changing CLI's/parameters in template XML according to needs, and importing it back after changing the template name. You can also import templates from a client machine and these templates are stored as user-defined templates in LMS.

It is highly recommended to the user to understand the commands in the template and use it according to their network requirements and other configurations already done/to be done.

To access Template Center, go to Configuration > Tools > Template Center.

Table 3-1 describes a list of system-defined templates shipped into LMS 4.2.
### Table 3-1  
**System-defined Templates**

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMP Location Configuration</td>
<td>This template configures location information on access ports connected to Digital Media Player. This is a port-based template.</td>
</tr>
</tbody>
</table>
| Guaranteed Audio              | This Template offers voice services with point-to-point guarantees in an MPLS network. It also offers predictable packet delivery characteristics at various network conditions and loads.  
When you configure this profile, the system attempts to display video for all participants; however, it does not guarantee that the video of all participants is displayed. For those participants whose video is not displayed, participants are downgraded to audio-only and the profile guarantees preservation of the audio portion of the call. |
| Heterogeneous Video Conference| This template allows the participants to use different video formats. You can configure different frame rates, bit rates, codecs, or resolutions, and you have the flexibility to choose what profiles to configure, depending on the nature of the participants. |
| Homogeneous Video Conference  | This template allows all the participants in the conference to use the same video format. You must configure the same bit rate, frame rate, codec, resolution, and so on. Only one codec, resolution, and bit rate is configured. All other participants are forced to negotiate to match this profile to join the video conference. If negotiation fails, they fall back to audio-only participants. |
| Identity - Change of Authorization | This template provides a mechanism for changing the attributes of a session after authentication. When a change in authentication, authorization, and accounting (AAA) policy occurs for a user or user group, administrators can send the RADIUS CoA packets from the AAA server, such as the Cisco Secure Access Control Server (ACS), to re-initialize authentication and apply the new policies.  
In LMS, you can use this CoA template to generate the configuration commands that can be deployed on devices in your network device to enable Change of Authorization on the device. |
| IPVSC Location Configuration  | This template configures location information on access ports connected to IP Video Surveillance Camera. This is a port-based template.                                                                         |
| L2 Access Edge Interface Configuration | This template focuses on Ethernet access interface. It provides Cisco best practice for interface configuration that includes Port security, dhcp snooping, IP Source guard (IPSG), Dynamic ARP Inspection (DAI) and Quality of Service (QoS).  
This template requires global configuration for IPSG, DAI, and DHCP snooping. |
| Location Configuration        | This template configures location information on access ports connected to any endpoint. This is a port-based template.                                                                                   |
MACsec allows unauthorized LAN connections to be identified and excluded from communication within the network. MACsec defines a security infrastructure to provide data confidentiality and data integrity. MACsec can mitigate attacks on Layer 2 protocols and work with any type of traffic carried over Ethernet links.

You can use this template to configure:

- Security policy to be applied to the session after the supplicant passes 802.1x authentication.
- Authentication Failure Policy.
- MKA policy.

Guidelines for this template:

- Select any value from the Authentication Failure Policy drop-down list, only if Static Link Policy is Always Secure Sessions.
  For other values of Static Link Policy, select No Change as the Authentication Failure Policy.
- Enter a value for VLAN To Be Used only if Authentication Failure Policy is Authorize into a VLAN.
- Enter a name of the other MKA Policy only if MKA Policy is Other Policy.

Note: If you do not adhere to these guidelines, wrong commands can get deployed.

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
</table>
| MACsec   | This template allows you to enable MACsec to provide secure, encrypted communication on wired LANs. MACsec allows unauthorized LAN connections to be identified and excluded from communication within the network. MACsec defines a security infrastructure to provide data confidentiality and data integrity. MACsec can mitigate attacks on Layer 2 protocols and work with any type of traffic carried over Ethernet links. You can use this template to configure:
  - Security policy to be applied to the session after the supplicant passes 802.1x authentication.
  - Authentication Failure Policy.
  - MKA policy. Guidelines for this template:
    - Select any value from the Authentication Failure Policy drop-down list, only if Static Link Policy is Always Secure Sessions.
      For other values of Static Link Policy, select No Change as the Authentication Failure Policy.
    - Enter a value for VLAN To Be Used only if Authentication Failure Policy is Authorize into a VLAN.
    - Enter a name of the other MKA Policy only if MKA Policy is Other Policy. Note: If you do not adhere to these guidelines, wrong commands can get deployed. |
Performance Monitoring You can configure the following for endpoints like Cisco Unified Video Advantage (CUVA), Cisco TelePresence Movi, Tandberg, Webex Servers, and voice data on all endpoints:

- A flow record to specify the key and non-key fields you want to monitor.
- A flow monitor that includes the flow record and flow exporter.
- A class to specify the filtering criteria.
- A policy to include one or more classes.
- One or more performance-monitor type flow monitors.
- Reaction ID, jitter and threshold of lost packets.

Before you deploy any Performance Monitoring template on a router, you must apply the license command on the router devices.

To apply the license in a router:

1. Go to config mode.
2. Enter the following commands:
   
   ```
   license boot module <device series> technology-package datak9
   wr mem
   ```
3. Reboot the router.

### Table 3-1  System-defined Templates (continued)

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Monitoring</td>
<td>You can configure the following for endpoints like Cisco Unified Video Advantage (CUVA), Cisco TelePresence Movi, Tandberg, Webex Servers, and voice data on all endpoints:</td>
</tr>
<tr>
<td></td>
<td>- A flow record to specify the key and non-key fields you want to monitor.</td>
</tr>
<tr>
<td></td>
<td>- A flow monitor that includes the flow record and flow exporter.</td>
</tr>
<tr>
<td></td>
<td>- A class to specify the filtering criteria.</td>
</tr>
<tr>
<td></td>
<td>- A policy to include one or more classes.</td>
</tr>
<tr>
<td></td>
<td>- One or more performance-monitor type flow monitors.</td>
</tr>
<tr>
<td></td>
<td>- Reaction ID, jitter and threshold of lost packets.</td>
</tr>
<tr>
<td></td>
<td>Before you deploy any Performance Monitoring template on a router, you must apply the license command on the router devices.</td>
</tr>
<tr>
<td></td>
<td>To apply the license in a router:</td>
</tr>
<tr>
<td></td>
<td>1. Go to config mode.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the following commands:</td>
</tr>
</tbody>
</table>
|                                 |       license boot module <device series> technology-package datak9
|                                 |       wr mem |
|                                 |   3. Reboot the router. |
| Performance Monitoring-CUVA     | This template allows you to configure Performance Monitor on Cisco Unified Video Advantage (CUVA). CUVA adds video to your communications experience by providing video telephony functionality to Cisco Unified IP phones. |
| Performance Monitoring-Movi     | This template allows you to configure Performance Monitor on Cisco TelePresence Movi. Cisco TelePresence Movi extends the benefits of face-to-face video collaboration to remote workers. |
| Performance Monitoring-Tandberg | This template allows you to configure Performance Monitor on all Cisco all Tandberg Endpoints. Tandberg video endpoints work together to provide video users with the full functionality of IP telephony. |
| Performance Monitoring-Voice    | This template allows you to configure Performance Monitor for voice data on all endpoints. |
| Performance Monitoring-Webex Servers | This template allows you to configure Performance Monitor on Webex Servers. |
| PFR                             | This template caters for Performance Routing (PFR) that provides best path optimization and advanced load balancing of traffic over the WAN and to the Internet for enterprise networks with multiple paths. |
|                                 | You can |
|                                 |   - Configure traffic classes for performance routing. |
|                                 |   - Configure performance metrics of these individual traffic classes. |
|                                 |   - Control the traffic by applying suitable traffic class and link policies. |
### Table 3-1  System-defined Templates (continued)

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS</td>
<td>This template provides Quality of Service (QoS) macros to switch ports upon detection of a Medianet endpoint.</td>
</tr>
<tr>
<td></td>
<td>You can</td>
</tr>
<tr>
<td></td>
<td>• Select specific network traffic.</td>
</tr>
<tr>
<td></td>
<td>• Prioritize it according to its relative importance.</td>
</tr>
<tr>
<td></td>
<td>• Use QoS macros to provide preferential treatment of traffic in your network.</td>
</tr>
<tr>
<td>RSVP</td>
<td>Resource Reservation Protocol (RSVP) signals the QoS needs of an application's traffic along the devices, in the end-to-end path through the network.</td>
</tr>
<tr>
<td></td>
<td>You can configure:</td>
</tr>
<tr>
<td></td>
<td>• User or application that requires an RSVP request.</td>
</tr>
<tr>
<td></td>
<td>• Bandwidth that has to be reserved.</td>
</tr>
<tr>
<td></td>
<td>• Admission policy that the devices uses to admit the RSVP message.</td>
</tr>
<tr>
<td>SBA</td>
<td>LMS provides various Smart Business Architecture (SBA) templates to configure resilience, QoS, security and, scalability for SBA networks, for different types of devices. For more information, see <a href="#">Creating Configuration Templates</a>.</td>
</tr>
<tr>
<td>SCH</td>
<td></td>
</tr>
<tr>
<td>SCH on IOS and ASA platforms</td>
<td>This template allows you to configure Smart Call Home (SCH) parameters on IOS and ASA devices.</td>
</tr>
<tr>
<td>SCH on MDS platform</td>
<td>This template allows you to configure Smart Call Home parameters on MDS devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You can use this template only on MDS devices with NX-OS 4.1(3) or higher software version. SanOS is not supported for the HTTPS transport.</td>
</tr>
<tr>
<td></td>
<td>In this template, when you enter the Contact Phone Number, it should be in international format and begin with a + sign. You can use hyphens but no spaces in between, for example:</td>
</tr>
<tr>
<td></td>
<td>• +1-100-100-1000</td>
</tr>
<tr>
<td></td>
<td>• +11001001000</td>
</tr>
<tr>
<td></td>
<td>• +919840011111</td>
</tr>
<tr>
<td></td>
<td>The phone number can have a maximum of 17 characters, including the + sign. LMS validates only the format of the phone number and not the maximum length. If the phone number has more than 17 characters, the command will fail when you deploy the template on the device.</td>
</tr>
</tbody>
</table>
Table 3-1  System-defined Templates (continued)

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCH on Nexus platform</td>
<td>This template allows you to configure Smart Call Home parameters on Nexus devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  You can use this template only on Nexus devices with NX-OS 4.1(3) or higher software version. SanOS is not supported for the HTTPS transport.</td>
</tr>
<tr>
<td></td>
<td>In this template, when you enter the Contact Phone Number, it should be in international format and begin with a + sign. You can use hyphens but no spaces in between, for example:</td>
</tr>
<tr>
<td></td>
<td>• +1-100-100-1000</td>
</tr>
<tr>
<td></td>
<td>• +11001001000</td>
</tr>
<tr>
<td></td>
<td>• +919840011111</td>
</tr>
<tr>
<td></td>
<td>The phone number can have a maximum of 17 characters, including the + sign. LMS validates only the format of the phone number and not the maximum length. If the phone number has more than 17 characters, the command will fail, when you deploy the template on the device.</td>
</tr>
<tr>
<td>SGA Access</td>
<td>The Security Group Access (SGA) Access template allows you to enable SXP on the Access devices and allows you to propagate the Security Group Tags (SGT) across network devices that do not have hardware support for Cisco TrustSec.</td>
</tr>
<tr>
<td></td>
<td>You can use this template to configure:</td>
</tr>
<tr>
<td></td>
<td>• Default SGT Exchange Protocol (SXP) password.</td>
</tr>
<tr>
<td></td>
<td>• SXP address connection.</td>
</tr>
<tr>
<td></td>
<td>• Default SXP source IP address.</td>
</tr>
<tr>
<td>SGACL-IOS</td>
<td>In security group access lists (SGACLs), you can control the operations based on assigned security groups. The grouping of permissions into a role simplifies the management of the security policy. As you add users to the Cisco NX-OS device, you simply assign one or more security groups and they immediately receive the appropriate permissions. You can modify security groups to introduce new privileges or restrict current permissions.</td>
</tr>
<tr>
<td>SGACL-NEXUS</td>
<td>In security group access lists (SGACLs), you can control the operations based on assigned security groups. The grouping of permissions into a role simplifies the management of the security policy. As you add users to the Cisco NX-OS device, you simply assign one or more security groups and they immediately receive the appropriate permissions. You can modify security groups to introduce new privileges or restrict current permissions.</td>
</tr>
<tr>
<td>SGA Core</td>
<td>The Security Group Access (SGA) Core template allows you to enable SXP on the Nexus devices and allows you to propagate the Security Group Tags (SGT) across Nexus devices that do not have hardware support for Cisco TrustSec.</td>
</tr>
<tr>
<td></td>
<td>You can use this template to configure:</td>
</tr>
<tr>
<td></td>
<td>• Default SGT Exchange Protocol (SXP) password.</td>
</tr>
<tr>
<td></td>
<td>• SXP address connection.</td>
</tr>
<tr>
<td></td>
<td>• Default SXP source IP address.</td>
</tr>
</tbody>
</table>
### Table 3-1  System-defined Templates (continued)

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small Branch EIGRP DMVPN FaxRelay</td>
<td>This Template caters for services ready small branch. The configuration includes security features like DMVPN (primary and backup), Firewall (Zone based), IPS and unified communications (SRST). The WAN link is T1, encapsulation is Frame Relay. Backup is SHSDL with ATM IMA. <strong>Hardware and Software Pre-requisites</strong> HWIC-1T1/E1, PVDM2-32, AIM-CUE, 128 MB DRAM, 64 MB flash 1800 series with IOS 12.4.(20)T2 K9 and above with advanced enterprise package.</td>
</tr>
<tr>
<td>Small Branch EIGRP DMVPN Only</td>
<td>This Template caters for services ready small branch. The configuration includes security features like DMVPN (primary and backup), Firewall (Zone based), IPS. The WAN link is T1, encapsulation is Frame Relay. Backup is SHSDL with ATM IMA. <strong>Hardware and Software Pre-requisites</strong> HWIC-1T, HWIC-2SHDSL, 128 MB DRAM, 64 MB flash 1800 series with IOS 12.4.(15)T7 K9 and above with advanced enterprise package. T100 Crads should be available in the device.</td>
</tr>
<tr>
<td>Small Branch EIGRP GETVPN FaxPassThrough</td>
<td>This Template caters for services ready small branch. The configuration includes security features like GETVPN (primary) and DMVPN (backup), Firewall (Zone based), IPS and unified communications (CME SIP). The WAN link is T1 encapsulation is PPP. Backup is SHSDL with ATM IMA. <strong>Hardware and Software Pre-requisites</strong> HWIC-1T1/E1, PVDM2-32, AIM-CUE, 128 MB DRAM, 64 MB flash 1800 series with IOS 12.4.(20)T2 K9 and above with advanced enterprise package.</td>
</tr>
<tr>
<td>Small Branch OSPF GETVPN FaxPassThrough</td>
<td>This Template caters for services ready small branch. The configuration includes security features like GETVPN (primary) and DMVPN (backup), Firewall (Zone based), IPS and unified communications (SIP SRST). The WAN link is T1, encapsulation is Frame Relay. Backup is SHSDL with ATM IMA. <strong>Hardware and Software Pre-requisites</strong> HWIC-1T1/E1, PVDM2-32, AIM-CUE, 128 MB DRAM, 64 MB flash 1800 series with IOS 12.4.(20)T2 K9 and above with advanced enterprise package.</td>
</tr>
<tr>
<td>SXP-IOS</td>
<td>Some network devices do not support secured group tag (SGT). For such devices, you can use the SGT Exchange Protocol (SXP) to propagate SGTs. This template is used for SXP configuration. An SXP peer that sends IP-to-SGT binding information to another peer is called SXP Speaker. Any device that receives the binding table and applies it to the ingress port for tagging is called SXP listener. You must configure the SXP peer connection on both the speaker and the listener. When using password protection, make sure that you use the same password on both the speaker and the listener devices.</td>
</tr>
</tbody>
</table>
Chapter 3 Managing and Deploying Templates

Accessing Template Center

Table 3-1 System-defined Templates (continued)

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SXP-NEXUS</td>
<td>Some network devices do not support secured group tag (SGT). For such devices, you can use the SGT Exchange Protocol (SXP) to propagate SGTs. This template is used for SXP configuration. An SXP peer that sends IP-to-SGT binding information to another peer is called SXP Speaker. Any device that receives the binding table and applies it to the ingress port for tagging is called SXP listener. You must configure the SXP peer connection on both the speaker and the listener. When using password protection, make sure that you use the same password on both the speaker and the listener devices.</td>
</tr>
<tr>
<td>Video Transcode</td>
<td>The template provides video transcoding services, where video can be converted from one format to another. You can configure video transcoding when the bit rate, frame rate, resolution, or codec is different between two endpoints.</td>
</tr>
</tbody>
</table>

**Note**

The Basic Small Branch Network provides security and network manageability for the small branch, and integrates the various network services to the branch office router. To deploy these templates ensure that device management IP address is configured in Fa 0/0. This template will remove the IP address in all the other interfaces mentioned in the template.

The above note is applicable for templates such as Small Branch EIGRP DMVPN Only, Small Branch OSPF GETVPN FaxPassThrough, Small Branch EIGRP DMVPN FaxRelay and Small Branch EIGRP GETVPN FaxPassThrough.

Supported SBA Templates

LMS provides various SBA templates to configure resilience, QoS, security, and scalability for Smart Business Architecture networks, for different types of devices. The various SBA templates supported in this release are:

<table>
<thead>
<tr>
<th>Name of Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Switch Global Configuration</td>
<td>Use this template to configure Virtual LANs, in-band management, DHCP snooping and ARP inspection on the switch.</td>
</tr>
<tr>
<td>Distribution Layer Switch Global Configuration</td>
<td>Use this template to configure an in-band management interface, IP unicast routing, and IP multicast routing.</td>
</tr>
<tr>
<td>Core Switch Global Configuration</td>
<td>Use this template to configure an in-band management interface, IP unicast routing, IP multicast routing. Use this template to configure an in-band management interface, IP unicast routing, and IP multicast routing.</td>
</tr>
<tr>
<td>LAN Switch Universal Configuration</td>
<td>Use this template to configure the features and services that are common across all LAN switches, regardless of the type of platform or role in the network. These are system settings that simplify and secure the management of the solution.</td>
</tr>
<tr>
<td>Name of Template</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Client Connectivity Configuration</td>
<td>Use this template to configure switch interfaces to support clients and IP phones, port security on the interface, DHCP snooping, and ARP inspection and BPDU guard on the interface.</td>
</tr>
<tr>
<td>Multicast Source Discovery Protocol (MSDP) for Core Switches</td>
<td>Use this template to enable Multicast Source Discovery Protocol (MSDP) for core switches.</td>
</tr>
<tr>
<td>Catalyst 4500 Access Switch Global Configuration</td>
<td>Use this template to configure Virtual LANs, in-band management, DHCP snooping and ARP inspection on the switch.</td>
</tr>
<tr>
<td>Catalyst 4500 Distribution Layer Connectivity to Access Layer</td>
<td>Use this template to configure connectivity to access layer switches.</td>
</tr>
<tr>
<td>Catalyst 4500 Client Connectivity Configuration</td>
<td>Use this template to configure switch interfaces to support clients and IP phones, port security on the interface, DHCP snooping, ARP inspection and BPDU guard on the interface.</td>
</tr>
<tr>
<td>Catalyst 4500 Platform Configuration</td>
<td>This is a platform template that defines macros used in Catalyst 4500 Series templates to apply the platform specific configuration.</td>
</tr>
<tr>
<td>Catalyst 4500 and 6500 LAN Switch Universal Configuration</td>
<td>Use this template to configure the features and services that are common across all LAN switches, regardless of the type of platform or role in the network. These are system settings that simplify and secure the management of the solution.</td>
</tr>
<tr>
<td>Catalyst 6500 Series switches Platform Configuration</td>
<td>This is a platform template that defines macros used in Catalyst 6500 Series templates to apply the platform specific configuration.</td>
</tr>
<tr>
<td>Catalyst 6500 Distribution Layer Switch Global Config</td>
<td>Use this template to configure an in-band management interface, IP unicast routing, IP multicast routing.</td>
</tr>
<tr>
<td>Catalyst 3750 and 3750X Platform Configuration</td>
<td>This is a platform template that defines macros used in Catalyst 3750 and 3750X series templates to apply the platform specific configuration.</td>
</tr>
<tr>
<td>Catalyst 3750G Distribution Layer Switch Global Config</td>
<td>Use this template to configure an in-band management interface, IP unicast routing, IP multicast routing.</td>
</tr>
<tr>
<td>Catalyst 2960-S and 3750-X Platform Configuration</td>
<td>This is a platform template that defines macros that is used in Catalyst 2960-S and 3750-X series templates to apply the platform specific configuration.</td>
</tr>
<tr>
<td>Distribution Layer Aggregation Configuration</td>
<td>Use this template to configure links in the core layer that are configured as point-to-point Layer 3 routed EtherChannels.</td>
</tr>
<tr>
<td>Connectivity to WAN Routers and LAN Core</td>
<td>Use this template to configure connectivity to WAN Routers and LAN Core.</td>
</tr>
<tr>
<td>Infrastructure Connectivity to Routers for 2960 Switches</td>
<td>Use this template when connecting to a network infrastructure device that does not support LACP like a router.</td>
</tr>
<tr>
<td>Catalyst 4500 Infrastructure Connectivity to Switches</td>
<td>Use this template to connect to another switch when LACP is set to active on both sides to ensure a proper EtherChannel is formed.</td>
</tr>
<tr>
<td>Catalyst 4500 Infrastructure Connectivity to Routers</td>
<td>Use this template to connect to a network infrastructure device that does not support LACP like a router.</td>
</tr>
<tr>
<td>Name of Template</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cat6500 Connectivity to WAN Routers and LAN Core</td>
<td>Use this template to connect to WAN Routers and LAN Core.</td>
</tr>
<tr>
<td>Cat6500 Distribution Layer Connectivity to Access Layer</td>
<td>Use this template to configure connectivity to access layer switches.</td>
</tr>
<tr>
<td>3750X 3560X Infrastructure Connectivity to Distribution Switch</td>
<td>Use this template to connect to another switch when Link Aggregation Control Protocol (LACP) is set to active on both sides to ensure that a proper EtherChannel is formed.</td>
</tr>
<tr>
<td>3750X 3560X Infrastructure Connectivity to WAN Router</td>
<td>Use this template to connect to a network infrastructure device that does not support LACP like a router.</td>
</tr>
<tr>
<td>Catalyst 3750 Distribution Layer Connectivity to Access</td>
<td>Use this template to configure connectivity to access layer switches.</td>
</tr>
<tr>
<td>Cat 2960S Infrastructure Configuration to Distribution Switches</td>
<td>Use this template to connect to another switch when LACP is set to active on both sides to ensure that a proper EtherChannel is formed.</td>
</tr>
<tr>
<td>Catalyst 3560-X Platform Configuration</td>
<td>This is a platform template that defines macros used in Catalyst 3560-X series templates to apply the platform specific configuration.</td>
</tr>
</tbody>
</table>
Creating Configuration Templates

CLI templates are user-defined templates that are created based on your own parameters. CLI templates allow you to choose the elements in the configurations. LMS provides variables that you replace with actual values and logic statements.

Prerequisites for Creating CLI Templates

Creating CLI templates is an advanced function that should be done by expert users. Before you create a CLI template, you should:

• Understand to what devices the CLI you create can be applied.
• Understand the data types supported by Prime NCS (WAN).

To create a new configuration template:

Step 1 Select Configuration > Tools > Template Center > CLI Template Creation.
Step 2 Enter the name of the template.
Step 3 Enter the help description for the template.
Step 4 Enter the template description.
Step 5 Click the icon to select the device type for applying the configuration template.
Step 6 Select the device type from the device selector and click OK.

Note You cannot create configuration template, if you select a non supported device type.
Configuration template will be created only for supported device type, if you select both supported and non-supported device types.

Step 7 Select the OS Name from the dropdown list.
Step 8 Enter the CLI content in the text area provided in the Template Detail pane.
For example, enter hostname
Step 9 Click Manage Variables button to include variables in the CLI content. The Manage Variable window appears.
To add a new variable to the CLI content:

a. Click Add Row.

b. Enter the name of the variable. For example, enter devicehostname.

c. Select the variable type as String, Integer or IPv4Address. For example, select string.

d. Enter the display label of the variable. For example, Enter HostName

e. Enter the help description for the variable.

f. Select Required checkbox, if you want the variable to appear as mandatory field.
g. Click the arrow icon next to Name to enter the range, default value and validation expression for the variable.

Validation expression indicates an expression which is used to validate the variable. For example, if the variable is hostname, the following validation expression can be used:

```
[\S]+$  
```

The above expression indicates that you can enter only a single word without any spaces as hostname.

Range field will be disabled, if you select variable type as String or IPv4Address.

h. Click Save to save the variable details.

i. Click Add to add the variable to the CLI content. For example, hostname ${devicehostname} will be displayed.

To close the Manage Variable window, click Close.

You can see the content in form view on clicking the Form View tab.

You can edit or delete the required variable from the Manage Variable window.

You can also filter the variables using the Filter or Advanced Filter option.
### Table 3-2 Filter Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Filter</td>
<td>You can filter the variable based on the following:</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Type</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Display Name</td>
</tr>
<tr>
<td></td>
<td>• Required</td>
</tr>
<tr>
<td>Advanced Filter</td>
<td>Select Match type as All or Any.</td>
</tr>
<tr>
<td></td>
<td>• All - To filter the variables that match all the selected parameters.</td>
</tr>
<tr>
<td></td>
<td>• Any - To filter the variables that match any of the selected parameter.</td>
</tr>
<tr>
<td></td>
<td>Select a parameter for which you want to filter the variables. The values</td>
</tr>
<tr>
<td></td>
<td>displayed are:</td>
</tr>
<tr>
<td></td>
<td>• Default Value</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Display Name</td>
</tr>
<tr>
<td></td>
<td>• Max Value</td>
</tr>
<tr>
<td></td>
<td>• Min Value</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Required</td>
</tr>
<tr>
<td></td>
<td>• Type</td>
</tr>
<tr>
<td></td>
<td>• Validation Expression</td>
</tr>
<tr>
<td></td>
<td>Select the right criterion with respect to the parameter. The values are:</td>
</tr>
<tr>
<td></td>
<td>• Contains</td>
</tr>
<tr>
<td></td>
<td>• Does not contain</td>
</tr>
<tr>
<td></td>
<td>• Starts with</td>
</tr>
<tr>
<td></td>
<td>• Ends with</td>
</tr>
<tr>
<td></td>
<td>• Is empty</td>
</tr>
<tr>
<td></td>
<td>• Is not empty</td>
</tr>
<tr>
<td></td>
<td>• Is exactly (or equals)</td>
</tr>
<tr>
<td></td>
<td>• Does not equal</td>
</tr>
<tr>
<td></td>
<td>• Is greater than</td>
</tr>
<tr>
<td></td>
<td>• Is less than</td>
</tr>
<tr>
<td></td>
<td>• Is greater than or equal to</td>
</tr>
<tr>
<td></td>
<td>• Is less than or equal to</td>
</tr>
<tr>
<td>Manage Preset Filter</td>
<td>You can edit or remove a preset filter.</td>
</tr>
</tbody>
</table>
Step 10  Click **Save to File** to save the newly created template details. To return to the previous page, click **Cancel**.

Click **Import to Template Center** to import the newly created configuration template to Template Center.

For details on how to use IF and FOREACH statements while generating configuration templates, see **Guidelines for Creating Configuration Templates Using IF and FOREACH Statements**.

## Deploying Templates

Templates are deployed to devices using Deploy Template job in LMS. You can deploy these templates for devices, ports and modules.

By default, LMS groups the templates as:
- Custom Templates—Lists all the user-defined templates assigned to the current user.
- Cisco Best Practises Templates—Lists all the system-defined templates.

You can use the filter option to group the templates.

In LMS 4.2, click the expandable icon before each template (triangle-shaped) to see the details of each template. For more details, see **Template Details**.

To deploy a template:

### Step 1
Select **Configuration > Tools > Template Center > Deploy**.

The Template Deployment page appears, displaying Template Selector pane.

You can select templates to deploy configurations.

**Table 3-3** describes the Template Selector pane.

<table>
<thead>
<tr>
<th><strong>Table 3-3 Template Selector</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column/Button</strong></td>
</tr>
<tr>
<td>Template Name</td>
</tr>
<tr>
<td>Features</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Role In Network</td>
</tr>
<tr>
<td>Category</td>
</tr>
<tr>
<td>Created By</td>
</tr>
</tbody>
</table>
Deploying Templates

Step 2

Select templates and click Next.

You can select:

- One Complete with multiple partial templates
- Multiple partial templates

You cannot select multiple Complete templates.

When you select multiple templates, if conflicting features exists between templates, then the deploy template flow will not proceed and a warning message is shown. See Importing Templates for more information on conflicting features.

The Choose Device Groups pane appears, displaying the Device Selector. Choose the devices, or device groups on which you wish to deploy the templates.

The Device Selector displays devices that are common and applicable to the selected templates.

Note

Starting from LMS 4.2.2 Release, the single Performance Routing template will be replaced with three templates namely PfR Basic MC (Master Controller) Template, PfR Basic Border Router, and PfR Advanced MC Template.

Note

If the devices selected is more than 2000, the progress bar is not shown.

Step 3

Select devices from the Device Selector and click Next.

If you are unable to view any devices in the Device Selector, you do not have any supported devices for the template.

- If you have selected port-related templates, Choose Port Groups pane appears, displaying the Port Selector.
  - Select port groups from the Port Group Selector and click Next.

  The Review Port Groups page appears with a list of selected devices and selected ports, from the previous page, associated with each device.

Table 3-3 Template Selector

<table>
<thead>
<tr>
<th>Column/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Shows the scope of the template for device, port, or module.</td>
</tr>
<tr>
<td>Filter (button)</td>
<td>Click Filter. Select a Filter By criteria from the drop-down list and enter the details in the Equals field. Click Go to filter details.</td>
</tr>
<tr>
<td></td>
<td>The following Filter By options are available:</td>
</tr>
<tr>
<td></td>
<td>- Template Name—Select Template Name and enter the complete name.</td>
</tr>
<tr>
<td></td>
<td>- Type—Select Type and enter the type (partial, complete)</td>
</tr>
<tr>
<td></td>
<td>- Role In Network—Select RIN and enter the RIN (access, distribution, core)</td>
</tr>
<tr>
<td></td>
<td>- Category—Select Category and enter the device category</td>
</tr>
<tr>
<td></td>
<td>- Created By—Select Created By and enter the user name</td>
</tr>
<tr>
<td></td>
<td>- Scope—Select Scope and enter the scope (device, port, module)</td>
</tr>
<tr>
<td></td>
<td>You can also use wild card character (*) along with the search text to filter.</td>
</tr>
</tbody>
</table>
– Unselect the ports that you want to exclude from the deployment.

• If you have selected module-related templates, Choose Module Groups pane appears, displaying the Device Selector.

**Step 4** Click Next, the corresponding template pane appears, allowing you to enter the applicable values for the template.

**Note** For SGACL-IOS template, the configuration command will fail if the device having SYSOID “1.3.6.1.4.1.9.1.282” and image version “12.2(50)SY” is not present in "adventerprisek9" package.

**Step 5** Enter the values and click Next.

The Adhoc Configuration for Selected Port/Device Groups pane appears, allowing you to enter the configuration commands that will be deployed on the selected devices or ports in addition to the commands in the template. The commands that you enter here will not be validated by LMS.

This is optional.

**Step 6** Click Next.

The Schedule Deployment pane appears, displaying Scheduler and Job Options details.

**Table 3-4** Schedule Deployment Pane Description

<table>
<thead>
<tr>
<th>Options/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Options</td>
<td>Specifies the type of schedule for the job:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs the report immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs the report once at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>• Daily—Runs daily at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly—Runs weekly on a day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Monthly—Runs monthly on a day of the month and at the specified time.</td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter a description for the job that you are scheduling. This is a mandatory</td>
</tr>
<tr>
<td></td>
<td>field. Accepts alphanumeric values and special characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter the e-mail address to which the job sends messages when the job has</td>
</tr>
<tr>
<td></td>
<td>run. You can enter multiple e-mail addresses separated by comma.</td>
</tr>
<tr>
<td>Job Options</td>
<td>The following job options are available:</td>
</tr>
<tr>
<td></td>
<td>• Copy Startup to Running Config upon failure—If template deployment job</td>
</tr>
<tr>
<td></td>
<td>fails, the startup configuration of the device is copied to running</td>
</tr>
<tr>
<td></td>
<td>configuration.</td>
</tr>
<tr>
<td></td>
<td>• Enable Job Password—Select Enable Job Password and enter the Login user</td>
</tr>
<tr>
<td></td>
<td>name, Login Password and Enable Password details.</td>
</tr>
<tr>
<td>Preview CLI</td>
<td>Click Preview CLI to open the Configuration Preview pop-up dialog box.</td>
</tr>
<tr>
<td>(button)</td>
<td>You can select the device name from the drop-down list to view the CLI</td>
</tr>
<tr>
<td></td>
<td>commands that will be deployed on to the device.</td>
</tr>
</tbody>
</table>
Step 7  Enter a Job Description, select the Schedule and Job options and click **Finish**.
A notification message appears along with the Job ID. The newly created job appears in the Template Center Jobs.

---

**Template Details**
You can see the following details when you click the expandable icon before each template (triangle-shaped) to see the details of each template:

- **Name**—Name of the template. For example, Access PortChannel Interface.
- **Description**—Description of the template. For example, Template for configuring Portchannel Interface on Access Switches.
- **Task**—Configuration task of the template. For example, Port Configuration.
- **Version**—Version of the template. For example, 1.0.
- **Feature**—Features supported for this template.
- **Hardware**—The hardware platform supported for deploying this template.
- **Reference**—Displays any reference text for the template. It can be a link for additional information about the template, or a file in the server.
- **Tag**—Displays the tags that have been specified for the template. You can have multiple tags for a single template. You can use this for filtering the templates using the Advanced Filter.

**Managing Templates**

LMS allows you to edit, delete, export and view templates.

By default, LMS groups the templates as:

- **Custom Templates**—Lists all the user-defined templates assigned to the current user.
- **Cisco Best Practices Templates**—Lists all the system-defined templates.

You can use the filter option to group the templates.

This section details:

- **Editing Templates**
- **Deleting Templates**
- **Exporting Templates**
- **Handling Multi-line Commands**
- **Viewing Template Details**
Editing Templates

You can edit the default values of a template (system or user-defined) and save it as user-defined template.

In LMS 4.2, each template has a reference section. In the reference section, you can add a link to provide additional information about the template. The information that you enter in the Text To Display text box appears as a link in the expandable pane of the template. When you click the link, it launches the URL or opens the file specified and provides the additional information. You can provide the additional information from a URL or from a file in the server.

The link must start with http://. The reference files can have the following extensions: html, txt, csv, pdf, doc, docx, xls, xlsx, and have to be stored in the location:

- \NMSROOT\htdocs\config-templates-help (On Windows)
- \NMSROOT\htdocs\config-templates-help (On Solaris and Soft Appliance)

\NMSROOT is the LMS install directory. For Solaris and Soft Appliance, it will be /opt/CSCOpx.

You can also specify tags for your template that can be used as filters for the templates. You can specify multiple tags for a single template, each tag should be comma separated.

To edit a template:

---

**Step 1** Select **Configuration > Tools > Template Center > Manage**.

The Manage Templates page appears, displaying the Template Selector pane.

**Table 3-3** describes the Template Selector pane.

---

**Step 2** Select the template that you need to edit and click **Edit**.

The Edit Template page appears.

---

**Step 3** You can edit the Reference link.

**Step 4** You can edit the Tag.

---

**Step 5** Edit the default values of the template and click **Save**.

You can create a new template from an existing template (system or user-defined) and click **Save As** to save it as user-defined template.

You can edit a Cisco Best Practices Template and click **Save As** to save the template as a new template.

The Template Management page appears, displaying the Template with edited values.
Deleting Templates

You can use the Delete option to remove an existing template from the Template Selector pane.

Note
You cannot delete a system-defined template from the Template Selector pane.

To delete an existing template:

Step 1
Select Configuration > Tools > Template Center > Manage.
The Manage Templates page appears, displaying the Template Selector pane.
Table 3-3 describes the Template Selector pane.

Step 2
Select an existing user-defined template from the Template Selector pane.

Step 3
Click Delete.
The selected user-defined template is deleted from the Template Selector pane.

Exporting Templates

You can use the Export option to export an existing template to a remote or a client machine. The template exported will be in XML format.

To export an existing template:

Step 1
Select Configuration > Tools > Template Center > Manage.
The Manage Templates page appears, displaying the Template Selector pane.
Table 3-3 describes the Template Selector pane.

Step 2
Select an existing template from the Template Selector pane.

Step 3
Click Export.
A dialog box appears, prompting you to open or save the template XML file.
Handing Multi-line Commands

In LMS 4.2, you can enter multi-line commands like, banner and crypto certificate commands, as a part of the templates in Template Center. The multi-line commands must be within the tag <MLTCMD> and </MLTCMD>. The commands within the MLTCMD tags are considered as a single command and will be downloaded as a single command onto the device.

These tags are case-sensitive and you must enter them only in uppercase. You cannot start this tag with a space. You can have a blank line within a multi-line command.

Example 1

<MLTCMD> banner login "Welcome to Cisco Prime LMS - you are using Multi-line commands" </MLTCMD>

Example 2

cmd1<MLTCMD>cmd2
cmd3
cmd4
cmd5</MLTCMD>cmd6

In Example 1 and 2, cmd1,cmd2,cmd3,cmd4,cmd5 and cmd6 are all commands and will be deployed to the device as a single command.

Viewing Template Details

You can use the View Template option to view the details of an existing template from the Template Selector pane.

To view the details of an existing template:

Step 1 Select Configuration > Tools > Template Center > Manage.

The Manage Templates page appears, displaying the Template Selector pane.

Step 2 Select an existing template from the Template Selector pane.

Step 3 Click View.

A pop-up window appears, you can view the selected template as XML.
Importing Templates

LMS allows you to create a user-defined configuration template by importing:

- Configuration commands from an existing template (.xml file) stored on a client machine (See Importing from XML File)
- A text file generated using Cisco Configuration Professional tool stored on a client machine (See Importing from a Cisco Configuration Professional File)
- A running configuration from a device (See Importing Running Config from Device)

You can also create a new template file (.xml) using the guideline specified in the XML schema. See Config Template XML Schema for information.

You can also download config templates from Cisco.com from the URL:

**Note** When you import a template with a name that is already used by another template in LMS, a message appears prompting you to overwrite the template (user-defined) in LMS. System-defined templates cannot be overwritten.

### Importing from XML File

To import a template from XML file:

**Step 1** Select Configuration > Tools > Template Center > Import.

The Import Templates page appears, displaying Choose Import Mode pane.

**Step 2** Select Config Template from Choose Source Type option.

**Step 3** Click Browse to select the configuration file (.xml file) stored on a client machine.

Before you import a template, you must ensure that the values of each field do not exceed the respective character limitation. The details are given in the table below.

If the values of each field exceed the character limitation, you will not be able to import the template.

<table>
<thead>
<tr>
<th>Field</th>
<th>Maximum Number of Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>64</td>
</tr>
<tr>
<td>Author</td>
<td>64</td>
</tr>
<tr>
<td>Description</td>
<td>1024</td>
</tr>
<tr>
<td>Template Version</td>
<td>64</td>
</tr>
<tr>
<td>Task</td>
<td>64</td>
</tr>
<tr>
<td>Scope</td>
<td>64</td>
</tr>
<tr>
<td>Template Type</td>
<td>64</td>
</tr>
<tr>
<td>Features</td>
<td>255</td>
</tr>
</tbody>
</table>
Chapter 3      Managing and Deploying Templates

Importing Templates

### Importing Templates

<table>
<thead>
<tr>
<th>Field</th>
<th>Maximum Number of Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Platform</td>
<td>600</td>
</tr>
<tr>
<td>PIN</td>
<td>64</td>
</tr>
<tr>
<td>Reference Text</td>
<td>100</td>
</tr>
<tr>
<td>Reference URL</td>
<td>100</td>
</tr>
<tr>
<td>Reference Type</td>
<td>10</td>
</tr>
<tr>
<td>Tags</td>
<td>1024</td>
</tr>
</tbody>
</table>

**Step 4**  Click **Finish**.

A message appears stating that the template has been imported successfully.

### Importing from a Cisco Configuration Professional File

To import a template from a Cisco Configuration Professional file:

**Step 1**  Select **Configuration > Tools > Template Center > Import**.

The Import Templates page appears, displaying Choose Import Mode pane.

**Step 2**  Select **CCP Config** from Choose Source Type option.

**Step 3**  Click **Browse** to select the Cisco Configuration Professional file (.txt format) stored on a client machine.

**Step 4**  Click **Next**.

The View and Edit Configuration pane appears, displaying the configuration commands in the text box.

You can edit these configuration commands. You must ensure that the configuration commands are valid because LMS does not validate these commands.

**Step 5**  Click **Next**.

The Choose Device Types pane appears.

You need to:

- Choose the image platform for applying the imported configuration from the drop-down list.
- Enter the minimum supported image version for the image platform.
- Choose the device groups for applying the configuration.

**Step 6**  Click **Next**.

The Choose Conflicting Tags pane appears, displaying the List of Conflicting Features dialog box.

Here, you need to add the list of conflicting features in a file and add it in the Import Template flow. This is optional.

A feature in the template might conflict with a feature of another template. In this case, if you have selected templates that have feature conflicts with each other, then deploy flow will not proceed, and a warning message is shown.
For example,

In the Template Center, you have the following two templates:

- Template A—Deploys Auto Smartport feature and the conflicting feature is CDP
- Template B—Deploys CDP feature

If you have selected both Template A and Template B in the Deploy Template flow, the conflicting feature CDP of Template A with the CDP feature of Template B creates a conflict and this will prevent the Deploy Template job flow to proceed, and a warning message is displayed.

In this case, you have to select templates that do not have feature conflicts with each other and then proceed with the deploy flow.

Table 3-5 describes the fields in the List of Conflicting Features dialog box.

**Table 3-5  List of Conflicting Features**

<table>
<thead>
<tr>
<th>Column/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Name of the conflicting feature.</td>
</tr>
<tr>
<td>Warning Message</td>
<td>Warning message displayed if the conflicting feature exists</td>
</tr>
<tr>
<td>Configuration</td>
<td>Shows the configuration commands of the conflicting feature</td>
</tr>
<tr>
<td>Delete (Button)</td>
<td>Delete the conflicting feature file.</td>
</tr>
<tr>
<td>Add (Button)</td>
<td>Create a conflicting feature file.</td>
</tr>
<tr>
<td>Edit (Button)</td>
<td>Modify an existing conflicting feature file.</td>
</tr>
</tbody>
</table>

**Step 7**  Click Next.

The Enter Template Details pane appears, allowing you to enter the template details described in table.

Table 3-6 describes the fields in Enter Template Details pane.

**Table 3-6  Enter Template Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>Enter a valid name for the template. Ensure the template name you enter is unique.</td>
</tr>
<tr>
<td>Note</td>
<td>When you import a template with a name that is already used by another template in LMS, a message appears prompting you to overwrite the template (user-defined) in LMS. System-defined templates cannot be overwritten.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide a description of the template. You can enter a maximum of 1024 characters.</td>
</tr>
<tr>
<td>Task</td>
<td>Enter the task description of the template. You can enter a maximum of 64 characters.</td>
</tr>
</tbody>
</table>
Importing Running Config from Device

To import a running config as a template from a device:

Step 1 Select Configuration > Tools > Template Center > Import.

The Import Templates page appears, displaying Choose Import Mode pane.

Step 2 Select Running Config from Device from Choose Source Type option.

Step 3 Select a device from the Device Selector.

Step 4 Click Next.

The View and Edit Configuration pane appears, displaying the configuration commands in the text box. You can edit these configuration commands. You must ensure that the configuration commands are valid because LMS does not do any validation on these commands.

Step 5 Click Next.

The Choose Device Types pane appears.

You need to:
- Choose the applicable image platform from the drop-down list.
- Enter the minimum supported image version for the image platform.
- Select the applicable device categories from the Device Type Selector.

Step 6 Click Next.

The Choose Conflicting Tags pane appears, displaying the List of Conflicting Features dialog box. Table 3-5 describes the fields in the List of Conflicting Features dialog box.

Table 3-6 Enter Template Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Enter the version of the template.</td>
</tr>
<tr>
<td></td>
<td>You can enter a maximum of 64 characters.</td>
</tr>
<tr>
<td>Scope</td>
<td>Choose the scope of the template. For example, device, port, or module.</td>
</tr>
<tr>
<td>Feature</td>
<td>Enter the template feature.</td>
</tr>
<tr>
<td></td>
<td>You can enter a maximum of 255 characters.</td>
</tr>
<tr>
<td>Hardware Platform</td>
<td>Enter the applicable hardware platform for the template.</td>
</tr>
<tr>
<td></td>
<td>You can enter a maximum of 600 characters.</td>
</tr>
<tr>
<td>PIN</td>
<td>Choose the PIN (place of the device in the network) for the template.</td>
</tr>
<tr>
<td></td>
<td>For example, edge.</td>
</tr>
<tr>
<td>Image Feature</td>
<td>Enter the image feature for the template.</td>
</tr>
<tr>
<td>Type</td>
<td>Choose the type of the template (Complete, Partial)</td>
</tr>
</tbody>
</table>

Step 8 Click Finish.

A message appears stating that the template has been created successfully.
Assigning Templates to Users

You can assign templates to users with Network Operator and Network Administrator privileges. A network administrator must assign template access privileges to other users.

To assign templates to users:

Step 1 Select Configuration > Tools > Template Center > Assign Template to User. The Assign Templates to Users page appears, displaying the Assign Templates dialog box.

Step 2 Enter the username of the user to whom you want to assign the templates. This should be a valid LMS user.

Step 3 Select the template that you want to allocate to the user from the Available templates list box and click Add.

You can select more than one template, by holding down the Shift key while selecting the template. The selected templates appear in the Selected Templates list box.

To remove assigned templates, select the templates from the Selected Templates list box and click Remove.

Step 4 Add all the required Templates to the Selected Templates list box.

Note View the Permission Report (Reports > System > Users > Permission) to check whether you have the required privileges to perform this task.
Step 5  Click **Assign** to assign the template access privileges to the specified user.

For a specified user, to see the assigned templates, enter the username in the Username field and click **Show Assigned**.

The templates assigned to the user appear in the Selected Templates list box.

Step 6  Click **Report** to generate the User Template Report.

The User Template Report shows the list of users and the templates assigned for each user.

**Note**  By default, all the templates are assigned to admin users. Therefore, the User Template Report will not list the users with Admin privileges.

---

# Understanding the Template Center Jobs Browser

You can browse the template deployment jobs registered on the system. Using the Template Center Jobs, you can manage template jobs. That is, you can stop, delete, refresh, or filter jobs using this job browser. You can also view the template job details such as work order, device details, job summary.

**Note**  View Permission Report (**Reports > System > Users > Permission**) to check whether you have the required privileges to perform this task.

Select either:

**Configuration > Tools > Template Center > Jobs.**

Or

**Configuration > Job Browsers > Template Center**

The Template Center Jobs page appears, displaying the List of Template Deployment Jobs pane and Job Details pane for a job.

**Table 3-7** describes the List of Template Jobs pane in the Template Center Jobs.
## Understanding the Template Center Jobs Browser

### Table 3-7 List of Template Center Jobs

<table>
<thead>
<tr>
<th>Column/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job ID</strong></td>
<td>Unique number assigned to a template job when it is created. For periodic jobs such as Daily, Weekly, the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the Job ID 1001.</td>
</tr>
</tbody>
</table>
| **Status**    | Status of the job:  
  • Successful—When the job is successful.  
  • Failed—When the job has failed.  
    The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed.  
    For example, if the status displays Failed(5), then the count of devices that had failed amounts to 5.  
  • Stopped—When the job has been stopped.  
  • Running—When the job is in progress.  
  • Waiting—When the job is awaiting approval (if job approval has been enabled).  
  • Rejected—When the job has been rejected (if job approval has been enabled). |
| **Owner**     | User who created the job. |
| **Scheduled at** | Date and time at which the job was scheduled. |
| **Completed at** | Date and time at which the job was completed. |
| **Schedule Type** | Type of job schedule—Immediate, Once, Daily, Weekly, Monthly. For periodic jobs, the subsequent instances will run only after the earlier instance of the job is complete. |
| **Stop (button)** | Stop or cancel a running job. |
| **Delete (button)** | Deletes the selected job from the Template Center Jobs. You can select more than one job to delete. |
| **Refresh Job (button)** | Select a Job and click Refresh Job.  
  The Job Details pane gets refreshed showing the latest status of the job. |
Table 3-7  List of Template Center Jobs

<table>
<thead>
<tr>
<th>Column/Button (button)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Click Filter and select a Filter By criteria from the drop-down list and enter the details in the Equals field. The following Filter By options are available:</td>
<td></td>
</tr>
<tr>
<td>Job ID—Select Job ID and enter the Job ID number.</td>
<td></td>
</tr>
<tr>
<td>Status—Select Status and enter the status (Successful, Failed, Cancelled, Running, Waiting, Rejected).</td>
<td></td>
</tr>
<tr>
<td>Description—Select Description and enter the complete name.</td>
<td></td>
</tr>
<tr>
<td>Owner—Select Owner and enter the user name.</td>
<td></td>
</tr>
<tr>
<td>Scheduled at—Select Scheduled at and enter the schedule time details.</td>
<td></td>
</tr>
<tr>
<td>Completed at—Select Completed at and enter the completed time details.</td>
<td></td>
</tr>
<tr>
<td>Schedule Type—Select Schedule Type and enter the type (Immediate, Once, Daily, Weekly, Monthly)</td>
<td></td>
</tr>
<tr>
<td>Refresh Click to refresh the List of Template Jobs table.</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-8 describes the Job Details pane in the Template Center Jobs.

Table 3-8  Template Deployment Job Details

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Order Shows the work order details for the selected job.</td>
<td></td>
</tr>
<tr>
<td>General Info The General Info in the work order displays the following details:</td>
<td></td>
</tr>
<tr>
<td>Description—Job description entered at the time of job creation.</td>
<td></td>
</tr>
<tr>
<td>Owner—User who created the job.</td>
<td></td>
</tr>
<tr>
<td>Schedule Type—Type of job schedule (Immediate, Once, Daily, Weekly, Monthly).</td>
<td></td>
</tr>
<tr>
<td>Schedule Time—Time at which the job was scheduled to run. The Schedule Time is applicable for periodic jobs and not for Immediate jobs.</td>
<td></td>
</tr>
<tr>
<td>Job Policies The Job Policies in the work order displays the following details:</td>
<td></td>
</tr>
<tr>
<td>E-mail Notification—E-mail notification status (Enabled/Disabled)</td>
<td></td>
</tr>
<tr>
<td>E-mail Ids—E-mail IDs registered for e-mail notification</td>
<td></td>
</tr>
<tr>
<td>Execution Policy—Job Execution policy as Parallel</td>
<td></td>
</tr>
<tr>
<td>Copy Startup to Running Config upon failure—Displays the status (Enabled/Disabled)</td>
<td></td>
</tr>
<tr>
<td>Job Password—Login Password for the job.</td>
<td></td>
</tr>
<tr>
<td>Job UserName—Login Username for the job.</td>
<td></td>
</tr>
</tbody>
</table>
### Understanding the Template Center Jobs Browser

#### Device and Template Details
- Device Template Details
- Devices List
- Port Template Details
- Port Group Details
- Module Template Details
- Module Details

#### Device Details
- Shows the list of devices added in the Template Deployment job.

#### Device
- Shows the device name.

#### Status
- Status of the device (Success, Failure).

#### Message Summary
- Shows the device status summary.

#### Show Details
- Select the device name and click **Show Details**. A pop-up window appears, displaying the following details for the device:
  - Device Name—Name of the device.
  - Device Status—Status of the device (Success, Failure).
  - Protocol—Protocol details running on the device.
  - Summary—Shows the device status summary.
  - CLI Output—Shows the CLI output.

#### Filter
- Click **Filter**. Select a Filter By criteria from the drop-down list and enter the details in the Equals field. Click **Go** to filter details.

The following Filter By options are available:
- Device—Select **Device** and enter the first few letters or the complete name of the device.
- Status—Select **Status** and enter the status (Success, Failure)
- Message Summary—Select **Message Summary** and enter the first few letters of the message summary.

### Table 3-8  Template Deployment Job Details

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device and Template Details</td>
<td>Shows the following Device and Template details of the job:</td>
</tr>
<tr>
<td></td>
<td>• Device Template Details</td>
</tr>
<tr>
<td></td>
<td>• Devices List</td>
</tr>
<tr>
<td></td>
<td>• Port Template Details</td>
</tr>
<tr>
<td></td>
<td>• Port Group Details</td>
</tr>
<tr>
<td></td>
<td>• Module Template Details</td>
</tr>
<tr>
<td></td>
<td>• Module Details</td>
</tr>
<tr>
<td>Device Details</td>
<td>Shows the list of devices added in the Template Deployment job.</td>
</tr>
<tr>
<td>Device</td>
<td>Shows the device name.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the device (Success, Failure).</td>
</tr>
<tr>
<td>Message Summary</td>
<td>Shows the device status summary.</td>
</tr>
<tr>
<td>Show Details</td>
<td>Select the device name and click <strong>Show Details</strong>. A pop-up window appears,</td>
</tr>
<tr>
<td></td>
<td>displaying the following details for the device:</td>
</tr>
<tr>
<td></td>
<td>• Device Name—Name of the device.</td>
</tr>
<tr>
<td></td>
<td>• Device Status—Status of the device (Success, Failure).</td>
</tr>
<tr>
<td></td>
<td>• Protocol—Protocol details running on the device.</td>
</tr>
<tr>
<td></td>
<td>• Summary—Shows the device status summary.</td>
</tr>
<tr>
<td></td>
<td>• CLI Output—Shows the CLI output.</td>
</tr>
<tr>
<td>Filter</td>
<td>Click <strong>Filter</strong>. Select a Filter By criteria from the drop-down list and</td>
</tr>
<tr>
<td></td>
<td>enter the details in the Equals field. Click <strong>Go</strong> to filter details.</td>
</tr>
<tr>
<td></td>
<td>The following Filter By options are available:</td>
</tr>
<tr>
<td></td>
<td>• Device—Select <strong>Device</strong> and enter the first few letters or the complete</td>
</tr>
<tr>
<td></td>
<td>name of the device.</td>
</tr>
<tr>
<td></td>
<td>• Status—Select <strong>Status</strong> and enter the status (Success, Failure)</td>
</tr>
<tr>
<td></td>
<td>• Message Summary—Select <strong>Message Summary</strong> and enter the first few letters</td>
</tr>
<tr>
<td></td>
<td>of the message summary.</td>
</tr>
</tbody>
</table>
Guidelines for Creating Configuration Templates Using IF and FOREACH Statements

The following are the guidelines that have to be followed while creating configuration templates:

- Parameter can be specified in two ways:
  - `${vlan-id}` - This is how parameters are specified in the old templates. The same can be used in LMS 4.2.
  - `$vlan-id` - Recommended from LMS 4.2.
- Parameter name should not start with number. For example, it should not be `$[123vlan-id]`. The correct way of representing it is `$[vlan-id]`.
- Parameter name and other special characters (, or and etc) / commands should be separated by space. For example, interface range `${interfaceType} ${port1} , ${interfaceType} ${port2}`

### Table 3-8 Template Deployment Job Details

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Summary</td>
<td>Shows the job summary details for the selected job.</td>
</tr>
<tr>
<td>General Info</td>
<td>The General Info in the job summary shows the following details:</td>
</tr>
<tr>
<td></td>
<td>• Status—Status of the device at the time of job creation.</td>
</tr>
<tr>
<td></td>
<td>• Start Time—Start time of the job.</td>
</tr>
<tr>
<td></td>
<td>• End Time—End time of the job.</td>
</tr>
<tr>
<td>Job Messages</td>
<td>Shows the following job messages:</td>
</tr>
<tr>
<td></td>
<td>• Pre-job Execution</td>
</tr>
<tr>
<td></td>
<td>• Post-job Execution</td>
</tr>
<tr>
<td>Device Updates</td>
<td>Shows the following update on the devices in the job:</td>
</tr>
<tr>
<td></td>
<td>• Successful</td>
</tr>
<tr>
<td></td>
<td>• Failed</td>
</tr>
<tr>
<td></td>
<td>• Not Attempted</td>
</tr>
<tr>
<td></td>
<td>• Pending</td>
</tr>
</tbody>
</table>

Guidelines for Creating Configuration Templates Using IF and FOREACH Statements

The following are the guidelines that have to be followed while creating configuration templates:

- Parameter can be specified in two ways:
  - `${vlan-id}` - This is how parameters are specified in the old templates. The same can be used in LMS 4.2.
  - `$vlan-id` - Recommended from LMS 4.2.
- Parameter name should not start with number. For example, it should not be `$[123vlan-id]`. The correct way of representing it is `$[vlan-id]`.
- Parameter name and other special characters (, or and etc) / commands should be separated by space. For example, interface range `${interfaceType} ${port1} , ${interfaceType} ${port2}`
Guidelines for Creating Configuration Templates Using IF and FOREACH Statements

Chapter 3      Managing and Deploying Templates

Syntax/Example for IF

The following show the syntax/example of If / if – else / nested – if statement:

```
#if( $option == "heterogeneous" )
  dspfarm profile $PROFILE_ID conference video heterogeneous
#endif
#else
  dspfarm profile $PROFILE_ID conference video homogeneous
#endif
```

See Sample Template for IF Statement for more details.

Table 3-9 lists the relational and logical operators used in If / if - else / nested - if statement. You can use short version or text version while creating templates.

### Table 3-9 Relational and Logical Operators

<table>
<thead>
<tr>
<th>Type of operator</th>
<th>short version</th>
<th>text version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equal</td>
<td>==</td>
<td>eq</td>
</tr>
<tr>
<td>not equal</td>
<td>!=</td>
<td>ne</td>
</tr>
<tr>
<td>greater than</td>
<td>&gt;</td>
<td>gt</td>
</tr>
<tr>
<td>greater or equal than</td>
<td>&gt;=</td>
<td>ge</td>
</tr>
<tr>
<td>less than</td>
<td>&lt;</td>
<td>lt</td>
</tr>
<tr>
<td>less or equal than</td>
<td>&lt;=</td>
<td>le</td>
</tr>
<tr>
<td>logical and</td>
<td>&amp;&amp;</td>
<td>and</td>
</tr>
<tr>
<td>logical or</td>
<td></td>
<td></td>
</tr>
<tr>
<td>logical not</td>
<td>!</td>
<td>not</td>
</tr>
</tbody>
</table>

Example

```
## logical AND
#if( $foo && $bar )
  dspfarm profile $PROFILE_ID
#endif
## logical OR
#if( $foo || $bar )
  dspfarm profile $PROFILE_ID
#endif
##logical NOT
#if( !$foo )
  dspfarm profile $PROFILE_ID
#endif
```
Syntax/Example for FOREACH

The following show the syntax/example of foreach:

```yaml
#foreach( $product in $allProducts )
  this is the for loop for $product
#end
```

This #foreach loop causes the $allProducts list to be looped over for all of the products in the list. Each time through the loop, the value from $allProducts is placed into the $product variable.

XML Specification for Template

The following are the xml specification for template:

- Textarea / Textbox component can be used
- Data type should be specified as list

Example

```xml
<parameter name="allProducts">
  <description>Enter the product ids separated by comma [A,B,C]</description>
  <html-component>textarea</html-component>
  <data-type>list</data-type>
  <mandatory>true</mandatory>
  <isGlobal>true</isGlobal>
  <help-description>Enter the product IDs</help-description>
  <syntax/>
  <min/>
  <max/>
  <pattern/>
</parameter>
```

You cannot enter special characters such as < and &&, as the parser interprets it as the start of a new element and character entity.

There are two ways where you can use special character such as < and &&:

- Parser ignores the special characters if you enter it within CDATA section. A CDATA section starts with "<![CDATA[“ and ends with ”]]>". See Example 1.
- Use "and" instead of "&&" and "lt" instead of ". See Example 2.

Example 1

```xml
<![CDATA[
  sccp ccm group ${UCM_GROUP_ID}
  #foreach ( ${PROFILE_ID} in $ALL-PROFILE_ID )
    this is the for loop for $PROFILE_ID
    #if (${PROFILE_ID} == "vas" && ${UCM_GROUP_ID} == "vvv")
      PROFILE_ID is vas
    #else
      wrong PROFILE_ID : ${PROFILE_ID}
    #end
  #end
```
Note

Nested CDATA sections are not allowed. The CDATA closing tag "]]>" should not have spaces or line breaks.

Example 2

```plaintext
#if (${interfaceType} and "FastEthernet")
interface range ${interfaceType} ${port1}, ${interfaceType} ${port2}
#end

#if (${interfaceType} lt "FastEthernet")
interface range ${interfaceType} ${port1}, ${interfaceType} ${port2}
#end
```
Using Compliance and Audit Manager Feature

This chapter provides information about how to manage Policy Groups, Policy Profiles and check network devices for compliance against selected compliance rules and user defined policy.

This chapter contains the following:

- Managing Policy Groups
- Managing Policy Profile
- Fixing Profile Violations
- Understanding Compliance Violation Fix Job Browser
- Understanding Compliance and Audit Manager (CAAM) Policies
- Data Synchronization between LMS and CAAM
- Compliance Management License
- Compliance and Audit Reports

Managing Policy Groups

Policy Group is a collection of Policies. Policies are defined by a set of rules. LMS supports 293 policies. In addition to the system defined Policy Groups, you can create your own Policy Groups by selecting a set of system defined policies.

This section details:

- Adding Policy Groups
- Cloning Policy Groups
- Editing Policy Groups
- Deleting User-Defined Policy Groups
- Deleting a Policy from User-Defined Policy Group
- Understanding Compliance and Audit Manager (CAAM) Policies

Adding Policy Groups

This section details:
• Adding New Policy Group by Selecting Policies from Existing System-Defined Policy Group
• Adding a New Policy Group by Adding New Policies
Adding New Policy Group by Selecting Policies from Existing System-Defined Policy Group

To add a new Policy Group from existing System-Defined Policy Group:

**Step 1**
Select Configuration > Compliance > Compliance and Audit Manager > Compliance Policies and Groups.
The Compliance Policies and Groups page appears.

**Step 2**
Select the required System Policy Group from the tree view.
The list of policies associated with the selected Policy Group appears in the Policies and Rules pane.

**Step 3**
Select a policy for which you want to modify the rules.
The rules corresponding to the selected policy appears.

**Step 4**
Edit the rules.

**Step 5**
Repeat Step 3 and Step 4 if you want to modify the rules associated with other policies listed in Policies and Rules pane.

**Step 6**
Click Add to add new policies to the group.
The Policy Selector appears.

**Step 7**
Select the required policies and click Select.
The selected policies will be added to the Policies and Rules pane. To return to Compliance Policies and Groups page, click Cancel.

**Step 8**
Select the newly added policy for which you want to modify the rules. The rules corresponding to the selected policy appears.

**Step 9**
Edit the rules.

**Step 10**
Click Save As to save as a new Policy Group.
A Create Group pop-up appears.

**Step 11**
Enter the name of the new Policy Group.

**Step 12**
Enter the description of the Policy Group.

**Step 13**
Click Save to save the newly created Policy Group. To return to Compliance Policies and Groups page, click Cancel.
The newly created Policy Group will be listed under My Policy Groups.

Related Topics
- Adding a New Policy Group by Adding New Policies
- Editing Policy Groups
- Deleting User-Defined Policy Groups
- Deleting a Policy from User-Defined Policy Group
- Understanding Compliance and Audit Manager (CAAM) Policies

Adding a New Policy Group by Adding New Policies

To add a new Policy Group:
Step 1  Select Configuration > Compliance > Compliance and Audit Manager > Compliance Policies and Groups.

The Compliance Policies and Groups page appears.

Step 2  Click the icon in the Policy Group Selector section.

Step 3  Click Add Policy Group.

Step 4  Enter the name of the new Policy Group.

Step 5  Enter the description of the Policy Group.

Step 6  Click Add in the policies and rules pane, to add new policies to the group.

The Policy Selector appears. See Table 4-1 for the list of policies grouped under each policy group.

Step 7  Select the required policies and click Select.

The selected policies will be added to the Policies and Rules pane. To return to the Compliance Policies and Groups page, click Cancel.

Step 8  Select the newly added policy for which you want to modify the rules.

The rules corresponding to the selected policy appears.

Step 9  Set values for each rule.

Step 10 Click Save to save the new Policy Group.

The newly created Policy Group will be listed under My Policy Groups.

<table>
<thead>
<tr>
<th>Policy Group Name</th>
<th>Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>ACL on Interfaces</td>
</tr>
<tr>
<td></td>
<td>Distributed DoS Attacks</td>
</tr>
<tr>
<td></td>
<td>Land Attack</td>
</tr>
<tr>
<td></td>
<td>Martian Traffic</td>
</tr>
<tr>
<td></td>
<td>Null (Black Hole) Routing</td>
</tr>
<tr>
<td></td>
<td>Risky Traffic</td>
</tr>
<tr>
<td></td>
<td>SMURF Attack</td>
</tr>
<tr>
<td></td>
<td>Traffic Rules</td>
</tr>
</tbody>
</table>
## Table 4-1  Policy Group Details

<table>
<thead>
<tr>
<th>Policy Group Name</th>
<th>Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Protocols</td>
<td>Control Plane Policing</td>
</tr>
<tr>
<td></td>
<td>HTTP Server</td>
</tr>
<tr>
<td></td>
<td>Hot Standby Router Protocol (HSRP)</td>
</tr>
<tr>
<td></td>
<td>ICMP</td>
</tr>
<tr>
<td></td>
<td>Miscellaneous Services</td>
</tr>
<tr>
<td></td>
<td>Routing and Forwarding</td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
</tr>
<tr>
<td></td>
<td>SSH Parameters</td>
</tr>
<tr>
<td></td>
<td>TCP Parameters</td>
</tr>
<tr>
<td>Switching</td>
<td>DHCP Snooping</td>
</tr>
<tr>
<td></td>
<td>Dynamic Trunking Protocol (DTP)</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.1X Port-Based Authentication</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.3 Flow Control</td>
</tr>
<tr>
<td></td>
<td>IP Phone Ports</td>
</tr>
<tr>
<td></td>
<td>Management VLAN</td>
</tr>
<tr>
<td></td>
<td>Port Security</td>
</tr>
<tr>
<td></td>
<td>Spanning Tree Protocol (STP)</td>
</tr>
<tr>
<td></td>
<td>Unidirectional Link Detection (UDLD)</td>
</tr>
<tr>
<td></td>
<td>Unused Ports</td>
</tr>
<tr>
<td></td>
<td>VLAN1</td>
</tr>
<tr>
<td></td>
<td>VLAN Trunking Protocol (VTP)</td>
</tr>
<tr>
<td>Global Configuration</td>
<td>ACLs</td>
</tr>
<tr>
<td></td>
<td>CDP</td>
</tr>
<tr>
<td></td>
<td>Clock</td>
</tr>
<tr>
<td></td>
<td>FTP</td>
</tr>
<tr>
<td></td>
<td>Miscellaneous Services On Firewalls</td>
</tr>
<tr>
<td></td>
<td>NTP Configuration</td>
</tr>
<tr>
<td></td>
<td>Traceroute</td>
</tr>
<tr>
<td>Others</td>
<td>Device Version Checks</td>
</tr>
<tr>
<td></td>
<td>Device Running outdated OS Versions</td>
</tr>
<tr>
<td></td>
<td>Devices with outdated modules</td>
</tr>
<tr>
<td></td>
<td>Outdated Devices As Per Vendor Specific</td>
</tr>
<tr>
<td></td>
<td>EOL/EOS Announcements</td>
</tr>
</tbody>
</table>
Table 4-1  Policy Group Details

<table>
<thead>
<tr>
<th>Policy Group Name</th>
<th>Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Protocols</td>
<td>BGP</td>
</tr>
<tr>
<td></td>
<td>EIGRP</td>
</tr>
<tr>
<td></td>
<td>OSPF</td>
</tr>
<tr>
<td></td>
<td>RIP</td>
</tr>
<tr>
<td>Cisco Security Advisories (PSIRT)</td>
<td>For PSIRT policies see Cisco Security Advisory (PSIRT).</td>
</tr>
<tr>
<td>Network Access Services</td>
<td>Loopback Interfaces</td>
</tr>
<tr>
<td></td>
<td>Remote Commands</td>
</tr>
<tr>
<td>Audit and Management</td>
<td>Banners</td>
</tr>
<tr>
<td></td>
<td>Console Access</td>
</tr>
<tr>
<td></td>
<td>DHCP</td>
</tr>
<tr>
<td></td>
<td>Domain Name</td>
</tr>
<tr>
<td></td>
<td>Host Name</td>
</tr>
<tr>
<td></td>
<td>Logging and Syslog</td>
</tr>
<tr>
<td></td>
<td>Terminal Access</td>
</tr>
<tr>
<td></td>
<td>User Passwords</td>
</tr>
<tr>
<td>AAA Services</td>
<td>AAA</td>
</tr>
<tr>
<td></td>
<td>AAA Accounting - Commands</td>
</tr>
<tr>
<td></td>
<td>AAA Accounting - Connections</td>
</tr>
<tr>
<td></td>
<td>AAA Accounting - Exec</td>
</tr>
<tr>
<td></td>
<td>AAA Accounting - Network</td>
</tr>
<tr>
<td></td>
<td>AAA Accounting - System</td>
</tr>
<tr>
<td></td>
<td>AAA Authentication - Enable</td>
</tr>
<tr>
<td></td>
<td>AAA Authentication - Login</td>
</tr>
<tr>
<td></td>
<td>AAA Authorization - Configuration</td>
</tr>
<tr>
<td></td>
<td>AAA Authorization - Exec</td>
</tr>
<tr>
<td></td>
<td>AAA Authorization - Network</td>
</tr>
</tbody>
</table>

Related Topics
- Adding New Policy Group by Selecting Policies from Existing System-Defined Policy Group
- Editing Policy Groups
- Deleting User-Defined Policy Groups
- Deleting a Policy from User-Defined Policy Group
- Understanding Compliance and Audit Manager (CAAM) Policies
Cloning Policy Groups

To clone a Policy Group:

**Step 1** Select Configuration > Compliance > Compliance and Audit Manager > Compliance Policies and Groups.

The Compliance Policies and Groups page appears.

**Step 2** Mouse-hover on the System or My Policy Groups and then mouse-hover on the quick view picker icon next to System or My Policy Groups.

The policy details such as Group Name, Description and Policy Count appear in the mouse-hover pop-up window. You can also clone or delete groups.

*Note* You cannot delete stem defined Policy groups.

**Step 3** Click Clone Group in the mouse-hover pop-up window to create a copy of the selected Policy Group.

**Step 4** Enter the name of the Policy Group.

**Step 5** Enter the description of the Policy Group.

**Step 6** Click Save to save the Policy Group.

The copy of the selected Policy Group will be listed under My Policy Groups.

Related Topics

- Adding Policy Groups
- Editing Policy Groups
- Deleting User-Defined Policy Groups
- Deleting a Policy from User-Defined Policy Group
- Understanding Compliance and Audit Manager (CAAM) Policies

Editing Policy Groups

To edit a Policy Group:

**Step 1** Select Configuration > Compliance > Compliance and Audit Manager > Compliance Policies and Groups.

The Compliance Policies and Groups page appears.

**Step 2** Select the required System or My Policy Groups from the tree view.

The list of policies associated with the selected Policy Group appears in the Policies and Rules pane.

**Step 3** Select a policy for which you want to modify the rules.

The rules corresponding to the selected policy appears.

**Step 4** Edit the rules.
Step 5Repeat Step 3 and Step 4 if you want to modify the rules associated with other policies listed in Policies and Rules pane.

Step 6Click **Add** to add new policies to the group.

The Policy Selector appears.

To delete a policy, select a policy and click **Delete**.

Step 7Select the required policies and click **Select**.

The selected policies will be listed in the Policies and Rules pane. To return to Compliance Policies and Groups page, click **Cancel**.

Step 8Select the newly added policy for which you want to modify the rules. The rules corresponding to the selected policy appears.

Step 9Edit the rules.

Step 10Do one of the following:

- Click **Save** to save the changes made in the selected My Policy Group.

  **Note** You cannot edit and save the System Policy Group. Hence, Save option will be disabled for System Policy Group.

  Or

- Click **Save As** to save it as a new My Policy Groups and follow Step 11.

Step 11Enter the name of the new Policy Group.

Step 12Enter the description of the Policy Group.

Step 13Click **Save** to save the new Policy Group. To return to Compliance Policies and Groups page, click **Cancel**.

The newly created Policy Group will be listed under My Policy Groups.

**Related Topics**

- Adding Policy Groups
- Cloning Policy Groups
- Deleting User-Defined Policy Groups
- Deleting a Policy from User-Defined Policy Group
- Understanding Compliance and Audit Manager (CAAM) Policies

**Deleting User-Defined Policy Groups**

To delete a user-defined Policy Group:

Step 1Select **Configuration > Compliance > Compliance and Audit Manager > Compliance Policies and Groups**.

The Compliance Policies and Groups page appears.
Step 2  Mouse-hover the user-defined Policy Group which you want to delete and then mouse-hover on the quick view picker icon next to the user-defined Policy Group. The policy details appear in the mouse-hover pop-up window.

Step 3  Click Delete Group to delete the selected Policy Group. A warning message appears.

Step 4  Click OK to delete the selected Policy Group. To return to the Compliance Policies and Groups page, click Cancel.

Related Topics
- Adding Policy Groups
- Cloning Policy Groups
- Editing Policy Groups
- Deleting a Policy from User-Defined Policy Group
- Understanding Compliance and Audit Manager (CAAM) Policies

Deleting a Policy from User-Defined Policy Group

To delete a policy from the user-defined Policy Group:

Step 1  Select Configuration > Compliance > Compliance and Audit Manager > Compliance Policies and Groups.

The Compliance Policies and Groups page appears.

Step 2  Select a user-defined Policy Group.

A list of policies associated with the selected Policy Group will be displayed in the Policies and Rules pane.

Step 3  Select a policy and click Delete.

A confirmation message appears.

Step 4  Click OK to delete the selected policy. To return to the Compliance Policies and Groups page, click Cancel.

Related Topics
- Adding Policy Groups
- Cloning Policy Groups
- Editing Policy Groups
- Deleting User-Defined Policy Groups
- Understanding Compliance and Audit Manager (CAAM) Policies
Managing Policy Profile

Policy Profile is a set of Policy Groups where each Policy Groups are mapped with set of devices/device groups.

This section details:
- Adding a New Policy Profile
- Cloning Policy Profiles
- Editing Policy Profile
- Deleting Policy Profiles
- Running Compliance Check
- Viewing Job History

Adding a New Policy Profile

To add a new Policy Profile:

**Step 1** Select Configuration > Compliance > Compliance and Audit Manager > Compliance Profiles and Execution.

The Compliance Policy Profile page appears.

**Step 2** Click the icon in the Policy Profile Selector section.

**Step 3** Click Add Policy Profile.

**Step 4** Enter the name of the new Policy Profile.

**Step 5** Enter the description of the Policy Profile.

**Step 6** Click Add to add new Policy Groups.

The Policy Group Selector appears.

**Step 7** Select the required Policy Group and click Select.

The selected Policy Group and a list of devices will be displayed. To return to Compliance Policy Profile page, click Cancel.

**Step 8** Select a device(s) from the device selector.

**Step 9** Click Save to save the newly created Policy Profile.

Related Topics
- Cloning Policy Profiles
- Editing Policy Profile
- Deleting Policy Profiles
- Running Compliance Check
- Viewing Job History
- Fixing Profile Violations
Cloning Policy Profiles

To clone a Policy Profile:

**Step 1** Select **Configuration > Compliance > Compliance and Audit Manager > Compliance Profiles and Execution**. The Compliance Policy Profile page appears.

**Step 2** Mouse-hover on the Policy Profile and then mouse-hover on the quick view picker icon next to the Policy Profile. The policy details appear in the mouse-hover pop-up window.

**Step 3** Click **Clone Policy Profile** to create a copy of the selected Policy Profile.

**Step 4** Enter a new Policy Profile name.

**Step 5** Enter the description of the Policy Profile.

**Step 6** Click **Save** to save the Policy Profile.

Related Topics
- Adding a New Policy Profile
- Editing Policy Profile
- Deleting Policy Profiles
- Running Compliance Check
- Viewing Job History
- Fixing Profile Violations

Editing Policy Profile

To edit a Policy Profile:

**Step 1** Select **Configuration > Compliance > Compliance and Audit Manager > Compliance Profiles and Execution**. The Compliance Policy Profile page appears.

**Step 2** Select the Policy Profile which you want to edit. The list of policy groups and devices associated with the selected Policy Profile appears in the Policy Group Selection and Device Mapping pane.

**Step 3** Click **Add** to add new policy groups. The Policy Group Selector appears. To delete a Policy Group, select a Policy Group and click **Delete**.

**Step 4** Select the required Policy Groups and click **Select**. The selected Policy Groups will be listed in the Policy Group Selection and Device Mapping pane. To return to Compliance Policy Profile page, click **Cancel**.

**Step 5** Select the device(s) from the device selector.
Step 6  Do one of the following:

- Click **Save** to save the changes made in the selected Policy Profile.
- Or
- Click **Save As** to save it as a new Policy Profile and follow **Step 7**.
Chapter 4      Using Compliance and Audit Manager Feature

Managing Policy Profile

Step 7 Enter the name of the new Policy Profile.
Step 8 Enter the description of the Policy Profile.
Step 9 Click **Save** in the Create Policy Profile pop-up to save the new Policy Profile. To return to Compliance Policy Profile page, click **Cancel**.

The newly created Policy Profile will be listed under tree view.

---

**Related Topics**

- Adding a New Policy Profile
- Deleting Policy Profiles
- Running Compliance Check
- Viewing Job History
- Fixing Profile Violations

### Deleting Policy Profiles

To delete a Policy Profile:

**Step 1** Select **Configuration > Compliance > Compliance and Audit Manager > Compliance Profiles and Execution**.

The Compliance Policy Profile page appears.

**Step 2** Mouse-hover on the Policy Profile and then mouse-hover on the quick view picker icon next to the Policy Profile.

The policy details appear in the mouse-hover pop-up window.

**Step 3** Click **Delete Policy Profile** to delete the selected Policy Profile.

A warning message appears.

**Step 4** Click **OK** to delete the selected Policy Profile. To return to the Compliance Policy Profile page, click **Cancel**.

---

**Related Topics**

- Adding a New Policy Profile
- Cloning Policy Profiles
- Editing Policy Profile
- Running Compliance Check
- Viewing Job History
- Fixing Profile Violations

### Running Compliance Check

To run a compliance check:

---

Configuration Management with Cisco Prime LAN Management Solution 4.2
Managing Policy Profile

Step 1  Select **Configuration > Compliance > Compliance and Audit Manager > Compliance Profiles and Execution**.

The Compliance Policy Profile page appears.

Step 2  Mouse-hover on the Policy Profile and then mouse-hover on the quick view picker icon next to the Policy Profile.

The policy details appear in the mouse-hover pop-up window.

Step 3  Click **Compliance Check**.

The Schedule Compliance window appears.
Step 4  Select one of these scheduling options:
  • Immediate—Runs this task immediately.
  • Once—Runs this task once at the specified date and time.
  • Daily—Runs daily at the specified time.
  • Weekly—Runs weekly on the specified day of the week and at the specified time.
  • Monthly—Runs monthly on the specified day of the month and at the specified time.

Step 5  Enter a description for the job.

Step 6  Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas.

Step 7  Click **Submit**.
A message appears, Job *JobID* is created successfully.

Step 8  Where *JobID* is a unique Job number.

Step 9  Click **OK**.
Compliance Profile Execution Jobs page appears. You can check the status of your scheduled job in this page.

### Related Topics
- Adding a New Policy Profile
- Editing Policy Profile
- Deleting Policy Profiles
- Cloning Policy Profiles
- Viewing Job History
- Fixing Profile Violations

### Viewing Job History
To view the job history:

**Step 1**  Select **Configuration > Compliance > Compliance and Audit Manager > Compliance Profiles and Execution**.
The Compliance Policy Profile page appears.

**Step 2**  Mouse-hover on the Policy Profile and then mouse-hover on the quick view picker icon next to the Policy Profile.
The policy details appear in the mouse-hover pop-up window.

**Step 3**  Click **History** to view all the jobs related to the selected profile.
The Compliance Profile Execution Jobs window appears.
### Table 4-2 Compliance Profile Execution Job Details

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>
| Job ID            | Unique number assigned to this task at creation time. This number is never reused. There are two formats:  
|                   | • Job ID:  
|                   | Identifies the task. This does not maintain a history. For example: 1001  
|                   | • JobID.Instance ID:  
|                   | Here, in addition to the task, the instance of the task can also be identified. For example: 1001.1, 1001.2 |
| Status            | Provides the status of the current jobs. The status of the current jobs is displayed as succeeded or failed. It also displays the failure reasons. |
| Profile Name      | Name of the Profile for which the job is scheduled.                          |
| Description       | Description of the job.                                                       |
| Owner             | Username of the job creator.                                                  |
| Job Type          | Type of Compliance and Audit Report job. The type include Compliance, Life Cycle Management, and Service reports. |
| Scheduled At      | Date and time at which the job was scheduled.                                |
| Completed At      | Date and time at which the job was completed.                                |
| Schedule Type     | Frequency of the job. This can be:  
|                   | • Once  
|                   | • Immediate  
|                   | • Periodic (calendar/time based).                                             |
| Delete (button)   | Deletes the selected job from the Compliance Profile Execution Jobs window. You can select more than one job to delete. |
| Refresh (button)  | Select a Job and click Refresh Job. The Job Details pane gets refreshed showing the latest status of the job. |
Select a job and click View Report icon. The report is launched in a new browser. You can also click the link Click here to see Report available in the Job Info pane to launch the report.

Click Filter and select a Filter By criteria from the drop-down list and enter the details in the Equals field. The following Filter By options are available:

- Job ID—Select Job ID and enter the Job ID number.
- Status—Select Status and enter the status (Successful, Failed, Cancelled, Running, Waiting, Rejected).
- Description—Select Description and enter the complete name.
- Owner—Select Owner and enter the user name.
- Scheduled at—Select Scheduled at and enter the schedule time details.
- Completed at—Select Completed at and enter the completed time details.
- Schedule Type—Select Schedule Type and enter the type (Immediate, Once, Daily, Weekly, Monthly)

### Table 4-2 Compliance Profile Execution Job Details

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Report (icon)</td>
<td>Select a job and click View Report icon. The report is launched in a new browser. You can also click the link Click here to see Report available in the Job Info pane to launch the report.</td>
</tr>
</tbody>
</table>
| Filter (button) | Click Filter and select a Filter By criteria from the drop-down list and enter the details in the Equals field. The following Filter By options are available:  
- Job ID—Select Job ID and enter the Job ID number.  
- Status—Select Status and enter the status (Successful, Failed, Cancelled, Running, Waiting, Rejected).  
- Description—Select Description and enter the complete name.  
- Owner—Select Owner and enter the user name.  
- Scheduled at—Select Scheduled at and enter the schedule time details.  
- Completed at—Select Completed at and enter the completed time details.  
- Schedule Type—Select Schedule Type and enter the type (Immediate, Once, Daily, Weekly, Monthly) |
Fixing Profile Violations

The Profile Violations Fix Report lists all the devices that do not comply with a defined user profile. A profile is defined as a policy or a set of policies applied on either a device or a set of devices.

To fix a profile violation:

Step 1  Select **Configuration > Compliance > Compliance and Audit Manager > Compliance Profile Execution Jobs**.
The Job Browser Page appears.

**Step 2** Select a job and click **View Report**.

The Compliance Report Page appears.

The **View Report** button will be disabled if the rules are not violated.

**Step 3** Select a device from the Devices table to view the Policies associated with the device. For more details, see Table 4-4.

**Step 4** Select a Policy from the Policies table to view the violation details. For more details, see Table 4-4.

**Step 5** Select the violation that have to be fixed, from the Violations table. For more details, see Table 4-4.

**Step 6** Click **Fix Violations**.

The Fix Compliance Violation Window appears.

<table>
<thead>
<tr>
<th>Table 4-4</th>
<th>Compliance Violation Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Devices Table</td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the profile violated device.</td>
</tr>
<tr>
<td>Selected Violations to fix</td>
<td>Number of violations selected to fix.</td>
</tr>
<tr>
<td>Total Violations</td>
<td>Total number of violations for the device.</td>
</tr>
<tr>
<td>Highest Severity</td>
<td>Highest violation severity for the device.</td>
</tr>
<tr>
<td>Policies Table</td>
<td></td>
</tr>
<tr>
<td>Policy Name</td>
<td>Name of the violated policy.</td>
</tr>
<tr>
<td>Selected Violations to fix</td>
<td>Number of violations selected for fix.</td>
</tr>
<tr>
<td>Total Violations</td>
<td>Total number of violations for the policy</td>
</tr>
<tr>
<td>Policy Info</td>
<td>Information about the violated Policy.</td>
</tr>
<tr>
<td>Violations Table</td>
<td></td>
</tr>
<tr>
<td>Violations with Fix</td>
<td>Lists the violations that can be fixed.</td>
</tr>
<tr>
<td>Violations without Fix</td>
<td>Lists the violations that cannot be fixed.</td>
</tr>
<tr>
<td>Violation Description</td>
<td>Description about the violation.</td>
</tr>
<tr>
<td>Severity</td>
<td>Severity of the Violation.</td>
</tr>
<tr>
<td>Info</td>
<td>Additional violation information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 4-5</th>
<th>Compliance Violation Fix Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Review Fix Commands</td>
<td></td>
</tr>
<tr>
<td>Devices</td>
<td>Name of the profile violated device.</td>
</tr>
<tr>
<td>Commands</td>
<td>Configuration commands for fixing the violation.</td>
</tr>
</tbody>
</table>
Chapter 4  Using Compliance and Audit Manager Feature

### Understanding Compliance Violation Fix Job Browser

You can browse the compliance fix violation jobs registered on the system. Using the Compliance Fix Violation Jobs browser, you can stop, delete, refresh, or filter jobs. You can also view the job details such as work order, device details and job summary.

#### Note
View Permission Report (Reports > System > Users > Permission) to check whether you have the required privileges to perform this task.

Select either:
- Configuration > Compliance > Compliance and Audit Manager > Compliance Profile Violation Fix Jobs.
- Configuration > Job Browsers > Compliance Profile Violation Fix Jobs

The Compliance Fix Violation Jobs page appears.

### Step 7
Select a Scheduler, enter a Job Description, and click **Finish**.

A notification message appears along with the Job ID. Click **OK**. The newly created job appears in the Compliance Profile Violation Fix Job Browser.

### Related Topics
- Adding a New Policy Profile
- Editing Policy Profile
- Deleting Policy Profiles
- Running Compliance Check
- Cloning Policy Profiles
- Viewing Job History

---

<table>
<thead>
<tr>
<th>Table 4-5 Compliance Violation Fix Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column</strong></td>
</tr>
<tr>
<td><strong>Schedule</strong></td>
</tr>
<tr>
<td>Scheduler</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Start Date</td>
</tr>
<tr>
<td>Start Time</td>
</tr>
<tr>
<td>Job Description</td>
</tr>
<tr>
<td>E-mail</td>
</tr>
</tbody>
</table>

---

**Step 7**
Select a Scheduler, enter a Job Description, and click **Finish**.

A notification message appears along with the Job ID. Click **OK**. The newly created job appears in the Compliance Profile Violation Fix Job Browser.

### Related Topics
- Adding a New Policy Profile
- Editing Policy Profile
- Deleting Policy Profiles
- Running Compliance Check
- Cloning Policy Profiles
- Viewing Job History
## Compliance Violation Fix Job Details

Table 4-6 describes the List of Compliance Fix Violation Jobs pane.

<table>
<thead>
<tr>
<th>Column/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique number assigned to a Compliance Fix Violation job when it is created. For periodic jobs such as Daily, Weekly, the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the Job ID 1001.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the job: • Successful—When the job is successful. • Failed—When the job has failed. The number within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, if the status displays Failed(5), then the count of devices that had failed accounts to 5. • Stopped—When the job has been stopped. • Running—When the job is in progress.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the job, entered at the time of job creation.</td>
</tr>
<tr>
<td>Owner</td>
<td>User who created the job.</td>
</tr>
<tr>
<td>Scheduled at</td>
<td>Date and time at which the job was scheduled.</td>
</tr>
<tr>
<td>Completed at</td>
<td>Date and time at which the job was completed.</td>
</tr>
<tr>
<td>Schedule Type</td>
<td>Type of job schedule—Immediate, Once.</td>
</tr>
<tr>
<td>Stop (button)</td>
<td>Stop or cancel a running job.</td>
</tr>
<tr>
<td>Delete (button)</td>
<td>Deletes the selected job from the Compliance Fix Violation Jobs. You can select more than one job to delete.</td>
</tr>
<tr>
<td>Refresh Job (button)</td>
<td>Select a Job and click Refresh Job. The Job Details pane gets refreshed showing the latest status of the job.</td>
</tr>
</tbody>
</table>
Compliance Violation Fix Details

Table 4-7 describes the Job Details pane in the Compliance Fix Violation Jobs.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Order</td>
<td>Shows the work order details for the selected job.</td>
</tr>
<tr>
<td>General Info</td>
<td>The General Info in the work order displays the following details:</td>
</tr>
<tr>
<td></td>
<td>• Job ID</td>
</tr>
<tr>
<td></td>
<td>• Job Type</td>
</tr>
<tr>
<td></td>
<td>• Description—Job description entered at the time of job creation.</td>
</tr>
<tr>
<td></td>
<td>• Schedule Type—Type of job schedule (Immediate, Once, Daily)</td>
</tr>
<tr>
<td></td>
<td>• Policy Profile Execution Job Id</td>
</tr>
<tr>
<td></td>
<td>• Profile Name</td>
</tr>
<tr>
<td>Job Policies</td>
<td>The Job Policies in the work order displays the following details:</td>
</tr>
<tr>
<td></td>
<td>• E-mail Notification—E-mail notification status (Enabled/Disabled)</td>
</tr>
<tr>
<td></td>
<td>• E-mail Ids—E-mail IDs registered for e-mail notification</td>
</tr>
<tr>
<td>Device Details</td>
<td>Shows the Device List of the job.</td>
</tr>
<tr>
<td>Device Details</td>
<td>Shows the list of devices added in the Compliance Fix Violation job.</td>
</tr>
<tr>
<td>Device</td>
<td>Shows the device name.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the device (Success, Failure).</td>
</tr>
<tr>
<td>Message Summary</td>
<td>Shows the device status summary.</td>
</tr>
</tbody>
</table>
Table 4-7 Compliance Fix Violation Job Details

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
</table>
| Filter      | Click **Filter**. Select a Filter By criteria from the drop-down list and enter the details in the Equals field. Click **Go** to filter details. The following Filter By options are available:  
  - Device—Select **Device** and enter the first few letters or the complete name of the device.  
  - Status—Select **Status** and enter the status (Success, Failure)  
  - Message Summary—Select **Message Summary** and enter the first few letters of the message summary. |

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
</table>
| Filter      | **Filter**. Select a Filter By criteria from the drop-down list and enter the details in the Equals field. Click **Go** to filter details. The following Filter By options are available:  
  - Device—Select **Device** and enter the first few letters or the complete name of the device.  
  - Status—Select **Status** and enter the status (Success, Failure)  
  - Message Summary—Select **Message Summary** and enter the first few letters of the message summary. |

---

Configuration Management with Cisco Prime LAN Management Solution 4.2

OL-25941-01

4-23
Understanding Compliance and Audit Manager (CAAM) Policies

This section provides information about the System-defined Policy Groups, Policies supported in each System-defined Policy Group and the rules in each Policy.

LMS supports the following System-defined Policy Groups:

- Center of Internet Security (CIS)
- Cisco Security Best Practices (SAFE)
- Department Of Homeland Security (DHS)
- Defense Information Security Agency (DISA)
- End of Life (EOL)
- Healthcare Insurance Portability Act (HIPAA)
- ISO17799
- National Security Agency (NSA) Router
- Payment Card Industry (PCI)
- Cisco Security Advisory (PSIRT)
- SysAdmin, Audit, Network, Security (SANS)
- Sarbanes Oxley Act (SOX)

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Summary</td>
<td>Shows the job summary details for the selected job.</td>
</tr>
<tr>
<td>General Info</td>
<td>The General Info in the job summary shows the following details:</td>
</tr>
<tr>
<td></td>
<td>• Status—Status of the device at the time of job creation.</td>
</tr>
<tr>
<td></td>
<td>• Start Time—Start time of the job.</td>
</tr>
<tr>
<td></td>
<td>• End Time—End time of the job.</td>
</tr>
<tr>
<td>Job Messages</td>
<td>Shows the following job messages:</td>
</tr>
<tr>
<td></td>
<td>• Pre-job Execution</td>
</tr>
<tr>
<td></td>
<td>• Post-job Execution</td>
</tr>
<tr>
<td>Device Updates</td>
<td>Shows the following update on the devices in the job:</td>
</tr>
<tr>
<td></td>
<td>• Successful</td>
</tr>
<tr>
<td></td>
<td>• Failed</td>
</tr>
<tr>
<td></td>
<td>• Not Attempted</td>
</tr>
<tr>
<td></td>
<td>• Pending</td>
</tr>
</tbody>
</table>

Table 4-7 Compliance Fix Violation Job Details
Center of Internet Security (CIS)

CIS Policy Group supports the following policies:

- Banners
- Logging and Syslog
- Terminal Access
- User Passwords
- ACL on Interfaces
- SMURF Attack
- Loopback Interfaces
- AAA
- AAA Accounting - Commands
- AAA Accounting - Connections
- AAA Accounting - Exec
- AAA Accounting - Network
- AAA Accounting - System
- AAA Authentication - Enable
- AAA Authentication - Login
- HTTP Server
- Miscellaneous Service
- Routing and Forwarding
- SNMP
- SSH Parameters
- TCP Parameters
- BGP
- EIGRP
- OSPF
- RIP
- CDP
- Clock
- Miscellaneous Services On Firewalls
- NTP Configuration
- Device Version Checks

Note

The policies listed in CIS Policy Group may vary.
Cisco Security Best Practices (SAFE)

CiscoSafe Policy Group supports the following policies:

- Banners
- Console Access
- Domain Name
- Logging and Syslog
- Terminal Access
- User Passwords
- SMURF Attack
- Loopback Interfaces
- Remote Commands
- AAA
- AAA Accounting - Exec
- AAA Accounting - Network
- AAA Authentication - Login
- AAA Authorization - EXEC
- AAA Authorization - Network
- HTTP Server
- Miscellaneous Service
- Routing and Forwarding
- SNMP
- SSH Parameters
- TCP Parameters
- OSPF
- CDP
- Clock
- Miscellaneous Services On Firewalls
- NTP Configuration

Note

The policies listed in CiscoSafe Policy Group may vary.
Department Of Homeland Security (DHS)

DHS Policy Group supports the following policies:

- Banners
- Console Access
- Domain Name
- Logging and Syslog
- Terminal Access
- User Passwords
- AAA
- AAA Authentication - Login
- HTTP Server
- Miscellaneous Service
- Routing and Forwarding
- SNMP
- TCP Parameters
- BGP
- EIGRP
- OSPF
- CDP
- NTP Configuration

Note: The policies listed in DHS Policy Group may vary.

Defense Information Security Agency (DISA)

DISA Policy Group supports the following policies:

- Console Access
- Logging and Syslog
- Terminal Access
- Remote Commands
- AAA Authentication - Login
- HTTP Server
- SNMP
- BGP
- EIGRP
- OSPF
- RIP
Understanding Compliance and Audit Manager (CAAM) Policies

End of Life (EOL)

EOL Policy Group supports the following policies:
- Devices Running outdated OS Versions
- Devices with outdated modules
- Outdated Devices As Per Vendor Specific EOL/EOS Announcement

Note: The policies listed in DISA Policy Group may vary.

Healthcare Insurance Portability Act (HIPAA)

HIPAA Policy Group supports the following policies:
- Console Access
- Terminal Access
- User Passwords
- AAA
- AAA Authentication - Login
- AAA Authorization - Commands
- HTTP Server
- SNMP

Note: The policies listed in HIPAA Policy Group may vary.

ISO17799

ISO17799 Policy Group supports the following policies:
- Banners
- Logging and Syslog
- Terminal Access
- User Passwords
- ACL on Interfaces
- SMURF Attack
- AAA
- AAA Accounting - Commands
- AAA Accounting - Connections

Note: The policies listed in EOL Policy Group may vary.
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

- AAA Accounting - Exec
- AAA Accounting - Network
- AAA Accounting - System
- AAA Authentication - Enable
- AAA Authentication - Login
- AAA Authorization - Commands
- AAA Authorization - Configuration
- AAA Authorization - EXEC
- AAA Authorization - Network
- HTTP Server
- Miscellaneous Service
- SNMP
- BGP
- EIGRP
- OSPF
- RIP
- NTP Configuration

Note
The policies listed in ISO17799 Policy Group may vary.

National Security Agency (NSA) Router

NSA Router Policy Group supports the following policies:
- Banners
- Console Access
- Domain Name
- Host Name
- Logging and Syslog
- Terminal Access
- User Passwords
- Null (Black Hole) Routing
- SMURF Attack
- Dynamic Trunking Protocols (DTP)
- IEEE 802.3 Flow Control
- Spanning Tree Protocols (STP)
- Unidirectional Link Detection (UDLD)
- VLAN 1
- VLAN Trunking Protocols (VTP)
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

- Loopback Interfaces
- AAA
- AAA Authentication - Login
- Control Plane Policing
- HTTP Server
- Miscellaneous Service
- Routing and Forwarding
- SNMP
- TCP Parameters
- BGP
- EIGRP
- OSPF
- RIP
- ACLs
- CDP
- NTP Configuration
- Device Version Checks

Note  The policies listed in NSA Router Policy Group may vary.

Payment Card Industry (PCI)

PCI Policy Group supports the following policies:
- Console Access
- Logging and Syslog
- Terminal Access
- User Passwords
- Traffic Rules
- AAA
- AAA Authentication - Login
- HTTP Server
- Miscellaneous Service
- SNMP
- NTP Configuration

Note  The policies listed in PCI Policy Group may vary.
Cisco Security Advisory (PSIRT)

PSIRT Policy Group supports the following policies:

- AAA Command Authorization By-pass - 68840 [IOS]
- ARP Table Overwrite - 13600 [IOS]
- ASA Crafted IKE Message DoS Vulnerability - 111877 [ASA]
- ASA Crafted TCP Segment DoS Vulnerability - 111485 [ASA]
- ASA Crypto Accelerator Memory Leak Vulnerability - 108009 [ASA]
- ASA NTLMv1 Authentication Bypass Vulnerability - 111485 [ASA]
- ASA SCCP Inspection DoS Vulnerability - 111485 [ASA]
- ASA SIP Inspection DoS Vulnerability - 111485 [ASA]
- ASA SIP Inspection DoS Vulnerability - 111877 [ASA]
- ASA TCP Connection Exhaustion DoS Vulnerability - 111485 [ASA]
- ASA Three SunRPC Inspection DoS Vulnerability - 111877 [ASA]
- ASA Three TLS DoS Vulnerability - 111877 [ASA]
- ASA WebVPN DTLS DoS Vulnerability - 111485 [ASA]
- Access Point Memory Exhaustion from ARP Attacks - 68715 [IOS]
- Access Point Web-browser Interface - 70567 [IOS]
- Auth Proxy Buffer Overflow - 66269 [IOS]
- Authentication Proxy Vulnerability - 110478 [IOS]
- BGP Attribute Corruption - 10935 [IOS]
- BGP Logging - 63845 [IOS]
- BGP Long AS path Vulnerability - 110457 [IOS]
- BGP Packet - 53021 [IOS]
- BGP Update Message Vulnerability - 110457 [IOS]
- CEF Data Leak - 20640 [IOS]
- Call Processing Solutions - 63708 [IOS]
- CatOS Catalyst 5000 Series 802.1x Vulnerability - 13617 [CatOS]
- CatOS Denial-of-Service of TCP-based services - 43864 [CatOS]
- CatOS DoS using Telnet, HTTP and SSH - 52781 [CatOS]
- CatOS Embedded HTTP Server Buffer Overflow - 27962 [CatOS]
- CatOS Enable Password Bypass Vulnerability - 13619 [CatOS]
- CatOS Memory Leak Vulnerability - 13618 [CatOS]
- CatOS Multiple SSH Vulnerabilities - 8118 [CatOS]
- CatOS NAM (Network Analysis Module) Vulnerability - 81863 [CatOS]
- CatOS OpenSSH Server Vulnerabilities - 45322 [CatOS]
- CatOS Password Bypass Vulnerability - 42340 [CatOS]
- CatOS SNMP Malformed Message Handling - 19296 [CatOS]
• CatOS SNMP Multiple Community String Vulnerabilities - 13629 [CatOS]
• CatOS SNMP Version 3 Authentication Vulnerability - 107408 [CatOS]
• CatOS SSH Can Cause a Crash - 24862 [CatOS]
• CatOS SSH Protocol Mismatch Vulnerability - 10932 [CatOS]
• CatOS TCP Conn Reset - 50961 [CatOS]
• CatOS TCP State Manipulation DoS Vulnerability - 109444 [CatOS]
• Cisco IOS Software IGMP Vulnerability - 112027 [IOS]
• Crafted Encryption Packet DoS Vulnerability - 110393 [IOS]
• Crafted ICMP Messages DoS for IPSec Tunnels - 64520 [IOS]
• Crafted ICMP Messages DoS for L2TPv2 - 64520 [IOS]
• Crafted ICMP Messages DoS for TCP over IPv4 - 64520 [IOS]
• Crafted ICMP Messages DoS for TCP over IPv6 - 64520 [IOS]
• Crafted IP Option - 81734 [IOS]
• Crafted TCP Packet Denial of Service Vulnerability - 111450 [IOS]
• Crafted UDP Packet Vulnerability - 108558 [IOS]
• Crypto - 91890 [IOS]
• DFS ACL Leakage - 13655 [IOS]
• DHCP - 63312 [IOS]
• DLSw Denial of Service Vulnerabilities - 99758 [IOS]
• DLSw Vulnerability - 77859 [IOS]
• FTP Server - 90782 [IOS]
• Firewall Application Inspection Control Vulnerability - 107716 [IOS]
• H.323 Denial of Service Vulnerability - 111265 [IOS]
• H.323 Protocol DoS Vulnerability - 110396 [IOS]
• H323 DoS Vulnerability - 112021 [IOS]
• HTTP - 13627 [IOS]
• HTTP Auth - 13626 [IOS]
• HTTP Command Injection - 68322 [IOS]
• HTTP GET Vulnerability - 44162 [IOS]
• HTTP Server Query - 13628 [IOS]
• Hard-Coded SNMP Community Names in Cisco Industrial Ethernet 3000 Series Switches Vulnerability - 111895 [IOS]
• IKE Resource Exhaustion Vulnerability - 110559 [IOS]
• IKE Xauth - 64424 [IOS]
• IPS ATOMIC.TCP Signature Vulnerability - 81545 [IOS]
• IPS DoS Vulnerability - 107583 [IOS]
• IPS Fragmented Packet Vulnerability - 81545 [IOS]
- IPSec IKE Malformed Packet - 50430 [IOS]
- IPSec Vulnerability- 111266 [IOS]
- IPv4 - 44020 [IOS]
- IPv6 Crafted Packet - 65783 [IOS]
- IPv6 Routing Header - 72372 [IOS]
- Information Leakage Using IPv6 Routing Header - 97848 [IOS]
- Inter Process Communication (IPC) Vulnerability - 107661 [IOS]
- Layer 2 Tunneling Protocol (L2TP) DoS Vulnerability - 107441
- MPLS - 63846 [IOS]
- MPLS Forwarding Infrastructure DoS Vulnerability - 107646
- MPLS VPN May Leak Information Vulnerability - 107578
- Mobile IP and IPv6 Vulnerabilities - 109487
- Multicast Virtual Private Network (MVPN) Date Leak - 100374 [IOS]
- Multiple Crafted IPv6 Packets - 63844
- Multiple DNS Cache Poisoning Attacks - 107064 [IOS]
- Multiple Features Crafted TCP Sequence Vulnerability - 109337
- Multiple Features IP Sockets Vulnerability - 109333 [IOS]
- Multiple Multicase Vulnerabilities - 107550
- Multiple SIP DoS Vulnerabilities - 107617
- Multiple SSH Vulnerabilities - 8118
- Multi-protocol Label Switching Packet Vulnerability - 111458
- NAM (Network Analysis Module) Vulnerability - 81863
- NAT - 13659
- NAT Skinny Call Control Protocol Vulnerability - 111268
- NAT Skinny Call Control Protocol Vulnerability - 99866
- NTP - 23445
- NTP Packet Vulnerability - 110447
- Network Address Translation Vulnerability - 112028
- Next Hop Resolution Protocol Vulnerability - 91766
- OSPF Malformed Packet- 61365 [IOS]
- OSPF Malformed Packet- 61365 [IOS]
- OSPF, MPLS VPN Vulnerability - 100526 [IOS]
- Object-Group ACL Bypass Vulnerability - 110398 [IOS]
- OpenSSL Implementation DoS Vulnerability - 45643 [IOS]
- OpenSSL Implementation Vulnerability - 49898 [IOS]
- PIX Crafted MGCP Packet - 98711 [PIX, ASA]
- PIX Crafted TLS Packet - 98711 [PIX, ASA]
- PIX Erroneous SIP Processing Vulnerabilities - 107475 [PIX, ASA]
• PIX Buffer overflow - 28947 [PIX, ASA]
• PIX CBAC - 23885 [PIX, ASA]
• PIX Control Plane Access Control List Vulnerability - 105444 [PIX, ASA]
• PIX Crafted TCP ACK Packet Vulnerability - 105444 [PIX, ASA]
• PIX Crafted TLS Packet Vulnerability - 105444 [PIX, ASA]
• PIX Crypto - 23886 [PIX, ASA]
• PIX Crypto - 91890 [PIX, ASA]
• PIX DoS - 13635 [PIX, ASA]
• PIX Device Reload with SIP Inspection Vulnerability - 107475 [PIX, ASA]
• PIX Enhanced inspection of Malformed HTTP traffic - 77853 [PIX, ASA]
• PIX FTP - 13638 [PIX, ASA]
• PIX Firewall Unintentional Password Modification - 70811 [PIX, ASA]
• PIX IPSec Client Authentication Processing Vulnerability - 107475 [PIX, ASA]
• PIX ISAKMP - 28947 [PIX, ASA]
• PIX Inspection of a stream of malformed TCP packets - 77853 [PIX, ASA]
• PIX Inspection of malformed SIP packets - 77853 [PIX, ASA]
• PIX Instant Message Inspection Vulnerability - 105444 [PIX, ASA]
• PIX LDAP Authentication Bypass - 82451 [PIX, ASA]
• PIX Mailguard - 13636 [PIX, ASA]
• PIX Multiple SSH Vulnerabilities - 8118 [PIX, ASA]
• PIX OpenSSL Implementation DoS Vulnerability - 45643 [PIX, ASA]
• PIX OpenSSL Implementation Vulnerability - 49898 [PIX, ASA]
• PIX Potential Information Disclosure in Clientless VPNs - 107475 [PIX, ASA]
• PIX Privilege escalation - 77853 [PIX, ASA]
• PIX SMTP - 15235 [PIX, ASA]
• PIX SNMP - 19296 [PIX, ASA]
• PIX SNMPv3 - 47284 [PIX, ASA]
• PIX SSH - 24862 [PIX, ASA]
• PIX SSL VPN DOS - 82451 [PIX, ASA]
• PIX SSL VPN Memory Leak Vulnerability - 107475 [PIX, ASA]
• PIX Scan Denial of Service Vulnerability - 105444 [PIX, ASA]
• PIX TCP Conn Reset - 50961 [PIX, ASA]
• PIX TCP Prevention - 68268 [PIX, ASA]
• PIX TCP Reset - 13639 [PIX, ASA]
• PIX Time-to-Live Vulnerability - 100314 [PIX, ASA]
• PIX Traceback When Processing Malformed SIP Requests - 107475 [PIX, ASA]
• PIX URI Processing Error Vulnerability in SSL VPNs - 107475 [PIX, ASA]
• PIX VPN Password Expiry - 82451 [PIX, ASA]
• PIX VPNC - 47284 [PIX, ASA]
• PIX/ASA ACL Bypass Vulnerability - 109974 [PIX, ASA]
• PIX/ASA Crafted H.323 Packet DoS Vulnerability - 109974 [PIX, ASA]
• PIX/ASA Crafted HTTP Packet DoS Vulnerability - 109974 [PIX, ASA]
• PIX/ASA Crafted TCP Packet DoS Vulnerability - 109974 [PIX, ASA]
• PIX/ASA IPv6 Denial of Service Vulnerability - 108009 [PIX, ASA]
• PIX/ASA SQL *Net Packet DoS Vulnerability - 109974 [PIX, ASA]
• PIX/ASA TCP State Manipulation DoS Vulnerability - 109444 [PIX, ASA]
• PIX/ASA VPN Authentication Bypass Vulnerability - 109974 [PIX, ASA]
• PIX/ASA Windows NT Domain Authentication Bypass Vulnerability - 108009
• PPTP - 13640 [IOS]
• Radius - 65328 [IOS]
• Reload After Scanning - 136322 [IOS]
• SAA Packets - 42744 [IOS]
• SGBP Packet - 68793 [IOS]
• SIP - 81825 [IOS]
• SIP DoS Vulnerabilities - 109322 [IOS]
• SIP DoS Vulnerability - 110395 [IOS]
• SIP DoS Vulnerability - 112022 [IOS]
• SNMP Malformed Message Handling - 19294 [IOS]
• SNMP Message Processing - 50980 [IOS]
• SNMP Multiple Community String Vulnerabilities - 13629 [IOS]
• SNMP Read-Write ILMI Community String - 13630 [IOS]
• SNMP Trap Reveals WEP Key - 46468 [IOS]
• SNMP Version 3 Authentication Vulnerability - 107408 [IOS]
• SSH Can Cause a Crash - 24862 [IOS]
• SSH Malformed Packet - 29581 [IOS]
• SSH TACACS+ Authentication - 64439 [IOS]
• SSL - 91888 [IOS]
• SSL Packet Processing Vulnerability - 107631 [IOS]
• SSL VPN Vulnerability - 112029 [IOS]
• Secure Copy Authorization Bypass Vulnerability - 97261 [IOS]
• Secure Copy Privilege Escalation Vulnerability - 109323 [IOS]
• Secure Shell Denial of Services Vulnerabilities - 99725 [IOS]
• Session Initiation Protocol Denial of Services Vulnerability - 111448 [IOS]
• Syslog Crash - 13660 [IOS]
• TCP - 72318 [IOS]
• TCP Conn Reset - 50960 [IOS]
• TCP Denial of Service Service Vulnerability -112099 [IOS]
• TCP ISN -13631 [IOS]
• TCP State Manipulation DoS Vulnerability -109444 [IOS]
• Telnet DoS -61671 [IOS]
• Telnet Option-10939 [IOS]
• Timers Heap Overflow -68064 [IOS]
• Tunnels DoS Vulnerability -109482 [IOS]
• Unified Communications Manager Express Vulnerability -110451
• User Datagram protocol delivery issue -100638 [IOS]
• Virtual Private Dial-up Network DoS Vulnerability -97278 [IOS]
• Vulnerabilities Found by PROTOS IPSec Test Suite -68158 [IOS]
• Vulnerability in IOS Firewall Feature Set -9360 [IOS]
• WeBVPN and SSLVPN Vulnerabilities -107397 [IOS]
• Zone-Based Policy Firewall Vulnerability -110410 [IOS]
• cTCP Denial of Service Vulnerability -109314 [IOS]
• uBR10012 Series Devices SNMP Vulnerability -107696 [IOS]

Note  The policies listed in PSIRT Policy Group may vary.

SysAdmin, Audit, Network, Security (SANS)

SANS Policy Group supports the following policies:
• Banners
• Terminal Access
• User Passwords
• SMURF Attack
• AAA
• HTTP Server
• Miscellaneous Service
• SNMP

Note  The policies listed in SANS Policy Group may vary.
Sarbanes Oxley Act (SOX)

SOX Policy Group supports the following policies:

- Console Access
- Logging and Syslog
- Terminal Access
- User Passwords
- AAA
- AAA Accounting - Commands
- AAA Authentication - Login

Note: The policies listed in SOX Policy Group may vary.

Compliance and Audit Manager Policies

Policies are defined by a set of rules. This section explains the various policies that are supported in LMS.

Banners

Description
General banner and Message Of The Day (MOTD) related vulnerability checks.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

References
BS 7799, ISO/IEC 17799, ISO/IEC 27001(Section 11.5.1 of Second Edition, 2005-06-15)
Information Technology - Code of practice for information security management.
National Security Agency (NSA) Cisco Router Configuration Guide((Section 4.1.5 Page 58 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
SANS Router Security Policy(Sections 3.0(6), 3.0(7))
The SANS (SysAdmin, Audit, Network, Security) Institute publishes security policy to help system administrators with rapid development and implementation of information security policies.
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 5.2, Page 15 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Cisco SAFE Compliance(1.1b)
SAFE: A Security Blueprint for Enterprise Networks

Department of Homeland Security (DHS) Compliance(Section 2.1, Page 12 of Version 2.0)
This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Center for Internet Security, Benchmark for Cisco IOS.(Section 1.1.3, Page:12 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

Center for Internet Security, Benchmark for Cisco PIX/ASA.(Section 1.1.3, Page: 11 of Version 2.0, Nov 2007)
CIS PIX/ASA benchmark recommends the prudent level of minimum due care for operating system security. CIS PIX/ASA benchmark contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All PIX devices should implement these settings.

**Rule 1**

**Rule**
Message Of The Day (MOTD) should be configured [IOS, PIX, ASA]

**Description**
A Message of the day banner, which includes a legal notice, should be setup on each operational router. A legal notice usually includes a 'no trespassing' warning, a statement that all use of the router must be authorized by the owning organization, and perhaps a statement about the router being subject to monitoring.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
A proper legal notice protects the ability of the owning organization to pursue legal remedies against an attacker. Consult your organization’s legal staff or general counsel for suitable language to use in your legal notice.
Suggested Fix
Configure a Message of the day banner using the command:

```plaintext
[no] banner motd
line vty <begining number> - <end number>
[no] motd-banner
[no] exec-banner
```

Rule 2

Rule
Message Of The Day should contain given pattern [IOS, PIX, ASA]

Description
A Message of the day banner, which includes a legal notice, should be setup on each operational router. A legal notice usually includes a 'no trespassing' warning, a statement that all use of the router must be authorized by the owning organization, and perhaps a statement about the router being subject to monitoring.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
A proper legal notice protects the ability of the owning organization to pursue legal remedies against an attacker. Consult your organization's legal staff or general counsel for suitable language to use in your legal notice.

Suggested Fix
Modify a Message of the day banner to contain required information using the command:

```plaintext
banner motd
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match Type</td>
<td>Select if the given input is to be matched as a plain string or a regular expression.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>String or Regular Expression</td>
<td>A String(Regular Expression) that should be present in Message Of The Day</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Rule 3

Rule
Message of The Day should NOT contain given pattern [IOS, PIX, ASA]

Description
A Message of the day banner should not contain network architecture information and router configuration details. Router model and location information should be included only if necessary. Be especially careful not to provide information in the banner message that should not be shared with the general public, or information that is not visible from unprivileged EXEC mode.
Understanding Compliance and Audit Manager (CAAM) Policies

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
A proper legal notice protects the ability of the owning organization to pursue legal remedies against an attacker. Consult your organization's legal staff or general counsel for suitable language to use in your legal notice.

Suggested Fix
Modify the Message of the day banner not to contain prohibited information using the command:

`banner motd`

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match Type</td>
<td>Select if the given input is to be matched as a plain string or a regular expression.</td>
<td>Required: true Default: false</td>
</tr>
<tr>
<td>String or Regular Expression</td>
<td>A String(Regular Expression) that should be NOT present in Message Of The Day</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Rule 4

Rule
Login message should be configured [IOS, PIX, ASA]

Description
A login banner, which includes a legal notice, should be setup on each operational router. A legal notice usually includes a ‘no trespassing’ warning, a statement that all use of the router must be authorized by the owning organization, and perhaps a statement about the router being subject to monitoring.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
A proper legal notice protects the ability of the owning organization to pursue legal remedies against an attacker. Consult your organization's legal staff or general counsel for suitable language to use in your legal notice.

Suggested Fix
Configure a login banner using the command:

`[no] banner login`
Rule 5

Rule
Login message should contain given pattern [IOS, PIX, ASA]

Description
A login banner, which includes a legal notice, should be setup on each operational router. A legal notice usually includes a 'no trespassing' warning, a statement that all use of the router must be authorized by the owning organization, and perhaps a statement about the router being subject to monitoring.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
A proper legal notice protects the ability of the owning organization to pursue legal remedies against an attacker. Consult your organization's legal staff or general counsel for suitable language to use in your legal notice

Suggested Fix
Modify a login banner to contain required information using the command:

banner login

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match Type</td>
<td>Select if the given input is to be matched as a plain string or a regular expression.</td>
<td>Required: true  Default: false</td>
</tr>
<tr>
<td>String or Regular Expression</td>
<td>A String(Regular Expression) that should be present in the Login Message</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Rule 6

Rule
Login message should NOT contain given pattern [IOS, PIX, ASA]

Description
A login banner should not contain network architecture information and router configuration details. Router model and location information should be included only if necessary. Be especially careful not to provide information in the banner message that should not be shared with the general public, or information that is not visible from unprivileged EXEC mode.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices
Impact
A proper legal notice protects the ability of the owning organization to pursue legal remedies against an attacker. Consult your organization's legal staff or general counsel for suitable language to use in your legal notice.

Suggested Fix
Modify the log banner not to contain prohibited information using the command:

```
banner login
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match Type</td>
<td>Select if the given input is to be matched as a plain string or a regular expression.</td>
<td>Required: true, Default: false</td>
</tr>
<tr>
<td>String or Regular Expression</td>
<td>A String(Regular Expression) that should NOT be present in the Login Message</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Rule 7

Rule
Exec banner should be configured [IOS, PIX, ASA]

Description
A Exec banner, which includes a legal notice, should be setup on each operational router. A legal notice usually includes a ‘no trespassing’ warning, a statement that all use of the router must be authorized by the owning organization, and perhaps a statement about the router being subject to monitoring.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
A proper legal notice protects the ability of the owning organization to pursue legal remedies against an attacker. Consult your organization's legal staff or general counsel for suitable language to use in your legal notice.

Suggested Fix
Configure a exec banner using the command:

```
[no] banner exec
line vty <begining number > - <end number>
[no] exec-banner
```
Rule 8

Rule
Exec banner should contain given pattern [IOS, PIX, ASA]

Description
A Exec banner, which includes a legal notice, should be setup on each operational router. A legal notice usually includes a 'no trespassing' warning, a statement that all use of the router must be authorized by the owning organization, and perhaps a statement about the router being subject to monitoring.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
A proper legal notice protects the ability of the owning organization to pursue legal remedies against an attacker. Consult your organization's legal staff or general counsel for suitable language to use in your legal notice.

Suggested Fix
Modify a exec banner to contain required information using the command:

```
banner exec
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Match Type | Select if the given input is to be matched as a plain string or a regular expression. | Required: true  
  Default: false |
| String or Regular Expression | A String(Regular Expression) that should be present in Exec Banner | Required: true |

Rule 9

Rule
Exec banner should NOT contain given pattern [IOS, PIX, ASA]

Description
A Exec banner should not contain network architecture information and router configuration details. Router model and location information should be included only if necessary. Be especially careful not to provide information in the banner message that should not be shared with the general public, or information that is not visible from unprivileged EXEC mode.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices
Impact
A proper legal notice protects the ability of the owning organization to pursue legal remedies against an attacker. Consult your organization's legal staff or general counsel for suitable language to use in your legal notice.

Suggested Fix
Modify the exec banner not to contain prohibited information using the command:

\textit{banner exec}

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match Type</td>
<td>Select if the given input is to be matched as a plain string or a regular expression.</td>
<td>Required: true, Default: false</td>
</tr>
<tr>
<td>String or Regular Expression</td>
<td>A String(Regular Expression) that should be NOT present in Exec Banner</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Console Access

**Description**
Policies related to console and auxiliary terminal access.

**Applicable Platforms**
Cisco IOS Devices

**References**

- Control Objectives for Information and Related Technology(4.0)

COBIT (Control Objectives for Information and Related Technology) is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT is a de-facto standard used by most of the auditors when auditing for IT section of Sarbanes-Oxley (SOX) Compliance.

- National Security Agency (NSA) Cisco Router Configuration Guide(Section 8.1(3) Page 275, Section 3.4.4 Page 49, Section 4.1.6 Page 66 of Version 1.1c)

The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

- Cisco SAFE Compliance(1.1b)

SAFE: A Security Blueprint for Enterprise Networks

- Payment Card Industry Data Security Standard(2.3 of Version 1.1, September, 2006)

The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

- Health Insurance Portability and Accountability Act.(164.312(a)(1), 164.312(e)(1))
HIPAA (Health Insurance Portability and Accountability Act.) is designed to protect confidential healthcare information through improved security standards and federal privacy legislation. It defines requirements for storing patient information before, during and after electronic transmission. Centers for Medicare & Medicaid Services (CMS) has provided a Security Rule (45 CFR Part 160 and 164) which is adopted to implement provisions of the HIPAA.

Defence Information System Agency (Section NET0655 of Dec 2, 2005)

DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

Department of Homeland Security (DHS) Compliance (Section 2.2, Page 21 of Version 2.0)

This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

### Rule 1

#### Rule
Check console connection [IOS]

#### Description
Permit or block the router access using console ports as desired.

#### Applicable Platforms
Cisco IOS Devices

#### Impact
None

#### Suggested Fix
Enable or disable the console ports using the command:

```markdown
line con0
[no] exec
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Access   | Whether to allow connections using console terminal. | Required: true
|          |                                    | Default: true |

### Rule 2

#### Rule
Check auxiliary connection [IOS]

#### Description
Permit or block the router access using auxiliary ports as desired.
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Applicable Platforms
Cisco IOS Devices

Impact
None.

Suggested Fix
Enable or disable the auxiliary ports using the command:

```
line aux 0
[no] exec
```

Domain Name

Description
Using Domain Name Lookup Service, you can use device names in the commands instead of IP addresses. By default, the DNS lookups are broadcasted to 255.255.255.255. If there are trusted domain name servers, which can translate the hostnames into IP Addresses, you may configure the devices to send DNS queries to these servers.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

References
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.2.2 Page79 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

National Security Agency (NSA) Cisco Switch Configuration Guide(Section 6.2.2, Page 18 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Cisco SAFE Compliance(Appendix A, Page 39 of A Security Blueprint for Enterprise Networks)
SAFE: A Security Blueprint for Enterprise Networks
Department of Homeland Security (DHS) Compliance (Section 4.3, Page 29 of Version 2.0)
This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Rule 1

Rule
Check state of domain name configuration [IOS, PIX, ASA]

Description
Each device within a given domain should have a domain name to be configured with whatever is the local/global policy for that domain. Domain names will be used as part of fully qualified host name of the router and any unqualified name lookups. Setting a domain name is also necessary for using SSH.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
SSH can not be enabled with this violation. Also, all the host names would have to be fully qualified.

Suggested Fix
Configure domain name using the command:

[no] ip domain-name (for IOS)
[no] domain-name (for PIX)

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select whether the device should be configured with a domain name or not.</td>
<td>Required: true  Default: true</td>
</tr>
</tbody>
</table>

Rule 2

Rule
Check value of domain name [IOS, PIX, ASA]

Description
Each device within a given domain should have a domain name to be configured with whatever is the local/global policy for that domain. Domain names will be used as part of fully qualified host name of the router and any unqualified name lookups. Setting a domain name is also necessary for using SSH.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices
Impact
SSH can not be enabled with this violation. Also, all the host names would have to be fully qualified.

Suggested Fix
Configure domain name using the command:

- `ip domain-name <domain name>` (for IOS)
- `domain-name <domain name>` (for PIX)

Rule 3

Rule
Check state of domain lookup configuration [IOS, PIX, ASA]

Description
By default, IOS sends DNS name queries to the broadcast address 255.255.255.255. If you do not want your router to send queries, turn off DNS name resolution. In general, DNS name resolution should be enabled on a router only if one or more trustworthy DNS servers are available.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
If DNS lookup is disabled, If there are any host names given in the commands, those names will not be resolved to IP addresses, causing them to be unreachable. The commands with hostnames given in them instead of plain IP Addresses may not work completely. Also, whenever an IP address is changed, all the network devices' configurations would have to be updated if they have the old IP address in their configuration. If the DNS lookup is enabled, then it is advisable to have at least one DNS server is configured. Otherwise, all the hostname to IP Address resolution will be done by broadcasting the packets to 255.255.255.255

Suggested Fix
Configure the DNS name resolution (Domain name lookup) using the command:

- `[no] ip domain lookup` (for IOS)
- `[no] dns domain-lookup` (for PIX)

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enter the name of the network domain to which this device belongs to.</td>
<td>Required: true</td>
</tr>
<tr>
<td>Domain Name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select whether the device should do lookups to convert host names to IP Addresses.</td>
<td>Required: true, Default: true</td>
</tr>
</tbody>
</table>
Rule 4

**Rule**
Domain name servers should contain given hosts [IOS]

**Description**
All the devices within a network should be configured with a DNS server to be able to do address resolution.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
If the domain look up is enabled but no DNS servers are configured, then all the lookup packets are broadcasted to 255.255.255.255. Also, it is advisable to configure all the devices within a domain with the same DNS server so that the host name data base is maintained centrally.

**Suggested Fix**
Configure one or more of DNS servers using the command:

`ip name-server`

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Servers</td>
<td>Enter the IP address(es) of the DNS Servers that should be configured on the device. Using DNS Server Editor option, you can add, remove or update DNS Server details. You can also change the order of the server details.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Host Name

**Description**
Host name related policies.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**References**
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.2.2 Page 78 of Version 1.1c)

The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
Rule 1

Rule
Host name must be configured [IOS, PIX, ASA]

Description
It is advisable that all the devices are configured with distinct hostnames to identify them uniquely.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
No unique way of identifying the device.

Suggested Fix
Configure host name using the command

hostname

Logging and Syslog

Description
Logging a router's activities and status offers several benefits. Using the information in a log, the administrator can tell whether the router is working properly or whether it has been compromised. Configuring logging on the router should be done carefully. Send the router logs to a designated log host, which is a separate computer whose only job is to accept and store logs. Set the level of logging on the router to meet the needs of your security policy, and expect to modify the log settings as the network evolves. The logging level may need to be modified based on how much of the log information is useful.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

References
Payment Card Industry Data Security Standard(PCI).(10 of Version 1.1, September, 2006)
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

Control Objectives for Information and Related Technology(DS5.5 of 4.0)
COBIT (Control Objectives for Information and Related Technology) is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT is a de-facto standard used by most of the auditors when auditing for IT section of Sarbanes-Oxley (SOX) Compliance.
Understanding Compliance and Audit Manager (CAAM) Policies

National Security Agency (NSA) Cisco Router Configuration Guide (Section 8.1(11) Page 277, Section 8.1(17) Page 278, Section 4.5.2 Page 139, 142-145 of Version 1.1c)

The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

National Security Agency (NSA) Cisco Switch Configuration Guide (Section 12.2.1, Page 44 of Version 1.0)

The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.


Information Technology - Code of practice for information security management.

Cisco SAFE Compliance (1.1b)

SAFE: A Security Blueprint for Enterprise Networks

Defence Information System Agency (Section NET1021 of Dec 2, 2005)

DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

Department of Homeland Security (DHS) Compliance (Section 3.1, Page 14 of Version 2.0)

This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Center for Internet Security, Benchmark for Cisco PIX/ASA (Section 1.2.3, Page: 20 of Version 2.0, Nov 2007)

CIS PIX/ASA benchmark recommends the prudent level of minimum due care for operating system security. CIS PIX/ASA benchmark contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All PIX devices should implement these settings.

Center for Internet Security, Benchmark for Cisco IOS (Section 1.2.3, Page: 28 of Version 2.2, Nov. 2007)

CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.
Rule 1

Rule
Check if logging is enabled to all supported destinations [IOS, PIX, ASA]

Description
Check if state of event logging on the router is not same as that of desired state. Logging a router's activities and status offers several benefits. Using the information in a log, the administrator can tell whether the router is working properly or whether it has been compromised. In some cases, it can show what types of probes or attacks are being attempted against the router or the protected network.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
If the logging is disabled, The events that happen on the router are not logged anywhere. This might make it harder to troubleshoot any network issues. Also, this may cause some of the problems, including attempts to attacks go un-noticed, as well as not to have any evidence about any un-authorized activity. If the logging is enabled, make sure the logging messages are sent to only trusted host on a protected network so that the logs can not be compromised and can not viewed by anyone not authorized to view them.

Suggested Fix
Configure logging service using the command:

\[ \text{[no]} \text{ logging on (for IOS)} \]
\[ \text{[no]} \text{ logging enable (for PIX)} \]

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Logging State</td>
<td>Whether the global logging should be enabled or disabled.</td>
<td>Required: true Default: true</td>
</tr>
</tbody>
</table>

Rule 2

Rule
Check syslog logging related parameters [IOS, PIX, ASA]

Description
Logging level and state should be carefully chosen so that important information is logged but at the same time, the logging server is not flooded with too many log messages from the devices. Also, the device should be configured to send log messages to a designated host on the protected network.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA device
Impact
If the logging level and host(s) are not configured according to the policy, it may make it harder to troubleshoot problems.

Suggested Fix
Configure the logging host(s), level(s) using the command:

\[\text{[no]} \text{ logging <desired logging level}>\]

### Rule 3

**Rule**
Check syslog host related parameters [IOS]

**Description**
The device should be configured to send log messages to a designated host on the protected network.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
If the logging level and host(s) are not configured according to the policy, it may make it harder to troubleshoot problems.

**Suggested Fix**
Configure the logging hosts using the command:

- \(\text{logging <hostname or ip address} \) (for IOS)
- \(\text{logging host <hostname or ip address} \) (for PIX)

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog Logging State</td>
<td>Whether the syslog logging should be enabled or disabled.</td>
<td>Required: true Default: true</td>
</tr>
<tr>
<td>Syslog Logging Level</td>
<td>Syslog Logging level</td>
<td>Required: false Default: informational</td>
</tr>
</tbody>
</table>
Chapter 4 Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 4

Rule
Check logging facility [IOS, PIX, ASA]

Description
Check that the specified syslog facility is used when sending logging messages to the remote syslog server. You can direct log messages to the specified logging facility on your remote syslog server using the logging facility command. To do this, enable logging and define the UNIX system facility to which you want to send the log messages.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
Configure the required logging facility parameters using the command:

logging facility

Suggested Fix

Rule 5

Rule
Check buffer loggin state, level and logging buffer size [IOS, PIX, ASA]
Description
Setup the buffered logging state, level and size according to your security policy. This lets the device to log messages to its internal buffers in the memory.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
If the buffer logging level and size are set to buffer too many messages, it may cause the device to run out of memory for other tasks. If it is configured too low, it may cause the messages to be lost in the buffer too quickly.

Suggested Fix
Configure the required buffered logging parameters using the command logging buffered

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Logging State</td>
<td>Whether the buffer logging should be enabled or disabled</td>
<td>Required: true Default: true</td>
</tr>
<tr>
<td>Buffer Logging Level</td>
<td>Buffer Logging level</td>
<td>Required: false Default: informational</td>
</tr>
<tr>
<td>Minimum Buffer Size</td>
<td>Minimum logging buffer size. It would be a violation if the device is configured to have any buffer size that is less than the value given.</td>
<td>Required: false Default: informational Min Value: 4096 Max Value: 2147483647</td>
</tr>
</tbody>
</table>

Rule 6

Rule
Check console logging state and level [IOS, PIX, ASA]

Description
Setup the console logging state, level and size according to your security policy. This lets the device to log messages to the console terminal. In general, the logging level at the console should be set to display lots of messages only when the console is in use or its output is being displayed or captured.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
No known impact.
Suggested Fix
Configure the console logging parameters using the command:

\[ \text{[no] logging console} \]

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console Logging State</td>
<td>Whether the console logging should be enabled or disabled</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: true</td>
</tr>
<tr>
<td>Console Logging Level</td>
<td>Console Logging level</td>
<td>Required: false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: critical</td>
</tr>
</tbody>
</table>

Rule 7

Rule
Check monitor logging state and level [[IOS, PIX, ASA]

Description
Setup the monitor logging state, level and size according to your security policy. This controls the messages that are displayed on any terminal that connected to the router.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
No known impact

Suggested Fix
Configure the monitor logging parameters using the command:

\[ \text{logging monitor} \]

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Logging State</td>
<td>Whether monitor logging should be enabled or disabled</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>Monitor Logging Level</td>
<td>Monitor Logging level</td>
<td>Required: false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: informational</td>
</tr>
</tbody>
</table>

Rule 8

Rule
Check history logging level [IOS, PIX, ASA]
Description
Setup the history logging level according to your security policy. The level is used for limiting log messages stored in the history table and sent to the SNMP network management station. The default for IOS devices is warning. There is no default for PIX, FWSM, or ASA devices.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
Because SNMP traps are potentially unreliable, at least one syslog message, the most recent message, is stored in a history table on the device. You can view the history table using the show logging history command. Limit the types of messages stored in the history table based on the severity level your organization requires.

Suggested Fix
Configure the history logging level using the command:

```
logging history
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>History Logging Level</td>
<td>History Logging level</td>
<td>Required: false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: warnings</td>
</tr>
</tbody>
</table>

Rule 9

Rule
Check Timestamps in Log Messages [IOS, PIX, ASA]

Description
Check to see if timestamps are displayed in log messages

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
If the timestamps are not shown in the log messages, it may not be possible to sense the order of events occurring in the network.

Suggested Fix
Configure the device to show timestamps for log messages using the command:

```
[no] service timestamps log
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Timestamps in Log</td>
<td>Whether to show timestamps in each logging messages</td>
<td>Required: true</td>
</tr>
<tr>
<td>Messages</td>
<td></td>
<td>Default: true</td>
</tr>
</tbody>
</table>
Rule 10

Rule
Check Timestamps in Debug Messages

Description
Check to see if timestamps are displayed in debug messages

Applicable Platforms
Cisco IOS Devices

Impact
If the timestamps are not shown in the debug messages, it may not be possible to sense the order of events occurring in the network.

Suggested Fix
Configure the device to show timestamps for debug messages using the command:

\[\text{[no]} \text{ service timestamps debug}\]

<table>
<thead>
<tr>
<th>Rule Description Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show Timestamps in Debug Messages</strong></td>
</tr>
<tr>
<td>Whether to show timestamps in debugging messages</td>
</tr>
<tr>
<td>Required: true</td>
</tr>
<tr>
<td>Default: true</td>
</tr>
</tbody>
</table>

Rule 11

Rule
Check sequence numbers in log messages [IOS]

Description
Check to see if visible sequence numbering of system logging messages is enabled or not.

Applicable Platforms
Cisco IOS Devices

Impact
If the sequence numbers are not shown in the log messages, it may not be possible to sense the order of events occurring in the network.

Suggested Fix
Configure the device to show timestamps for log messages using the command:

\[\text{[no]} \text{ service sequence-numbers}\]

<table>
<thead>
<tr>
<th>Rule Description Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show Sequence Numbers in Log Messages</strong></td>
</tr>
<tr>
<td>Whether to show sequence numbers in each logging message</td>
</tr>
<tr>
<td>Required: true</td>
</tr>
<tr>
<td>Default: true</td>
</tr>
</tbody>
</table>
Terminal Access

Description
This policy checks for various access controls that need to be put in place to restrict access to the network device’s command line. One primary mechanism for remote administration of Cisco routers is logging in via Telnet or SSH. These connections are called virtual terminal lines. Login on the virtual terminal lines should be disabled if remote administration is not absolutely necessary. Remote administration without encryption is inherently dangerous because anyone with a network sniffer on the right LAN segment can acquire router passwords and would then be able to take control of the router.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

References
Control Objectives for Information and Related Technology (A12.4 of 4.0)
COBIT (Control Objectives for Information and Related Technology) is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT is a de-facto standard used by most of the auditors when auditing for IT section of Sarbanes-Oxley (SOX) Compliance.

National Security Agency (NSA) Cisco Router Configuration Guide(Section 8.1(6) Page 276, Section 4.1.5 Page 58, 59, 60, Section 4.1.6 Page 61 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Health Insurance Portability and Accountability Act.(164.312(a)(1), 164.312(e)(1))
HIPAA (Health Insurance Portability and Accountability Act.) is designed to protect confidential healthcare information through improved security standards and federal privacy legislation. It defines requirements for storing patient information before, during and after electronic transmission. Centers for Medicare & Medicaid Services (CMS) has provided a Security Rule (45 CFR Part 160 and 164) which is adopted to implement provisions of the HIPAA.

Information Technology - Code of practice for information security management.

National Security Agency (NSA) Cisco Switch Configuration Guide(Section 5.2, Page 12 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Payment Card Industry Data Security Standard(PCI).(2.3 of Version 1.1, September, 2006)
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

Cisco SAFE Compliance(1.1b)
SAFE: A Security Blueprint for Enterprise Networks

SANS Router Security Policy(3.0(8))
The SANS (SysAdmin, Audit, Network, Security) Institute publishes security policy to help system administrators with rapid development and implementation of information security policies.

Defence Information System Agency(Section NET0645,NET0740 of Dec 2, 2005)
DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

Department of Homeland Security (DHS) Compliance(Section 1.3,2.3, Page 10 of Version 2.0)
This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Center for Internet Security, Benchmark for Cisco PIX/ASA.(Section 1.1.2.4, Page: 9 of Version 2.0, Nov 2007)
CIS PIX/ASA benchmark recommends the prudent level of minimum due care for operating system security. CIS PIX/ASA benchmark contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All PIX devices should implement these settings.

Center for Internet Security, Benchmark for Cisco IOS.(Section 1.1.1.4, Page: 8; Section 1.1.2.3-1.1.2.6, Page:10-11; of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

**Rule 1**

**Rule**
No more than required VTY lines should be enabled on the device [IOS]

**Description**
Check that a given device does not have more VTY lines enabled than required.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
No known impact
Suggested Fix
If the router has more VTYs than needed, then either disable or delete the extra ones using the command:
\[\text{line vty } <\text{beg line number}> <\text{end line number}> \text{ no exec}\]

### Rule 2

**Rule**
Check Authentication parameters on terminal lines [IOS]

**Description**
Each terminal line should be configured with some type of authentication for logging on the device, failing to do so can enable an unauthorized user to gain device access. This rule checks other miscellaneous authentication parameters on the terminal lines including session time out, maximum default privilege level configured and any access restrictions on the terminal lines.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
An unauthorized user may gain access to the device.

**Suggested Fix**
Configure with some type of authentication for login on the terminal lines using the commands:
\[\text{line vty } <\text{beg line number}> <\text{end line number}> \text{ login authentication}\]
\[\text{login authentication}\]
\[\text{privilege level}\]
\[\text{exec-timeout}\]
\[\text{access-class}\]
You can add, update and delete terminal line configuration details.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Maximum VTY Lines      | Maximum number of VTY lines to be enabled         | Required: true  
Min Value: 1  
Max Value: 2147483647 |
| Terminal Line Group   | Group of terminal lines to apply the policy.      | Required: true          |
| Login Authentication   | Selected terminal lines should be configured to authenticate using login. | Required: true  
Default: login |
| Maximum default level allowed | Maximum default privilege level that should be given on lines. | Required: false  
Default: 0  
Min Value: 0  
Max Value: 15 |
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 3

Rule
Check for allowed incoming connections [IOS]

Description
Make sure that all the terminal lines are configured to block incoming connections using un-authorized protocols.

Applicable Platforms
Cisco IOS Devices

Impact
An unauthorized user may connect to the device using any undesired protocols violating the set policy.

Suggested Fix
Disable terminal line access for un-authorized incoming connections using the command:

```
line vty <beg line number> <end line number>
transport input
```

You can add, update and delete terminal line configuration details.

<table>
<thead>
<tr>
<th>Rule Description Constraints</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Idle Timeout (Minutes)</td>
<td>Idle timeout (in minutes) to be enforced on lines. If a user leaves the EXEC session idle for this much time, it will be disconnected automatically by the device.</td>
<td>Required: false &lt;br&gt; Default: 10 &lt;br&gt; Min Value: 1 &lt;br&gt; Max Value: 3579</td>
</tr>
<tr>
<td>Maximum Login Response Timeout (Seconds)</td>
<td>Maximum timeout (in seconds), the system will wait for login input (such as username and password) before timing out</td>
<td>Required: false &lt;br&gt; Min Value: 1 &lt;br&gt; Max Value: 300</td>
</tr>
<tr>
<td>Whether Access to this terminal lines should be controlled</td>
<td>Choose whether access to this terminal line should be controlled using an access list control or not</td>
<td>Required: false &lt;br&gt; Default: false</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Line Group</td>
<td>Group of terminal lines to apply the policy.</td>
<td>Required: true</td>
</tr>
<tr>
<td>Block all incoming connections</td>
<td>Block all incoming connections on this group of terminal lines</td>
<td>Required: true &lt;br&gt; Default: dontcare</td>
</tr>
<tr>
<td>Telnet</td>
<td>Telnet protocol</td>
<td>Required: false &lt;br&gt; Default: false</td>
</tr>
<tr>
<td>SSH</td>
<td>SSH protocol</td>
<td>Required: false &lt;br&gt; Default: true</td>
</tr>
</tbody>
</table>
Rule 4

Rule
Check for allowed outgoing connections [IOS]

Description
Make sure that all the terminal lines are configured to block outgoing connections using un-authorized protocols.

Applicable Platforms
Cisco IOS Devices

Impact
An unauthorized user may connect to other devices from this device using any undesired protocols violating the set policy.

Suggested Fix
Disable terminal line access for all un-authorized outgoing connections using the command:

```
line vty <beg line number> <end line number>
transport output
```

You can add, update and delete terminal line configuration details.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Line Group</td>
<td>Group of terminal lines to apply the policy.</td>
<td>Required: true</td>
</tr>
<tr>
<td>Block all outgoing connections</td>
<td>Block all outgoing connections on this group of terminal lines</td>
<td>Required: true</td>
</tr>
<tr>
<td>Telnet</td>
<td>Telnet protocol</td>
<td>Required: false</td>
</tr>
<tr>
<td>SSH</td>
<td>SSH protocol</td>
<td>Required: false</td>
</tr>
</tbody>
</table>

Rule 5

Rule
Check that Telnet access is prohibited. [PIX, ASA]

Description
Prohibit telnet access to the PIX device.

Applicable Platforms
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
Only use SSH and-or Cisco PDM or ASDM to manage the PIX. Do not use Telnet for remote administration of the PIX, it offers no confidentiality or integrity protections.
Rule 6

Suggested Fix
Prohibit Telnet access using the command:

```
no telnet
```

Rule 7

Rule
Check the maximum timeout for Telnet sessions. [PIX, ASA]

Description
Verify timeout is configured to automatically disconnect the telnet sessions after a fixed idle time.

Applicable Platforms
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
This prevents unauthorized users from misusing abandoned sessions.

Suggested Fix
Configure device timeout to disconnect sessions after a fixed idle time, using the command:

```
telnet timeout
```
Chapter 4   Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 8

Rule
Check the maximum timeout for SSH sessions. [PIX, ASA]

Description
Verify timeout is configured to automatically disconnect the SSH sessions after a fixed idle time.

Applicable Platforms
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
This prevents unauthorized users from misusing abandoned sessions.

Suggested Fix
Configure device timeout to disconnect sessions after a fixed idle time, using the command:
ssh timeout

<table>
<thead>
<tr>
<th>Rule Description Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Telnet Session idle Timeout (Minutes)</td>
</tr>
<tr>
<td>Required: true</td>
</tr>
<tr>
<td>Min Value: 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule Description Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum SSH Session idle Timeout (Minutes)</td>
</tr>
<tr>
<td>Required: true</td>
</tr>
<tr>
<td>Min Value: 1</td>
</tr>
</tbody>
</table>

User Passwords

Description
There are three ways of protection schemes in Cisco IOS.
- Plain password where there is no protection and encryption.
- Cisco defined encryption algorithm which is known to the commercial security community to be weak.
- Iterated MD5 hash which is much stronger.

Cisco recommends using the MD5 hash encryption for passwords where possible. (See “Configuring Passwords and Privileges” in the Cisco IOS Security Configuration Guide)
Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices
Cisco IOS Devices With AUTO_SECURE Capability

References
Payment Card Industry Data Security Standard(PCI).(8.1, 8.4, 8.5 of Version 1.1, September, 2006)
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

Control Objectives for Information and Related Technology(DS5 of 4.0)
COBIT (Control Objectives for Information and Related Technology) is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT is a de-facto standard used by most of the auditors when auditing for IT section of Sarbanes-Oxley (SOX) Compliance.

National Security Agency (NSA) Cisco Router Configuration Guide(Section 8.1(9) Page 276, 8.1(19) Page 279, Section 4.1.5 Page 63, Section 4.1.8 Page 66 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Health Insurance Portability and Accountability Act.(164.308(a)(5)(ii), 164.312(d))
HIPAA (Health Insurance Portability and Accountability Act.) is designed to protect confidential healthcare information through improved security standards and federal privacy legislation. It defines requirements for storing patient information before, during and after electronic transmission. Centers for Medicare & Medicaid Services (CMS) has provided a Security Rule (45 CFR Part 160 and 164) which is adopted to implement provisions of the HIPAA. BS 7799, ISO/IEC 17799, ISO/IEC 27001(Section 10, Section 11.2, 11.5 of First Edition, 2000-12-01)

Information Technology - Code of practice for information security management.

Cisco SAFE Compliance(1.1b) SAFE: A Security Blueprint for Enterprise Networks SANS Router Security Policy(3.0.2) The SANS (SysAdmin, Audit, Network, Security) Institute publishes security policy to help system administrators with rapid development and implementation of information security policies. Department of Homeland Security (DHS) Compliance(Section 1.1, Page 6 of Version 2.0) This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet. Center for Internet Security, Benchmark for Cisco PIX/ASA.(Section 1.1.4, Page: 13 of Version 2.0, Nov 2007) CIS PIX/ASA benchmark recommends the prudent level of minimum due care for operating system security. CIS PIX/ASA benchmark contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All PIX devices should implement these settings.
Center for Internet Security, Benchmark for Cisco IOS. (Section 1.1.2.1, Page: 9; Section 1.1.4, Page: 15 of Version 2.2, Nov 2007) CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

Rule 1

**Rule**
Passwords should not be shown in clear text in configuration [IOS]

**Description**
Make sure the passwords are not shown in clear text in the configuration.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
When passwords are shown in clear text, anyone who gets hold of a device configuration can access the router by using the username and password.

**Suggested Fix**
Encrypt all passwords using the command:

```
service password-encryption
```

Rule 2

**Rule**
Check enable password is configured and uses strong encryption [IOS, PIX, ASA]

**Description**
Make sure that the enable password is defined and it uses strong encryption.

**Applicable Platforms**
Cisco IOS Devices

Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
Access to the privileged EXEC mode (enable mode) should be protected by requiring a password. Additionally, for Cisco IOS software devices, you can create a strongly encrypted password using the enable secret command. There are two password protection schemes in Cisco IOS software. Type-7 uses the Cisco-defined encryption algorithm which is known to the commercial security community to be weak. Type-5 uses an iterated MD5 hash which is much stronger. Cisco recommends that Type-5 encryption to be used instead of Type-7 where possible. The enable password command uses Type-7 encryption, whereas the enable secret command uses Type-5 encryption.
Suggested Fix
Use strong encryption to configure enable password using the command:

```
enable secret [IOS]
enable password [PIX]
```

Rule 3

Rule
All users must have passwords configured [IOS, PIX, ASA]

Description
Make sure all users have passwords configured.

Applicable Platforms
- Cisco IOS Devices
- Cisco PIX Devices Running >= 7.x and ASA devices

Impact
When users do not have passwords, the device does not ask for password when someone tries to access. This may lead to an intruder to gain access to the device if they can guess/know the username.

Suggested Fix
Configure passwords for all users using the command:

```
username <user name> password|secret
```

Rule 4

Rule
Passwords must be MD5 encrypted [IOS]

Description
Make sure all user Passwords are MD5 encrypted. MD5 is the highest level security provided by Cisco to store the user passwords. Other methods of password storing (clear text or Cisco proprietary encoding) are known to be vulnerable for decoding.

Applicable Platforms
- Cisco IOS Devices

Impact
User passwords may be decoded and guessed by possible intruder.

Suggested Fix
Encrypt all user passwords with MD5 using the command:

```
username <user name> secret
```
Rule 5

**Rule**
Check minimum length for user/enable/line passwords [IOS]

**Description**
The minimum length, in characters, for passwords defined on the device. Specifying a minimum password length provides enhanced security access to the router by eliminating common passwords that are prevalent on most networks.

**Applicable Platforms**
Cisco IOS Devices With AUTO_SECURE Capability

**Impact**
One method attackers use to crack passwords is to try all possible combinations of characters until the password is discovered. Longer passwords have exponentially more possible combinations of characters, making this method of attack much more difficult.

**Suggested Fix**
Use security passwords min-length command to set the minimum length, in characters, for user/enable passwords defined on the device. Beware that if you use the security passwords min-length command, any configured passwords that are less than the specified minimum length will no longer work. Ensure that the user, enable, secret, and line passwords on the device satisfy the minimum length before using the command:

```
security passwords min-length
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length for passwords should be atleast</td>
<td>The minimum length, in characters, for passwords defined on the device.</td>
<td>Required: true  Default: 6  Min Value: 1  Max Value: 16</td>
</tr>
</tbody>
</table>

Rule 6

**Rule**
Check maximum authentication failure rate [IOS]

**Description**
The number of times a user can attempt to log into the device before the failure is logged to the syslog and user access is prohibited for 15 seconds. A device should be configured to lock access after some predefined number of unsuccessful login attempts whenever possible. One method of cracking passwords, called the dictionary attack, is to use software that attempts to log in using every word in a dictionary. This configuration causes access to the router to be locked for a period of 15 seconds after the predefined unsuccessful login attempts, disabling the dictionary method of attack. In addition to locking access to the device, this configuration causes a log message to be generated after the predefined unsuccessful login attempts, warning the administrator of the unsuccessful login attempts.
Applicable Platforms
Cisco IOS Devices With AUTO_SECURE Capability

Impact
Intruders may make continuous attempts to login into the device.

Suggested Fix
Configure authentication failure rate on the device using the command:

```
security authentication failure rate
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure rate threshold should be at most</td>
<td>The number of times a user can attempt to log into the device before the failure is logged to the syslog and user access is prohibited for 15 seconds.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min Value: 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max Value: 1024</td>
</tr>
</tbody>
</table>

Rule 7

Rule
Check unwanted usernames are not configured [IOS, PIX, ASA]

Description
Make sure unwanted usernames are not configured.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
This may lead to an intruder to gain access to the device if they can guess/know the username.

Suggested Fix
Delete unwanted username using the command:

```
no username <user name>
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banned Usernames</td>
<td>Banned usernames to check for. Using Banned Usernames - Editor option, you can add, update or remove banned username details. You can also change the order of the banned username details.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>
Rule 8

**Rule**
Check only one username is configured [IOS, PIX, ASA]

**Description**
Make sure only one username is configured.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
Configuring more than one username may lead to an intruder to gain access to the device if they can guess/know the username.

**Suggested Fix**
Delete unwanted username using the command:

```
no username <user name>
```

**ACL on Interfaces**

**Description**
Policies to make sure the interfaces have required Access Control Lists configured.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Rule 1

**Rule**
Check interfaces have access lists configured [IOS, PIX, ASA]

**Description**
This rule checks if given interfaces have required ACLs configured and those access lists have valid configuration.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
Interfaces may permit unwanted traffic.

**Suggested Fix**
Enable Access Control Lists on the interface using the command:
interface <interface name>

ip access-group <acl number or name> <in|out>

You can add, update or remove the interface details. You can also change the order of the interface details.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Group</td>
<td>Group of interfaces to apply the policy. Example valid Values: 'Any', 'AnyEthernet', 'FastEthernet', 'GigabitEthernet', 'FastEthernet0/1', 'FastEthernet0/.*' etc.</td>
<td>Required: true</td>
</tr>
<tr>
<td>Incoming ACL match type</td>
<td>ACL Match criterion to enforce for incoming traffic on this interface group.</td>
<td>Required: true</td>
</tr>
<tr>
<td>Incoming ACL ID</td>
<td>Incoming ACL ID to be applied on the interface to filter incoming traffic.</td>
<td>Required: false</td>
</tr>
<tr>
<td>Outgoing ACL match type</td>
<td>ACL Match criterion to enforce for outgoing traffic on this interface group.</td>
<td>Required: true</td>
</tr>
<tr>
<td>Outgoing ACL ID</td>
<td>Outgoing ACL ID to be applied on the interface to filter outgoing traffic.</td>
<td>Required: false</td>
</tr>
</tbody>
</table>

Note
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

Null (Black Hole) Routing

Description
Many administrators configure their routers to filter connections and drop packets using basic and extended access lists. Access lists provide the administrator with a high degree of precision in selectively permitting and denying traffic. For example, access lists would allow an administrator to block only Telnet (TCP port 23) traffic from exiting their network. The fine granularity access lists provide can impose significant administrative and performance burdens, depending on the network architecture, router configuration, and traffic load. Backbone routers, in particular, are often too heavily utilized to permit heavy use of access lists. An alternative to access lists for traffic control is a technique known as black hole routing, or null routing. Null routing (or black-hole routing) sacrifices the fine selectivity of access lists, it can be used only to impose a ban on all traffic sharing a specific destination address or network. There is no simple way to specify which protocols or types of traffic may or may not pass. If an address or network is null routed, ALL traffic sent to it will immediately be discarded. Because this type of filtering is done as part of normal routing, it imposes little or no performance burden on normal packet flow. It is important to note that null routing can only discard traffic based on its addresses (usually only the destination). This makes it well-suited to mitigating attack situations where 'bad' traffic into your network is all directed to one or a small number of address ranges. It is also well-suited for discarding data directed to unassigned or reserved addresses.

Applicable Platforms
Cisco IOS Devices With Static Routing Capability
References
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.4.6 Page 128 of Version 1.1c)

The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Rule 1

Rule
Check undesirable packets are directed to NULL interface [IOS]

Description
This rule checks that given ipaddress/mask combinations are black-holed and are routed to null interfaces. The simple way to configure null routing is to set up a null interface and create a static route that directs the undesirable packets to it.

Applicable Platforms
Cisco IOS Devices With Static Routing Capability

Impact
Undesired packets will be routed using normal routing table lookup.

Suggested Fix
Configure static routing for these subnets using the commands:

```
interface <Null interface>
!
ip route <ip address> <network mask> <Null Interface>
```

You can add, update or remove IP Address and Network Mask details.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP Address of the network to be routed to NULL interface</td>
<td>Required: true</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Network mask of the subnet that needs to be routed to NULL interface.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Note
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.
SMURF Attack

Description
The Smurf Attack involves sending a large amount of ICMP Echo packets to a subnet's broadcast address with a spoofed source IP address from that subnet.

Applicable Platforms
Cisco IOS Devices

References
National Security Agency (NSA) Cisco Router Configuration Guide(Section 8.1(2) Page 275, Section 4.3.3 Page 91 of Version 1.1c)

The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

National Security Agency (NSA) Cisco Switch Configuration Guide(Section 6.2.1, Page 18 of Version 1.0)

The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.


Information Technology - Code of practice for information security management.
Cisco SAFE Compliance(1.1b)
SAFE: A Security Blueprint for Enterprise Networks SANS Router Security Policy(3.0(3a))
The SANS (SysAdmin, Audit, Network, Security) Institute publishes security policy to help system administrators with rapid development and implementation of information security policies.

Rule 1

Rule
Check for SMURF attack vulnerability [IOS].

Description
The Smurf Attack involves sending a large amount of ICMP Echo packets to a subnet's broadcast address with a spoofed source IP address from that subnet.

Applicable Platforms
Cisco IOS Devices

Impact
This attack can lead to Denial of Service(DoS).
Suggested Fix
Disable directed broadcast on the interfaces. Alternatively, an inbound access-list can be used to deny any packets destined for broadcast addresses using the command:

```
interface <interface name>
no ip directed-broadcast
```

Traffic Rules

Description
Policies to make sure the interfaces have traffic rules

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

References
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

Rule 1

Rule
Check interfaces have access lists configured [IOS, PIX, ASA]

Description
This rule checks if given interfaces have required access controls configured.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
Interfaces may permit unwanted traffic.

Suggested Fix
Enable Access Control Lists on the interface using the command:

```
interface <interface name>
ip access-group <acl number or name> <in|out>
```
Chapter 4  Using Compliance and Audit Manager Feature

### Understanding Compliance and Audit Manager (CAAM) Policies

#### Note
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

#### Dynamic Trunking Protocols (DTP)

**Description**
Policy to specify required parameters for Dynamic Trunking Protocol (DTP). DTP is a protocol exchanged between switches to negotiate the trunking mode on the connected ports. Depending on the configuration on a neighboring port, the ports on this switch will be placed in either trunking mode or non-trunking mode dynamically. Cisco switches come up in this dynamic trunking mode by default and if they become trunk ports, it may cause to trunk all the VLANs, which further makes the management of VLANs harder.

**Applicable Platforms**
Cisco IOS Switches

**References**
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 9.5.2 Page 36 of Version 1.0)

The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Rule 1

Rule
Check DTP is disabled. [IOS]

Description
This check will make sure that DTP is disabled on the interfaces so that they are placed permanently in trunking mode or in non-trunking mode.

Applicable Platforms
Cisco IOS Switches

Impact
A port may use the Dynamic Trunking Protocol (DTP) to automatically negotiate which trunking protocol it will use, and how the trunking protocol will operate. By default, a Cisco Ethernet port's default DTP mode is "dynamic desirable", which allows the port to actively attempt to convert the link into a trunk. Even worse, the member VLANs of the new trunk are all the available VLANs on the switch. If a neighboring port's DTP mode becomes "trunk", "dynamic auto", or "dynamic desirable", and if the two switches support a common trunking protocol, then the line will become a trunk automatically, giving each switch full access to all VLANs on the neighboring switch. An attacker who can exploit DTP may be able to obtain useful information from these VLANs.

Suggested Fix
Set the port in either permanent trunk mode or permanent non-trunk mode using the command:

```
interface <interface name>
switchport mode <access|trunk>
```

IEEE 802.3 Flow Control

Description
In order to handle congestion, Ethernet ports are capable to respond to a flow control frame from a remote port and stop transmitting for some time. If a Gigabit Ethernet or 10-Gigabit Ethernet port receive buffer becomes full, the port transmits an IEEE 802.3Z pause frame that requests remote ports to delay sending frames for a specified time. All Ethernet ports (10 Gbps, 1 Gbps, 100 Mbps, and 10 Mbps) can receive and respond to IEEE 802.3Z pause frames from other devices.

Applicable Platforms
Cisco IOS Switches

References
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 8 Page 29 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Rule 1

**Rule**
Check Receive Flow Control [IOS]

**Description**
This check will ensure that the port is configured with a desired state of flow control in receive direction.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
802.3X Flow Control allows receiving ports to pause transmission of packets from the sender during times of congestion. If this feature is enabled, a pause frame can be received, stopping the transmission of data packets. Flow Control pause frames could be used in a denial of service attack.

**Suggested Fix**
Configure receiving of flow control frames on the interface using the command:

```
interface <interface name>
[no] flowcontrol receive
```
You can add, update or remove flow control details. You can also change the order of the flow control details.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Group</td>
<td>Group of interfaces to apply the policy. Example valid Values: 'Any', 'AnyEthernet', 'FastEthernet', 'GigabitEthernet', 'FastEthernet0/1', 'FastEthernet0/.*' etc.</td>
<td>Required: true</td>
</tr>
<tr>
<td>Desired state of receive flow control</td>
<td>10-Gigabit Ethernet port receive buffer becomes full, the port transmits an IEEE 802.3Z pause frame that requests remote ports to delay sending frames for a specified time. All Ethernet ports (10 Gbps, 1 Gbps, 100 Mbps, and 10 Mbps) can receive and respond to IEEE 802.3Z pause frames from other devices.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

**Note**
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

**Spanning Tree Protocols (STP)**

**Description**
Spanning Tree Protocol (STP), also known as 802.1d, is a Layer 2 protocol designed to prevent loops within switched networks. Loops can occur when redundant network paths have been configured to ensure resiliency. Typically, STP goes through a number of states (e.g., block, listen, learn, and forward) before a port is able to pass user traffic. This process can take between 30 and 50 seconds. In cases where
a single host is connected to a port, and there is no chance of a loop being created, the STP Portfast feature can be utilized to immediately transition the port into a forwarding state. However, it will still participate in STP calculations and move into a blocked state in the event of a network loop. A vulnerability associated with STP is that a system within the network can actively modify the STP topology. There is no authentication that would prevent such an action. The bridge ID, a combination of a two-byte priority and a six-byte MAC address, determines the root bridge within a network. The lower the bridge ID, the more likely the switch will be elected as the root bridge. A switch with the lowest bridge ID can become the root bridge, thereby influencing traffic flows and reducing the efficiency of the network.

Applicable Platforms
Cisco IOS Switches

References
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 10 Page 38 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Rule 1

Rule
Check that BPDU Guard is enabled on all the ACCESS ports [IOS]

Description
This check will make sure the BPDU guard is enabled/disabled on given interfaces as per the policy. The STP Portfast BPDU Guard allows network administrators to enforce the STP topology on ports enabled with Portfast. Systems attached to ports with the Portfast BPDU Guard enabled will not be allowed to modify the STP topology. Upon reception of a BPDU message, the port is disabled and stops passing all network traffic. This feature can be enabled both globally and individually for ports configured with Portfast. By default, STP BPDU guard is disabled.

Applicable Platforms
Cisco IOS Switches

Impact
A vulnerability associated with STP is that a system within the network can actively modify the STP topology. There is no authentication that would prevent such an action. The bridge ID, a combination of a two-byte priority and a six-byte MAC address, determines the root bridge within a network. The lower the bridge ID, the more likely the switch will be elected as the root bridge. A switch with the lowest bridge ID can become the root bridge, thereby influencing traffic flows and reducing the efficiency of the network.

Suggested Fix
Configure BPDU Guard on the ports based on the policy using the command:

```
interface <interface name>
```
*no* spanning-tree bpduguard

**Rule 2**

**Rule**
Check the BPDU State [IOS]

**Description**
This check will make sure the BPDU guard is enabled/disabled on given interfaces as per the policy. The STP Portfast BPDU Guard allows network administrators to enforce the STP topology on ports enabled with Portfast. Systems attached to ports with the Portfast BPDU Guard enabled will not be allowed to modify the STP topology. Upon reception of a BPDU message, the port is disabled and stops passing all network traffic. This feature can be enabled both globally and individually for ports configured with Portfast. By default, STP BPDU guard is disabled.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
A vulnerability associated with STP is that a system within the network can actively modify the STP topology. There is no authentication that would prevent such an action. The bridge ID, a combination of a two-byte priority and a six-byte MAC address, determines the root bridge within a network. The lower the bridge ID, the more likely the switch will be elected as the root bridge. A switch with the lowest bridge ID can become the root bridge, thereby influencing traffic flows and reducing the efficiency of the network.

**Suggested Fix**
Configure BPDU Guard on the ports based on the policy using the command:

```
interface <interface name>
[no] spanning-tree bpduguard
```

You can add, update or remove BPDU State details. You can also change the order of the BPDU State details.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Group</td>
<td>Group of interfaces to apply the policy. Example valid Values: 'Any', 'AnyEthernet', 'FastEthernet', 'GigabitEthernet', 'FastEthernet0/1', 'FastEthernet0/.*' etc.</td>
<td>Required: true</td>
</tr>
<tr>
<td>Desired state of BPDU Guard</td>
<td>the administrator must manually put the Layer 2 LAN interface back in service. BPDU Guard can be configured at the interface level. When configured at the interface level, BPDU Guard shuts the port down as soon as the port receives a BPDU, regardless of the PortFast configuration.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>
Chapter 4 Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 3

Rule
Check that Root Guard State is enabled on all the ACCESS ports [IOS]

Description
This check will make sure the interface is configured with a proper root guard state. The STP Root Guard feature is a mechanism used to protect the STP topology. Unlike the BPDU Guard, STP Root Guard allows participation in STP as long as the attached system does not attempt to become the root. If the Root Guard is activated, then the port recovers automatically after it quits receiving the superior BPDUs that would make it the root. Root Guard can be applied to one or more ports on edge switches and on internal switches on a network. In general, apply this feature to those ports on each switch that should not become the root.

Applicable Platforms
Cisco IOS Switches

Impact
A vulnerability associated with STP is that a system within the network can actively modify the STP topology. There is no authentication that would prevent such an action. The bridge ID, a combination of a two-byte priority and a six-byte MAC address, determines the root bridge within a network. The lower the bridge ID, the more likely the switch will be elected as the root bridge. A switch with the lowest bridge ID can become the root bridge, thereby influencing traffic flows and reducing the efficiency of the network.

Suggested Fix
Configure root Guard on the ports based on the policy using the command:

```
interface <interface name>
[no] spanning-tree guard root
```

Rule 4

Rule
Check the Root Guard State [IOS]

Description
This check will make sure the interface is configured with a proper root guard state. The STP Root Guard feature is a mechanism used to protect the STP topology. Unlike the BPDU Guard, STP Root Guard allows participation in STP as long as the attached system does not attempt to become the root. If the Root Guard is activated, then the port recovers automatically after it quits receiving the superior BPDUs that would make it the root. Root Guard can be applied to one or more ports on edge switches and on internal switches on a network. In general, apply this feature to those ports on each switch that should not become the root.

Applicable Platforms
Cisco IOS Switches
Impact
A vulnerability associated with STP is that a system within the network can actively modify the STP topology. There is no authentication that would prevent such an action. The bridge ID, a combination of a two-byte priority and a six-byte MAC address, determines the root bridge within a network. The lower the bridge ID, the more likely the switch will be elected as the root bridge. A switch with the lowest bridge ID can become the root bridge, thereby influencing traffic flows and reducing the efficiency of the network.

Suggested Fix
Configure root Guard on the ports based on the policy using the command:

```
interface <interface name>
[no] spanning-tree guard root
```

You can add, update or remove Root Guard State details. You can also change the order of the Root Guard State details.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Group</td>
<td>Group of interfaces to apply the policy. Example valid Values: 'Any', 'AnyEthernet', 'FastEthernet', 'GigabitEthernet', 'FastEthernet0/1', 'FastEthernet0/.*' etc.</td>
<td>Required: true</td>
</tr>
<tr>
<td>Desired state of STP Root Guard</td>
<td>NOTE: Enabling root Guard functionality on a port may disable that port as soon as it receives a superior BPDU message. The STP root guard feature prevents a port from becoming root port or blocked port. If a port configured for root guard receives a superior BPDU, the port immediately goes to the root-inconsistent (blocked) state.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Note
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

Unidirectional Link Detection (UDLD)

Description
The Cisco-proprietary UDLD protocol allows devices connected through fiber-optic or copper (for example, Category 5 cabling) Ethernet cables connected to LAN ports to monitor the physical configuration of the cables and detect when a unidirectional link exists. When a unidirectional link is detected, UDLD shuts down the affected LAN port and alerts the user. Unidirectional links can cause a variety of problems, including spanning tree topology loops. A unidirectional link occurs whenever traffic transmitted by the local device over a link is received by the neighbor but traffic transmitted from the neighbor is not received by the local device. If one of the fiber strands in a pair is disconnected, as long as autonegotiation is active, the link does not stay up. In this case, the logical link is undetermined, and UDLD does not take any action. If both fibers are working normally at Layer 1, then UDLD at Layer 2 determines whether those fibers are connected correctly and whether traffic is flowing bidirectionally between the correct neighbors.
Applicable Platforms
Cisco IOS Switches

References
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 8 Page 29, 30 of Version 1.0)

The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Rule 1

Rule
Check UDLD state on all fiber-optic interfaces [IOS]

Description
This check will make sure UDLD state on the fiber-optic interfaces is configured as per the policy.

Applicable Platforms
Cisco IOS Switches

Impact
Directly connected switches running the Unidirectional Link Detection (UDLD) protocol can determine if a unidirectional link exists between them. If one is detected, then the link is shutdown until manually restored. UDLD messages could be used in a denial of service attack.

Suggested Fix
configure UDLD on the interface or globally using the command:

\[ \text{[no]} \text{ udld enable interface } <\text{interface name}> \]
\[ \text{[no]} \text{ udld port} \]

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired state of UDLD</td>
<td>Desired state of UDLD configuration.</td>
<td>Required: true&lt;br&gt;Default: false</td>
</tr>
</tbody>
</table>

Rule 2

Rule
Check UDLD state on all copper interfaces [IOS]

Description
This check will make sure UDLD state on the copper interfaces is configured as per the policy.
Applicable Platforms
Cisco IOS Switches

Impact
Directly connected switches running the Unidirectional Link Detection (UDLD) protocol can determine if a unidirectional link exists between them. If one is detected, then the link is shutdown until manually restored. UDLD messages could be used in a denial of service attack.

Suggested Fix
configure UDLD on the interface or globally using the command:

\[\text{[no]}\ udld \text{enable interface <interface name>}\]
\[\text{[no]}\ udld \text{port}\]

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired state of UDLD</td>
<td>Desired state of UDLD configuration.</td>
<td>Required: true Default: false</td>
</tr>
</tbody>
</table>

Rule 3

Rule
Check UDLD state on specific interfaces [IOS]

Description
This check will make sure UDLD state on given interfaces is configured as per the policy.

Applicable Platforms
Cisco IOS Switches

Impact
Directly connected switches running the Unidirectional Link Detection (UDLD) protocol can determine if a unidirectional link exists between them. If one is detected, then the link is shutdown until manually restored. UDLD messages could be used in a denial of service attack.

Suggested Fix
Configure UDLD on the interface or globally using the command:

\[\text{[no]}\ udld \text{enable interface <interface name>}\]
\[\text{[no]}\ udld \text{port}\]

You can add, update or remove UDLD state details. You can also change the order of the UDLD state details.
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Group</td>
<td>Group of interfaces to apply the policy. Example valid Values: 'Any', 'AnyEthernet', 'FastEthernet', 'GigabitEthernet', 'FastEthernet0/1', 'FastEthernet0/.*' etc.</td>
<td>Required: true</td>
</tr>
<tr>
<td>Desired state of STP Root Guard</td>
<td>Desired state of UDLD configuration.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

**Note**
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

---

**VLAN 1**

**Description**
Policy to specify whether to use VLAN 1 on switches. Cisco switches use VLAN 1 as the default VLAN to assign to their ports, including their management ports. Additionally, Layer 2 protocols, such as CDP and VTP, need to be sent on a specific VLAN on trunk links, so VLAN 1 was selected. In some cases, VLAN 1 may span the entire network if not appropriately pruned. It also provides attackers easier access and extended reach for their attacks.

**Applicable Platforms**
Cisco IOS Switches

**References**
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 9.2 Page 32 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 1

Rule
Check to make sure VLAN 1 is not used on any access interface [IOS]

Description
This check makes sure none of the interfaces on the switch use VLAN 1 in either ACCESS mode or trunk mode. It also makes sure the VLAN 1 is not used as a native VLAN for the trunk ports.

Applicable Platforms
Cisco IOS Switches

Impact
VLAN 1 may span the entire network if not appropriately pruned. It also provides attackers easier access and extended reach for their attacks.

Suggested Fix
Do not use VLAN 1 for either out-of-band management or in-band management. To provide network-based, out-of-band management, dedicate a physical switch port and VLAN on each switch for management use. Create a Switch Virtual Interface (SVI) Layer Three interface for that VLAN, and connect the VLAN to a dedicated switch and communications path back to the management hosts. Do not allow the operational VLANs access to the management VLAN. Also, do not trunk the management VLAN off the switch. Remove the access to VLAN1 using the command:

```
interface <interface name>
switchport access vlan <any vlan other than 1>
```

Rule 2

Rule
Check to make sure VLAN 1 is not allowed on any trunk interface [IOS]

Description
This check makes sure none of the interfaces on the switch use VLAN 1 in either ACCESS mode or trunk mode. It also makes sure the VLAN 1 is not used as a native VLAN for the trunk ports.

Applicable Platforms
Cisco IOS Switches

Impact
VLAN 1 may span the entire network if not appropriately pruned. It also provides attackers easier access and extended reach for their attacks.

Suggested Fix
Do not use VLAN 1 for either out-of-band management or in-band management. To provide network-based, out-of-band management, dedicate a physical switch port and VLAN on each switch for management use. Create a Switch Virtual Interface (SVI) Layer Three interface for that VLAN, and
connect the VLAN to a dedicated switch and communications path back to the management hosts. Do not allow the operational VLANs access to the management VLAN. Also, do not trunk the management VLAN off the switch. Remove the VLAN1 from the trunks using the command:

```
interface <interface name>
switchport trunk allowed vlan remove 1
```

### Rule 3

**Rule**
Check to make sure VLAN 1 is not allowed on any trunk interface as a native VLAN [IOS]

**Description**
This check makes sure none of the interfaces on the switch use VLAN 1 in either ACCESS mode or trunk mode. It also makes sure the VLAN 1 is not used as a native VLAN for the trunk ports.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
VLAN 1 may span the entire network if not appropriately pruned. It also provides attackers easier access and extended reach for their attacks.

**Suggested Fix**
Do not use VLAN 1 for either out-of-band management or in-band management. To provide network-based, out-of-band management, dedicate a physical switch port and VLAN on each switch for management use. Create a Switch Virtual Interface (SVI) Layer Three interface for that VLAN, and connect the VLAN to a dedicated switch and communications path back to the management hosts. Do not allow the operational VLANs access to the management VLAN. Also, do not trunk the management VLAN off the switch. Remove the VLAN1 from the trunks as a native VLAN using the command:

```
interface <interface name>
switchport trunk allowed vlan remove 1
```

### Rule 4

**Rule**
Check to make sure VLAN 1 is not configured as a voice vlan on any interface [IOS]

**Description**
This check makes sure none of the interfaces on the switch use VLAN 1 in either ACCESS mode or trunk mode. It also makes sure the VLAN 1 is not used as a native VLAN for the trunk ports.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
VLAN 1 may span the entire network if not appropriately pruned. It also provides attackers easier access and extended reach for their attacks.
Understanding Compliance and Audit Manager (CAAM) Policies

Suggested Fix
Do not use VLAN 1 for either out-of-band management or in-band management. To provide network-based, out-of-band management, dedicate a physical switch port and VLAN on each switch for management use. Create a Switch Virtual Interface (SVI) Layer Three interface for that VLAN, and connect the VLAN to a dedicated switch and communications path back to the management hosts. Do not allow the operational VLANs access to the management VLAN. Also, do not trunk the management VLAN off the switch. Change the voice VLAN to something other than 1 using the command:

   interface <interface name>
   switchport voice vlan <any vlan other than 1>

VLAN Trunking Protocols (VTP)

Description
Policy to specify required parameters for VTP

Applicable Platforms
Cisco IOS Switches

References
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 9.4.2 Page 35 of Version 1.0)

The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Rule 1

Rule
Check VTP Mode [IOS]

Description
A switch may be in one of three VTP modes: server, transparent and client. Set the VTP mode to desired state.

Applicable Platforms
Cisco IOS Switches

Impact
Even though VTP simplifies VLAN configuration where large number of VLANs are configured, it may cause some un-authorized switch to become a server and publish a wrong VLAN database.

Suggested Fix
Set the VTP mode to desired value using the command:

   vtp mode
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired Mode of VTP</td>
<td>VTP can operate in different modes. Server-In VTP server mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version and VTP pruning) for the entire VTP domain. VTP servers advertise their VLAN configuration to other network devices in the same VTP domain and synchronize their VLAN configuration with other network devices based on advertisements received over trunk links. VTP server is the default mode. Client?VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client. Transparent?VTP transparent network devices do not participate in VTP. A VTP transparent network device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent network devices do forward VTP advertisements that they receive out their trunking LAN ports.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Rule 2

Rule
Check VTP Pruning State [IOS]

Description
Enable or Disable VTP pruning for VTP servers based on the desired policy.

Applicable Platforms
Cisco IOS Switches

Impact
None

Suggested Fix
Configure VTP pruning for VTP servers using the command:

\[no\] vtp pruning

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired State of VTP Pruning</td>
<td>Desired state of VTP Pruning</td>
<td>Required: true Default: false</td>
</tr>
</tbody>
</table>
Rule 3

Rule
Make sure VTP Domain name is configured [IOS]

Description
This check will make sure VTP domain is configured. By default, all the switches respond to all the VTP messages in the network. By configuring VTP domains, it can be avoided to have mis-configured switch to overwrite the network's VLAN database.

Applicable Platforms
Cisco IOS Switches

Impact
A mis-configured switch that is added to the network can result in overwriting the VLAN database.

Suggested Fix
Configure a pre-defined domain name on all the VTP enabled switches using the command:

```plaintext
[no] vtp domain
```

Rule 4

Rule
Make sure Desired VTP Domain name is configured [IOS]

Description
This check will make sure VTP domain is configured. By default, all the switches respond to all the VTP messages in the network. By configuring VTP domains, it can be avoided to have mis-configured switch to overwrite the network's VLAN database.

Applicable Platforms
Cisco IOS Switches

Impact
A mis-configured switch that is added to the network can result in overwriting the VLAN database.

Suggested Fix
Configure a pre-defined domain name on all the VTP enabled switches using the command:

```plaintext
vtp domain
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Desired VLAN domain name. All the switches within a VLAN domain that want to share VLAN database should be configured with the same domain name.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>
Remote Commands

Description
remote Commands

Applicable Platforms
Cisco IOS Devices

References
Cisco SAFE Compliance
SAFE: A Security Blueprint for Enterprise Networks
Defence Information System Agency (Section NET0740 of Dec 2, 2005)
DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

Rule 1

Rule
Remote copy (RCP) service should be [IOS]

Description
Enforce whether RCP service should be enabled or not

Applicable Platforms
Cisco IOS Devices

Impact
None

Suggested Fix
Configure RCP service using the command:

\textit{no ip remd rcp-enable}

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Remote Copy Service Status</td>
<td>Required: true Default: false</td>
</tr>
</tbody>
</table>

Rule 2

Rule
Remote Shell (RSH) service should be [IOS]

Description
Remote Shell (RSH) service.
Applicable Platforms
Cisco IOS Devices

Impact
None

Suggested Fix
Configure RSH service using the command:

\texttt{no ip rcmd rsh-enable}

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
Rule & Description & Constraints \\
\hline
Status & Remote Shell Service Status & Required: true \\
& & Default: false \\
\hline
\end{tabular}
\end{table}

AAA

Description
By using AAA along with security server, you can control access to routers and other network services from a centralized location. This allows for easier management of user accounts and privileges and provides additional capabilities for auditing of network service usage.

Applicable Platforms
Cisco IOS Devices

References
Information Technology - Code of practice for information security management.

\textbf{Payment Card Industry Data Security Standard(PCI).}(8.3, 8.5 of Version 1.1, September, 2006)
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

\textbf{National Security Agency (NSA) Cisco Router Configuration Guide}(Section 4.1.5 Page 59, Section 4.6 Page 175,176, Section 4.6.2 Page 182, 185 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

\textbf{SANS Router Security Policy}(Section 3.0(1))
The SANS (SysAdmin, Audit, Network, Security) Institute publishes security policy to help system administrators with rapid development and implementation of information security policies.

\textbf{National Security Agency (NSA) Cisco Switch Configuration Guide}(Section 13.2, Page 48 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Cisco SAFE Compliance(1.1b)
SAFE: A Security Blueprint for Enterprise Networks

Control Objectives for Information and Related Technology(P04, DS5 of 4.0)

COBIT (Control Objectives for Information and Related Technology) is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT is a de-facto standard used by most of the auditors when auditing for IT section of Sarbanes-Oxley (SOX) Compliance.

Health Insurance Portability and Accountability Act.(164.308(a)(4)(ii), 164.312(a)(1), 164.312(d))

HIPAA (Health Insurance Portability and Accountability Act.) is designed to protect confidential healthcare information through improved security standards and federal privacy legislation. It defines requirements for storing patient information before, during and after electronic transmission. Centers for Medicare & Medicaid Services (CMS) has provided a Security Rule (45 CFR Part 160 and 164) which is adopted to implement provisions of the HIPAA.

Department of Homeland Security (DHS) Compliance(Section 1.2, Page 8 of Version 2.0)

This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet. Center for Internet Security, Benchmark for Cisco IOS.(Section 1.1.1.1, Page: 6 of Version 2.2, Nov 2007) CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

**Rule 1**

**Rule**
AAA service should be enabled [IOS]

**Description**
By using AAA along with security server, you can control access to routers and other network services from a centralized location. This allows for easier management of user accounts and privileges and provides additional capabilities for auditing of network service usage

**Applicable Platforms**
Cisco IOS Devices

**Impact**
No known impact
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Suggested Fix
Enable AAA configuration using the command:

`aaa new-model`

Rule 2

Rule
Minimum Number of Radius Servers Configured Globally [IOS]

Description
By using AAA along with security server, you can control access to routers and other network services from a centralized location. This allows for easier management of user accounts and privileges and provides additional capabilities for auditing of network service usage.

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Configure required RADIUS servers using the command:

`radius-server host <host name>`

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Radius Servers Configured Globally</td>
<td>Number of minimum Desired Radius Servers to be configured globally.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min Value: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max Value: 2147483647</td>
</tr>
</tbody>
</table>

Rule 3

Rule
Minimum Number of TACACS+ Servers Configured Globally [IOS]

Description
By using AAA along with security server, you can control access to routers and other network services from a centralized location. This allows for easier management of user accounts and privileges and provides additional capabilities for auditing of network service usage.

Applicable Platforms
Cisco IOS Devices
Impact
No known impact.

Suggested Fix
Configure required TACACS servers using the command:

```
tacacs-server host <host name>
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum TACACS+ Servers Configured Globally</td>
<td>Number of minimum Desired TACACS+ Servers to be configured globally.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min Value: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max Value: 2147483647</td>
</tr>
</tbody>
</table>

Rule 4

Rule
Radius Servers should be authenticated [IOS]

Description
This rule checks to make sure all the radius-servers configured on the router are configured with a shared key. This rule does not check to see if each radius-server is actually used in AAA or not. A RADIUS server and a Cisco router use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the router.

Applicable Platforms
Cisco IOS Devices

Impact
Communication between RADIUS server and the device are sent in plain text.

Suggested Fix
Configure RADIUS key using the commands:

```
radius-server key <password>
radius-server <host name> key <Key Name>
```

Rule 5

Rule
TACACS Servers should be authenticated [IOS]
Description
This rule checks to make sure all the tacacs-servers configured on the router are configured with a shared key. This rule does not check to see if each tacacs-server is actually used in AAA or not. A TACACS+ server and a Cisco router use a shared secret text string to encrypt passwords and exchange responses. To configure TACACS+ to use the AAA security commands, you must specify the host running the TACACS+ server daemon and a secret text (key) string that it shares with the router.

Applicable Platforms
Cisco IOS Devices

Impact
Communication between TACACS+ server and the device are sent in plain text.

Suggested Fix
Configure TACACS+ key using the commands:

```
tacacs-server key <password>
tacacs-server <host name> key <Key Name>
```

AAA Accounting - Commands

Description
Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

Commands accounting runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.

Applicable Platforms
Cisco IOS Devices

References
- Information Technology - Code of practice for information security management.
- National Security Agency (NSA) Cisco Router Configuration Guide (Section 4.6, Page 178 of Version 1.1c)
- The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
- National Security Agency (NSA) Cisco Switch Configuration Guide (Section 13.2.3, Page 50 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

**Control Objectives for Information and Related Technology (PO4, DS5 of 4.0)**

COBIT (Control Objectives for Information and Related Technology) is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT is a de-facto standard used by most of the auditors when auditing for IT section of Sarbanes-Oxley (SOX) Compliance.

Center for Internet Security, Benchmark for Cisco IOS.(Section 2.1.1.3, Page:36 of Version 2.2, Nov 2007)

CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

### Rule 1

**Rule**

Minimum Number of TACACS + Server to be used for Commands Accounting [IOS]

**Description**

Cisco IOS Devices

**Applicable Platforms**

Cisco IOS Devices

**Impact**

No known impact.

**Suggested Fix**

Include TACACS+ servers in AAA Commands accounting methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server tacacs+
server <Hostname or A.B.C.D IP address of server >
!
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server >
aaa accounting commands
line vty 0 15
accounting commands
```
Chapter 4 Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 2

Rule
Commands Accounting should include required TACACS + Server [IOS]

Description
This rule checks that required TACACS+ servers are used for Commands Accounting using AAA.

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.

Suggested Fix
Include TACACS+ servers in AAA Commands accounting methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server tacacs+
server <Hostname or A.B.C.D IP address of server >
!
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server >
aaa accounting commands
line vty 0 15
accounting commands
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| No. of Minimum Desired TACACS + Server | Number of minimum Desired TACACS+ Servers to be configured to use for accounting. | Required: true,  
Min Value: 1,  
Max Value: 2147483647 |

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included TACACS + server</td>
<td>List of TACACS+ servers that a device should be configured to use. Using TACACS+ Server Editor option, you can add, remove or update TACACS+ Server details. You can also change the order of the server details.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>
AAA Accounting - Connections

Description
Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

Connection accounting provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.

Applicable Platforms
Cisco IOS Devices

References
Information Technology - Code of practice for information security management.
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.6, Page 178 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 13.2.3, Page 50 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Center for Internet Security, Benchmark for Cisco IOS.(Section 2.1.1.4,Page:37 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.
Rule 1

Rule
Minimum Number of RADIUS Servers to be used for Connection Accounting [IOS]

Description
This rule checks that minimum Number of RADIUS Servers to be used for Connection Accounting

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.

Suggested Fix
Include RADIUS servers in AAA Connection accounting methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server >
aaa accounting connection
line vty 0 15
accounting connection
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Minimum Desired RADIUS Servers</td>
<td>Number of minimum Desired RADIUS Servers to be configured to use for accounting.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min Value: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max Value: 2147483647</td>
</tr>
</tbody>
</table>

Rule 2

Rule
Minimum Number of TACACS+ Servers to be used for Connection Accounting [IOS]

Description
This rule checks that minimum Number of TACACS+ Servers to be used for Connection Accounting

Applicable Platforms
Cisco IOS Devices

No known impact.
Suggested Fix
Include TACACS+ servers in AAA Connection accounting methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server tacacs+
server <Hostname or A.B.C.D IP address of server >
!
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server >
aaa accounting connection
line vty 0 15
accounting connection
```

### Rule 3

**Rule**
Connection Accounting should include required RADIUS Servers [IOS]

**Description**
This rule checks that connection Accounting should include required RADIUS Servers

**Applicable Platforms**
Cisco IOS Devices

**Impact**
No known impact.

**Suggested Fix**
Include RADIUS servers in AAA Connection accounting methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server >
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server >
aaa accounting connection
line vty 0 15
accounting connection
```
Understanding Compliance and Audit Manager (CAAM) Policies

Rule 4

Rule
Connection Accounting should include required TACACS+ Servers [IOS]

Description
This rule checks that connection Accounting should include required TACACS+ Servers

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.

Suggested Fix
Include TACACS+ servers in AAA Connection accounting methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server tacacs+
server <Hostname or A.B.C.D IP address of server >
!
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server >
aaa accounting connection
line vty 0 15
accounting connection
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included RADIUS Servers</td>
<td>List of RADIUS servers that a device should be configured to use.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td>Using RADIUS Server Editor option, you can add, remove or update RADIUS Server details. You can also change the order of the server details.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include TACACS+ Servers</td>
<td>List of TACACS+ servers that a device should be configured to use.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td>Using TACACS+ Server Editor option, you can add, remove or update TACACS+ Server details. You can also change the order of the server details.</td>
<td></td>
</tr>
</tbody>
</table>
AAA Accounting - Exec

Description
Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

EXEC accounting provides information about user EXEC terminal sessions (user shells) on the network access server, including username, date, start and stop times, the access server IP address, and (for dial-in users) the telephone number the call originated from.

Applicable Platforms
Cisco IOS Devices

References
Information Technology - Code of practice for information security management.
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.6, Page 178 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 13.2.3, Page 50 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Center for Internet Security, Benchmark for Cisco IOS.(Section 2.1.1.5,Page:37 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.
Rule 1

**Rule**
Minimum Number of RADIUS Servers to be used for EXEC Accounting [IOS]

**Description**
This rule checks that minimum Number of RADIUS Servers to be used for EXEC Accounting

**Applicable Platforms**
Cisco IOS Devices

**Impact**
No known impact.

**Suggested Fix**
Include RADIUS servers in AAA EXEC accounting methods which are used in the line configuration

```
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server >
aaa accounting exec
line vty 0 15
accounting exec
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Number of Minimum Desired RADIUS Servers | Number of minimum Desired RADIUS Servers to be configured to use for accounting. | Required: true
|                               |                                                                             | Min Value: 1
|                               |                                                                             | Max Value: 2147483647     |

Rule 2

**Rule**
Minimum Number of TACACS+ Servers to be used for EXEC Accounting [IOS]

**Description**
This rule checks that minimum Number of TACACS+ Servers to be used for EXEC Accounting

**Applicable Platforms**
Cisco IOS Devices

**Impact**
No known impact.
Suggested Fix
Include TACACS+ servers in AAA EXEC accounting methods which are used in the line configuration

```
aaa new-model
aaa group server tacacs+
server <Hostname or A.B.C.D IP address of server >
!
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server >
aaa accounting exec
line vty 0 15
accounting exec
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Minimum Desired TACACS+ Servers</td>
<td>Number of minimum Desired TACACS+ Servers to be configured to use for accounting.</td>
<td>Required: true Min Value: 1</td>
</tr>
</tbody>
</table>

Rule 3

Rule
EXEC Accounting should include required RADIUS Servers [IOS]

Description
This rule checks that EXEC Accounting should include required RADIUS Servers

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.

Suggested Fix
Include RADIUS servers in AAA EXEC accounting methods which are used in the line configuration

```
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server >
aaa accounting exec
line vty 0 15
accounting exec
```
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 4

Rule
EXEC Accounting should include required TACACS+ Servers [IOS]

Description
This rule checks that EXEC Accounting should include required TACACS+ Servers

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.

Suggested Fix
Include TACACS+ servers in AAA EXEC accounting methods which are used in the line configuration

```
aaa new-model
aaa group server tacacs+
server <Hostname or A.B.C.D IP address of server >
!
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server >
aaa accounting exec
line vty 0 15
accounting exec
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include RADIUS Servers</td>
<td>List of RADIUS servers that a device should be configured to use.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td>Using RADIUS Server Editor option, you can add, remove or update RADIUS Server details. You can also change the order of the server details.</td>
<td></td>
</tr>
<tr>
<td>Include TACACS+ Servers</td>
<td>List of TACACS+ servers that a device should be configured to use.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td>Using TACACS+ Server Editor option, you can add, remove or update TACACS+ Server details. You can also change the order of the server details.</td>
<td></td>
</tr>
</tbody>
</table>
AAA Accounting - Network

Description
Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

Network accounting provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.

Applicable Platforms
Cisco IOS Devices

References
Information Technology - Code of practice for information security management.
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.6, Page 178 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 13.2.3, Page 50 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Center for Internet Security, Benchmark for Cisco IOS.(Section 2.1.1.6,Page:38 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.
Rule 1

Rule
Minimum Number of RADIUS Servers to be used for Network Accounting [IOS]

Description
This rule checks that minimum Number of RADIUS Servers to be used for Network Accounting

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Include RADIUS servers in AAA network accounting methods which are used in the line configuration

```
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server >

aaa accounting network

line vty 0 15

accounting network
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Minimum Desired RADIUS Servers</td>
<td>Number of minimum Desired RADIUS Servers to be configured to use for accounting</td>
<td>Required: true Min Value: 1 Max Value: 2147483647</td>
</tr>
</tbody>
</table>

Rule 2

Rule
Minimum Number of TACACS+ Servers to be used for Network Accounting [IOS]

Description
This rule checks that minimum Number of TACACS+ Servers to be used for Network Accounting

Applicable Platforms
Cisco IOS Devices

Impact
No known impact
**Chapter 4  Using Compliance and Audit Manager Feature**

**Understanding Compliance and Audit Manager (CAAM) Policies**

---

**Suggested Fix**

Include TACACS+ servers in AAA network accounting methods which are used in the line configuration:

```plaintext
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>

! tacacs-server host <Hostname or A.B.C.D IP address of RADIUS server >

aaa accounting network
line vty 0 15
accounting network
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Minimum Desired TACACS+ Servers</td>
<td>Number of minimum Desired TACACS+ Servers to be configured to use for accounting</td>
<td>Required: true, Min Value: 1, Max Value: 2147483647</td>
</tr>
</tbody>
</table>

---

**Rule 3**

**Rule**

Network Accounting should include required RADIUS Servers [IOS]

**Description**

This rule checks that network Accounting should include required RADIUS Servers

**Applicable Platforms**

Cisco IOS Devices

**Impact**

No known impact

**Suggested Fix**

Include RADIUS servers in AAA network accounting methods which are used in the line configuration:

```plaintext
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>

! radius-server host <Hostname or A.B.C.D IP address of RADIUS server >

aaa accounting network
line vty 0 15
accounting network
```
Understanding Compliance and Audit Manager (CAAM) Policies

Chapter 4     Using Compliance and Audit Manager Feature

Rule

Network Accounting should include required TACACS+ Servers [IOS]

Description
This rule checks that network Accounting should include required TACACS+ Servers

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Include TACACS+ servers in AAA network accounting methods which are used in the line configuration

```
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
tacacs-server host <Hostname or A.B.C.D IP address of RADIUS server >

aaa accounting network
line vty 0 15
accounting network
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included RADIUS Servers</td>
<td>List of RADIUS servers that a device should be configured to use.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td>Using RADIUS Server Editor option, you can add, remove or update RADIUS Server details. You can also change the order of the server details.</td>
<td></td>
</tr>
<tr>
<td>Included TACACS+ Servers</td>
<td>List of TACACS+ servers that a device should be configured to use.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td>Using TACACS+ Server Editor option, you can add, remove or update TACACS+ Server details. You can also change the order of the server details.</td>
<td></td>
</tr>
</tbody>
</table>
AAA Accounting - System

Description
Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

System accounting provides information about all system-level events (for example, when the system reboots or when accounting is turned on or off).

Applicable Platforms
Cisco IOS Devices

References
Information Technology - Code of practice for information security management.
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.6, Page 178 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 13.2.3, Page 50 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Center for Internet Security, Benchmark for Cisco IOS.(Section 2.1.1.7,Page:38 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 1

Rule
Minimum Number of RADIUS Servers to be used for System Accounting [IOS]

Description
This rule checks minimum Number of RADIUS Servers to be used for System Accounting

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Include RADIUS servers in AAA system accounting methods which are used in the line configuration

```
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server >

aaa accounting system
line vty 0 15
accounting system
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Minimum Desired RADIUS Servers</td>
<td>Number of minimum Desired RADIUS Servers to be configured to use for accounting</td>
<td>Required: true Min Value: 1 Max Value: 2147483647</td>
</tr>
</tbody>
</table>

Rule 2

Rule
Minimum Number of TACACS+ Servers to be used for System Accounting [IOS]

Description
This rule checks minimum Number of TACACS+ Servers to be used for System Accounting

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Include TACACS+ servers in AAA system accounting methods which are used in the line configuration
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
tacacs-server host <Hostname or A.B.C.D IP address of RADIUS server>
aaa accounting system
line vty 0 15
accounting system

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Number of Minimum Desired TACACS+ Servers | Number of minimum Desired TACACS+ Servers to be configured to use for accounting. | Required: true
Min Value: 1
Max Value: 2147483647 |

Rule 3

Rule
System Accounting should include required RADIUS Servers [IOS]

Description
This rule checks that system Accounting should include required RADIUS Servers

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.

Suggested Fix
Include RADIUS servers in AAA system accounting methods which are used in the line configuration
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server>
aaa accounting system
line vty 0 15
accounting system
Rule 4

Rule
System Accounting should include required TACACS+ Servers [[IOS]

Description
This rule checks that system Accounting should include required TACACS+ Servers

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Include TACACS+ servers in AAA system accounting methods which are used in the line configuration

```
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
tacacs-server host <Hostname or A.B.C.D IP address of RADIUS server >

aaa accounting system
line vty 0 15
accounting system
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included RADIUS Servers</td>
<td>List of RADIUS servers that a device should be configured to use.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td>Using RADIUS Server Editor option, you can add, remove or update RADIUS Server details. You can also change the order of the server details.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Included TACACS+ Servers</td>
<td>List of TACACS+ servers that a device should be configured to use.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td>Using TACACS+ Server Editor option, you can add, remove or update TACACS+ Server details. You can also change the order of the server details.</td>
<td></td>
</tr>
</tbody>
</table>
AAA Authentication - Enable

Description
By using AAA along with security server, you can control access to routers and other network services from a centralized location. This allows for easier management of user accounts and privileges and provides additional capabilities for auditing of network service usage. Enable authentication specifies a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level.

Applicable Platforms
Cisco IOS Devices

References
Information Technology - Code of practice for information security management.
Center for Internet Security, Benchmark for Cisco IOS. (Section 1.1.1.3, Page: 7; Section 2.1.1.1, Page: 35 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

Rule 1

Rule
Minimum Number of RADIUS Servers to be used for Enable Authentication [IOS]

Description
This rule checks minimum Number of RADIUS Servers to be used for Enable Authentication

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Include RADIUS servers in AAA Enable Authentication methods using the commands

aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server>

aaa authentication enable
Rule 2

Rule
Minimum Number of TACACS+ Servers to be used for Enable Authentication [IOS]

Description
This rule checks that minimum Number of TACACS+ Servers to be used for Enable Authentication

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.

Suggested Fix
Include TACACS+ servers in AAA Enable Authentication methods using the commands

```
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
tacacs-server host <Hostname or A.B.C.D IP address of RADIUS server >
aaa authentication enable
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Minimum Desired RADIUS Servers</td>
<td>Number of minimum Desired RADIUS Servers to be configured to use for Authentication</td>
<td>Required: true, Min Value: 1, Max Value: 2147483647</td>
</tr>
<tr>
<td>Number of Minimum Desired TACACS+ Servers</td>
<td>Number of minimum Desired TACACS+ Servers to be configured to use for Authentication</td>
<td>Required: true, Min Value: 1, Max Value: 2147483647</td>
</tr>
</tbody>
</table>
Rule 3

Rule
Enable Authentication should include required RADIUS Servers [IOS]

Description
This rule checks that enable Authentication should include required RADIUS Servers

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.

Suggested Fix
Include RADIUS servers in AAA Enable Authentication methods using the commands

`aaa new-model`
`aaa group server radius
server <Hostname or A.B.C.D IP address of server>
`
`radius-server host <Hostname or A.B.C.D IP address of RADIUS server >`
`aaa authentication enable`

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included RADIUS Servers</td>
<td>List of RADIUS servers that a device should be configured to use. Using RADIUS Server Editor option, you can add, remove or update RADIUS Server details. You can also change the order of the server details.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Rule 4

Rule
Enable Authentication should include required TACACS+ Servers [IOS]

Description
This rule checks that enable Authentication should include required RADIUS Servers

Applicable Platforms
Cisco IOS Devices

Impact
No known impact
Suggested Fix
Include TACACS+ servers in AAA Enable Authentication methods using the commands

```
 aaa new-model
 aaa group server radius
 server <Hostname or A.B.C.D IP address of server>
 !
 tacacs-server host <Hostname or A.B.C.D IP address of RADIUS server >
 aaa authentication enable
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included TACACS+ Servers</td>
<td>List of TACACS+ servers that a device should be configured to use. Using TACACS+ Server Editor option, you can add, remove or update TACACS+ Server details. You can also change the order of the server details.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

**Rule 5**

Rule
Check for Usage of “none” in Enable Authentication

Description
This rule checks for usage of "none" in Enable Authentication

Applicable Platforms
Cisco IOS Devices

Impact
If none keyword is used at the end of an AAA Method, authentication is granted if none of the other authentication methods are available. In this case, users are able to pass authentication even without any credentials under circumstances where there are no AAA servers available. If this none keyword is not used, then it is possible to be locked out of the device when none of the AAA servers are available.

Suggested Fix
Add/remove the none keyword as per the requirement using the command:

```
 aaa new-model
 aaa authentication enable [none]
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage of “none” for method</td>
<td>Desired usage of &quot;none&quot; key word in the methods. If this keyword is used, authentication is successfull if none of the previous methods are available.</td>
<td>Required: true Default: false</td>
</tr>
</tbody>
</table>
AAA Authentication - Login

Description
By using AAA along with security server, you can control access to routers and other network services from a centralized location. This allows for easier management of user accounts and privileges and provides additional capabilities for auditing of network service usage. Login authentication specifies a series of authentication methods that are used to determine whether a user can access network device.

Applicable Platforms
Cisco IOS Devices

References
Information Technology - Code of practice for information security management.
Payment Card Industry Data Security Standard(PCI).(8.3, 8.5 of Version 1.1, September, 2006)
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.1.5 Page 59, Section 4.6 Page 175,176, Section 4.6.2 Page 182, 185 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
SANS Router Security Policy(Section 3.0(1))
The SANS (SysAdmin, Audit, Network, Security) Institute publishes security policy to help system administrators with rapid development and implementation of information security policies.
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 13.2, Page 48 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Cisco SAFE Compliance(1.1b)
SAFE: A Security Blueprint for Enterprise Networks
Control Objectives for Information and Related Technology(PO4, DS5 of 4.0)
COBIT (Control Objectives for Information and Related Technology) is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT is a de-facto standard used by most of the auditors when auditing for IT section of Sarbanes-Oxley (SOX) Compliance.
Health Insurance Portability and Accountability Act (164.308(a)(4)(ii), 164.312(a)(1), 164.312(d))

HIPAA (Health Insurance Portability and Accountability Act) is designed to protect confidential healthcare information through improved security standards and federal privacy legislation. It defines requirements for storing patient information before, during and after electronic transmission. Centers for Medicare & Medicaid Services (CMS) has provided a Security Rule (45 CFR Part 160 and 164) which is adopted to implement provisions of the HIPAA.

Defence Information System Agency (Section NET0430 of Dec 2, 2005)

DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

Department of Homeland Security (DHS) Compliance (Section 1.2, Page 8 of Version 2.0)

This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Center for Internet Security, Benchmark for Cisco IOS (Section 1.1.1.2, Page: 7; Section 2.1.1.2, Page: 36 of Version 2.2, Nov 2007)

CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

**Rule 1**

**Rule**
Minimum Number of RADIUS Servers to be used for User Authentication [IOS]

**Description**
By using AAA along with security server, you can control access to routers and other network services from a centralized location. This allows for easier management of user accounts and privileges and provides additional capabilities for auditing of network service usage.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
No known impact

**Suggested Fix**
Include RADIUS servers in AAA login authentication methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>

!```

radius-server host <Hostname or A.B.C.D IP address of RADIUS server >

aaa authentication login

line vty 0 15

login authentication

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Number of Minimum Desired RADIUS Servers | Number of minimum Desired Radius Servers to be configured to use for authentication. | Required: true  
Min Value: 1  
Max Value: 2147483647 |

**Rule 2**

**Rule**
Minimum Number of TACACS+ Servers to be used for User Authentication [IOS]

**Description**
By using AAA along with security server, you can control access to routers and other network services from a centralized location. This allows for easier management of user accounts and privileges and provides additional capabilities for auditing of network service usage.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
No known impact

**Suggested Fix**
Include TACACS+ servers in AAA login authentication methods which are used in the line configuration using the commands:

```shell
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
tacacs-server host <Hostname or A.B.C.D IP address of RADIUS server >

aaa authentication login

line vty 0 15

login authentication
```
**Rule 3**

**Rule**
Authentication method should not contain “none” at the end [IOS]

**Description**
AAA authentication login method should not contain none at the end.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
User may be able to login into the device without proper user name and password under situation when other authentication methods are not available for whatever reason.

**Suggested Fix**
Remove none keyword at the end of authentication method in the command:

```
 aaa new-model
 aaa authentication login [none]
```
Suggested Fix
Include RADIUS or TACACS+ servers in AAA login authentication methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server <tacacs+|radius>
aaa authentication login
line vty 0 15
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included RADIUS Servers</td>
<td>List of RADIUS servers that a device should be configured to use. Using RADIUS Server Editor option, you can add, remove or update RADIUS Server details. You can also change the order of the server details.</td>
<td>Required: false</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included TACACS+ Servers</td>
<td>List of TACACS+ servers that a device should be configured to use. Using TACACS+ Server Editor option, you can add, remove or update TACACS+ Server details. You can also change the order of the server details.</td>
<td>Required: false</td>
</tr>
</tbody>
</table>

Rule 5

Rule
All authentication methods should ask Username and Password [IOS]

Description
It is always important to choose the right order for the methods on a method list for 'AAA authentication'. For AAA login authentication, the first method on the list determines whether the user will be prompted for a username. Methods requiring only a password (e.g. the line method) should never be placed ahead of methods requiring both username and password, because the user will never be prompted for a username and the mechanism will always fail.

Applicable Platforms
Cisco IOS Devices

Impact
If the authentication method does not ask for username and password, all subsequent authentication methods in the list will fail.
Suggested Fix
Re-arrange the order of aaa authentication methods so that enable and line are always at the end in the command:

```
  aaa new-model
  aaa authentication login
```

Rule 6

Rule
At least one local username should be defined if “local” or “local-case” is used in AAA Authentication login methods [IOS]

Description
AAA authentication login method local uses local username database to authenticate users. If there is no username configured in the database, using local is not useful.

Applicable Platforms
Cisco IOS Devices

Impact
none

Suggested Fix
Add some users to the local username database using the command:

```
username <user name>
```

Rule 7

Rule
AAA Authentication login methods should include “local” or “local-case” [IOS]

Description
AAA authentication login methods should include local or local-case. Including local or local-case on your method list will guarantee that if the security server(s) is not available, administrators will still be able to gain remote access by using a username and password defined locally on the router.

Applicable Platforms
Cisco IOS Devices

Impact
If all the security servers are down and can not authenticate users, there will be no way to gain access to the router
Suggested Fix
Add local username database as an authentication mechanism using the command:

```
aaa new-model
aaa authentication login <list of groups> local
```

AAA Authorization - Commands

Description
AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it. Commands authorization applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.

Applicable Platforms
Cisco IOS Devices

References
Information Technology - Code of practice for information security management.
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.6, Page 177 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 13.2.2, Page 50 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Health Insurance Portability and Accountability Act.(164.308(a)(3)(ii))
HIPAA (Health Insurance Portability and Accountability Act.) is designed to protect confidential healthcare information through improved security standards and federal privacy legislation. It defines requirements for storing patient information before, during and after electronic transmission. Centers for Medicare & Medicaid Services (CMS) has provided a Security Rule (45 CFR Part 160 and 164) which is adopted to implement provisions of the HIPAA.
Rule 1

**Rule**
Minimum Number of TACACS+ Servers to be used for Commands Authorization [IOS]

**Description**
This rule checks that minimum number of TACACS+ Servers are used for Commands Authorization using AAA

**Applicable Platforms**
Cisco IOS Devices

**Impact**
No known impact

**Suggested Fix**
Include TACACS+ servers in AAA Commands Authorization methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server tacacs+
server <Hostname or A.B.C.D IP address of server >
!
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server >
aaa authorization commands
```

<table>
<thead>
<tr>
<th>Rule Description Constraints</th>
<th>Number of Minimum Desired TACACS+ Servers to be configured to use for authorization.</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required: true</td>
<td>Min Value: 1</td>
<td>Max Value: 2147483647</td>
</tr>
</tbody>
</table>

Rule 2

**Rule**
Commands Authorization should include Required TACACS+ Servers [IOS]

**Description**
This rule checks that required TACACS+ Servers are used for Commands Authorization using AAA

**Applicable Platforms**
Cisco IOS Devices

**Impact**
No known impact.
Suggested Fix
Include TACACS+ servers in AAA Commands Authorization methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server tacacs+
server <Hostname or A.B.C.D IP address of server >
!
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server >
aaa authorization commands
line vty 0 15
authorization commands
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included TACACS+ Servers</td>
<td>List of TACACS+ servers that a device should be configured to use.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td>Using TACACS+ Server Editor option, you can add, remove or update TACACS+ Server details. You can also change the order of the server details.</td>
<td></td>
</tr>
</tbody>
</table>

AAA Authorization - Configuration

Description
AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it. Configuration authorization applies to downloading configurations from the AAA server.

Applicable Platforms
Cisco IOS Devices

References
Information Technology - Code of practice for information security management.
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.6, Page 177 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
National Security Agency (NSA) Cisco Switch Configuration Guide (Section 13.2.2, Page 50 of Version 1.0)

The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Rule 1

Rule
Minimum Number of RADIUS Servers to be used for Configuration Authorization [IOS]

Description
This rule checks that minimum Number of RADIUS Servers to be used for Configuration Authorization

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Include RADIUS servers in AAA Configuration Authorization methods which are used in the line configuration using the commands:

```plaintext
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server>
aaa authorization configuration
line vty 0 15
authorization configuration
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Minimum Desired RADIUS Servers</td>
<td>Number of minimum Desired RADIUS Servers to be configured to use for authorization.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min Value: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max Value: 2147483647</td>
</tr>
</tbody>
</table>
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 2

Rule
Minimum Number of TACACS+ Servers to be used for Configuration Authorization [IOS]

Description
This rule checks that minimum Number of TACACS+ Servers to be used for Configuration Authorization

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.

Suggested Fix
Include TACACS+ servers in AAA Configuration Authorization methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server tacacs+
server <Hostname or A.B.C.D IP address of server >
!
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server >
aaa authorization configuration
line vty 0 15
authorization configuration
```

<table>
<thead>
<tr>
<th>Rule Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Minimum Desired TACACS+ Servers</td>
<td>Required: true Min Value: 1 Max Value: 2147483647</td>
</tr>
<tr>
<td>Number of minimum Desired TACACS+ Servers to be configured to use for authorization.</td>
<td></td>
</tr>
</tbody>
</table>

Rule 3

Rule
Configuration Authorization should include required RADIUS Servers [IOS]

Description
This rule checks that configuration Authorization should include required RADIUS Servers

Applicable Platforms
Cisco IOS Devices
Impact
No known impact.

Suggested Fix
Include RADIUS servers in AAA Configuration Authorization methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server radius
  server <Hostname or A.B.C.D IP address of server>
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server>
  aaa authorization configuration
  line vty 0 15
```

Rule 4

Rule
Configuration Authorization should include required TACACS+ Servers [IOS]

Description
This rule checks that configuration Authorization should include required TACACS+ Servers

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Include TACACS+ servers in AAA Configuration Authorization methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server tacacs+
  server <Hostname or A.B.C.D IP address of server>
```
Understanding Compliance and Audit Manager (CAAM) Policies

```
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server >
aaa authorization configuration
line vty 0 15
authorization configuration
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included TACACS+ Servers</td>
<td>List of TACACS+ servers that a device should be configured to use. Using TACACS+ Server Editor option, you can add, remove or update TACACS+ Server details. You can also change the order of the server details.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

### AAA Authorization - EXEC

#### Description

AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it. EXEC authorization applies to the attributes associated with a user EXEC terminal session.

#### Applicable Platforms

Cisco IOS Devices

#### References

  - Information Technology - Code of practice for information security management.
- National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.6, Page 177 of Version 1.1c)
  - The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
- National Security Agency (NSA) Cisco Switch Configuration Guide(Section 13.2.2, Page 50 of Version 1.0)
  - The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Rule 1

**Rule**
Minimum Number of RADIUS Servers to be used for EXEC Authorization [IOS]

**Description**
This rule checks that minimum Number of RADIUS Servers to be used for EXEC Authorization

**Applicable Platforms**
Cisco IOS Devices

**Impact**
No known impact.

**Suggested Fix**
Include RADIUS servers in AAA EXEC Authorization methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server>

aaa authorization exec
line vty 0 15
authorization exec
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Minimum Desired RADIUS Servers</td>
<td>Number of minimum Desired RADIUS Servers to be configured to use for authorization.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min Value: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max Value: 2147483647</td>
</tr>
</tbody>
</table>

Rule 2

**Rule**
Minimum Number of TACACS+ Servers to be used for EXEC Authorization [IOS]

**Description**
This rule checks that minimum Number of TACACS+ Servers to be used for EXEC Authorization

**Applicable Platforms**
Cisco IOS Devices
Impact
No known impact.

Suggested Fix
Include TACACS+ servers in AAA EXEC Authorization methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server tacacs+
server <Hostname or A.B.C.D IP address of server>
!
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server>
aaa authorization exec
line vty 0 15
authorization exec
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Minimum Desired TACACS+ Servers</td>
<td>Number of minimum Desired TACACS+ Servers to be configured to use for authorization.</td>
<td>Required: true&lt;br&gt;Min Value: 1&lt;br&gt;Max Value: 2147483647</td>
</tr>
</tbody>
</table>

Rule 3

Rule
EXEC Authorization should include required RADIUS Servers [IOS]

Description
This rule checks that EXEC Authorization should include required RADIUS Servers

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.

Suggested Fix
Include RADIUS servers in AAA EXEC Authorization methods which are used in the line configuration using the commands:

```
aaa new-model aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server>
aaa authorization exec
```
line vty 0 15
authorization exec

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included RADIUS Servers</td>
<td>List of RADIUS servers that a device should be configured to use. Using RADIUS Server Editor option, you can add, remove or update RADIUS Server details. You can also change the order of the server details.</td>
<td>Required: true</td>
</tr>
<tr>
<td>Included TACACS+ Servers</td>
<td>List of TACACS+ servers that a device should be configured to use.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

**Rule 4**

**Rule**
EXEC Authorization should include required TACACS+ Servers [IOS]

**Description**
This rule checks that EXEC Authorization should include required TACACS+ Servers

**Applicable Platforms**
Cisco IOS Devices

**Impact**
No known impact

**Suggested Fix**
Include TACACS+ servers in AAA EXEC Authorization methods which are used in the line configuration using the commands:

```
aaa new-model
aaa group server tacacs+
server <Hostname or A.B.C.D IP address of server >
!
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server >
aaa authorization exec
line vty 0 15
authorization exec
```
AAA Authorization - Network

Description
AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it. Network authorization applies to network connections. This can include a PPP, SLIP, or ARAP connection.

Applicable Platforms
Cisco IOS Devices

References
Information Technology - Code of practice for information security management.
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.6, Page 177 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 13.2.2, Page 50 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Rule 1

Rule
Minimum Number of RADIUS Servers to be used for Network Authorization [IOS]

Description
This rule checks that minimum Number of RADIUS Servers to be used for Network Authorization

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.
Suggested Fix
Include RADIUS servers in AAA Network Authorization methods which are used in the line configuration using the commands:

`aaa new-model`
`aaa group server radius`  
`server <Hostname or A.B.C.D IP address of server>`  
`radius-server host <Hostname or A.B.C.D IP address of RADIUS server>`
`aaa authorization network`
`line vty 0 15`
`authorization network`

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Number of Minimum Desired RADIUS Servers | Number of minimum Desired TACACS+ Servers to be configured to use for authorization. | Required: true  
Min Value: 1  
Max Value: 2147483647 |

Rule 2

Rule
Minimum Number of TACACS+ Servers to be used for Network Authorization [IOS]

Description
This rule checks that minimum Number of TACACS+ Servers to be used for Network Authorization

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.

Suggested Fix
Include TACACS+ servers in AAA Network Authorization methods which are used in the line configuration using the commands:

`aaa new-model`
`aaa group server tacacs+`  
`server <Hostname or A.B.C.D IP address of server>`  
`!`
Rule 3

Rule
Network Authorization should include required RADIUS Servers [IOS]

Description
This rule checks that network Authorization should include required RADIUS Servers

Applicable Platforms
Cisco IOS Devices

Impact
No known impact.

Suggested Fix
Include RADIUS servers in AAA Network Authorization methods which are used in the line configuration using the commands:

```plaintext
aaa new-model
aaa group server radius
server <Hostname or A.B.C.D IP address of server>
!
radius-server host <Hostname or A.B.C.D IP address of RADIUS server>
aaa authorization
network line vty 0 15
authorization network
```
Rule 4

Rule
Network Authorization should include required TACACS+ Servers [IOS]

Description
This rule checks that network Authorization should include required TACACS+ Servers

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Include TACACS+ servers in AAA Network Authorization methods which are used in the line configuration using the commands:

```plaintext
aaa new-model
aaa group server tacacs+
server <Hostname or A.B.C.D IP address of server >
!
tacacs-server host <Hostname or A.B.C.D IP address of TACACS server >
aaa authorization network
line vty 0 15
authorization network
```

Rule Description Constraints
Included RADIUS Servers
List of RADIUS servers that a device should be configured to use.
Using RADIUS Server Editor option, you can add, remove or update RADIUS Server details. You can also change the order of the server details.
Required: true
Control Plane Policing

Description
Policies related to Control Plane Policing. Control Plane Policing (CoPP) is a Cisco IOS feature that you can employ to counter resource starvation-based DoS attacks that target the central processor of a router (control plane and management plane). CPP protects the central processor via policies that filter or rate limit traffic directed to the processor. The Control Plane Policing feature allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

Applicable Platforms
Cisco IOS Devices With CoPP Capability

References
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.3.7 Page 98 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Rule 1

Rule
Check input Control Plane Policy is configured [IOS]

Description
This rule checks to make sure that a Control Plane Policy is configured in input direction. The Control Plane Policing feature allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

Applicable Platforms
Cisco IOS Devices With CoPP Capability

Impact
There is no classification of the data that needs to be handled by the device's central processor, and hence is not protected from various DDoS attacks
Suggested Fix
Configure Control Plane Policing using the commands

```
control-plane
service-policy input <policy name>
exit
```

---

**Rule 2**

**Rule**
Check output Control Plane Policy is configured [IOS]

**Description**
This rule checks to make sure that a Control Plane Policy is configured in output direction. The Control Plane Policing feature allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

**Applicable Platforms**
Cisco IOS Devices With CoPP Capability

**Impact**
There is no classification of the data that needs to be handled by the device’s central processor, and hence is is not protected from various DDoS attacks

**Suggested Fix**
Configure Control Plane Policing using the commands

```
control-plane
service-policy output <policy name>
exit
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of desired output policy</td>
<td>Desired output policy Name (Leave this blank if you dont want to check any specific policy name)</td>
<td>Required: false</td>
</tr>
</tbody>
</table>
HTTP Server

Description
HTTP Server allows web based remote administration of the router.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices
Cisco IOS Devices With HTTPS Capability

References
Payment Card Industry Data Security Standard(PCI).(2.3 of Version 1.1, September, 2006)
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

National Security Agency (NSA) Cisco Router Configuration Guide(Section 8.1(16) Page 278, Section 4.2.1 Page 71, Section 4.2.2 Page 73,74 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Information Technology - Code of practice for information security management.

National Security Agency (NSA) Cisco Switch Configuration Guide(Section 6.2.2, Page 18 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Cisco SAFE Compliance(1.1b)
SAFE: A Security Blueprint for Enterprise Networks

Health Insurance Portability and Accountability Act.(164.312(a)(1), 164.312(e)(1))
HIPAA (Health Insurance Portability and Accountability Act.) is designed to protect confidential healthcare information through improved security standards and federal privacy legislation. It defines requirements for storing patient information before, during and after electronic transmission. Centers for Medicare & Medicaid Services (CMS) has provided a Security Rule (45 CFR Part 160 and 164) which is adopted to implement provisions of the HIPAA.

SANS Router Security Policy(3.0(3f))
The SANS (SysAdmin, Audit, Network, Security) Institute publishes security policy to help system administrators with rapid development and implementation of information security policies.
Defence Information System Agency (Section NET0740 of Dec 2, 2005)

DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

Department of Homeland Security (DHS) Compliance (Section 4.3, Page 27 of Version 2.0)

This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Center for Internet Security, Benchmark for Cisco PIX/ASA, (Section 1.2.2.2, Page: 19 of Version 2.0, Nov 2007)

CIS PIX/ASA benchmark recommends the prudent level of minimum due care for operating system security. CIS PIX/ASA benchmark contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All PIX devices should implement these settings.

Center for Internet Security, Benchmark for Cisco IOS, (Section 1.1.2.5, Page: 24 of Version 2.2, Nov 2007)

CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

**Rule 1**

**Rule**

Check state of HTTP server [IOS]

**Description**

HTTP Server allows web based remote administration of the router. It is useful primarily when intervening routers or firewalls prevent use of Telnet for that purpose. However, it is important to note that both Telnet and web-based remote administration reveal critical passwords in clear text. Further, web-based administration imposes the requirement that users log in at full (level 15) privilege. Therefore, web-based remote administration should be avoided

**Applicable Platforms**

Cisco IOS Devices

**Impact**

Can be exploited to access the router.

**Suggested Fix**

Configure HTTP server using the command

```
[no] ip http server
```
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 2

Rule
Check HTTP server port value [IOS]

Description
TCP port number that the HTTP server listens on.

Applicable Platforms
Cisco IOS Devices

Impact
HTTP Server may not be accessible if the port is not configured properly

Suggested Fix
Configure port for HTTP server using the command

ip http port <port number>

Rule 3

Rule
Check state of HTTP Secure (HTTPS) server [PIX, ASA, IOS]

Description
HTTP Server allows web based remote administration of the router. It is useful primarily when
intervening routers or firewalls prevent use of Telnet for that purpose. However, it is important to note
that both Telnet and web-based remote administration reveal critical passwords in clear text. Further,
web-based administration imposes the requirement that users log in at full (level 15) privilege.
Therefore, web-based remote administration should be avoided, then it is preferable

Applicable Platforms
Cisco PIX Devices Running >= 7.x and ASA devices Cisco IOS Devices With HTTPS Capability

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Status</td>
<td>HTTP server status</td>
<td>Required: true Default: false</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port for HTTP server</td>
<td>Required: true Default: 80 Min Value: 1025 Max Value: 65535</td>
</tr>
</tbody>
</table>
Impact
Can be exploited to access the router.

Suggested Fix
Configure HTTPS server using the command
[n] ip http secure-server (for IOS)
[n] http server enable (for PIX)

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Secure Server Status  | HTTP Secured server status| Required: true
                              |                         | Default: false          |

Rule 4

Rule
Check HTTP Secure (HTTPS) server port value [PIX, ASA, IOS]

Description
TCP port number that the HTTP Secure server listens on.

Applicable Platforms
Cisco PIX Devices Running >= 7.x and ASA devices
Cisco IOS Devices With HTTPS Capability

Impact
HTTPS Server may not be accessible if the port is not configured properly

Suggested Fix
Configure port for HTTPS server using the command
ip http secure-port <port number>(for IOS)
http server enable <port number>(for PIX)

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Secure Server Port (IOS)    | Port for HTTP Secured server | Required: false
                              | Default: 443 Min Value: 1025 Max Value: 65535 |
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 5

Rule
ACL must be configured for restricting access to HTTP server [IOS]

Description
If web-based remote administration is required, HTTP server should be enabled and access must be restricted to the trusted users.

Applicable Platforms
Cisco IOS Devices

Impact
Unauthorized users may gain access if not restricted using an access-list.

Suggested Fix
Configure an access list to restrict the access to the HTTP server on the device using the command

\[ \text{ip http access-class <1-99} \]

Rule 6

Rule
Restrict access to HTTP server [IOS]

Description
If web-based remote administration is required, HTTP server should be enabled and access must be restricted to the trusted users.

Applicable Platforms
Cisco IOS Devices

Impact
Unauthorized users may gain access if not restricted using an access-list.
Chapter 4    Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Suggested Fix

Configure an access list to restrict the access to the HTTP server on the device, using the command

\textit{ip http access-class <1-99>}

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed Subnets</td>
<td>Access List for HTTP server. Using Allowed Subnets Editor option, you can add, remove or update Allowed Subnets details. You can also change the order of the server details.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Rule 7

Rule
Check HTTP server authentication methods [IOS]

Description
Specify the desired type of authentication for HTTP connections.

Applicable Platforms
Cisco IOS Devices

Impact
Unauthorized users can gain access if authentication is not used.

Suggested Fix
Set up usernames and passwords for all administrators. If possible, use AAA user access control which will give more control and better audit. Configure required authentication using

\textit{ip http authentication}

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Method</td>
<td>HTTP server authentication method. Violations cannot be fixed if you specify multiple methods for the input. Using Auth method Editor option, you can add, remove or update Auth method details. You can also change the order of the server details</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Rule 8

Rule
Check management access via ASDM is restricted [PIX, ASA]
Chapter 4 Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Description
Adaptive Security Device Manager (ASDM) ip address should be defined.

Applicable Platforms
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
Management access via the ASDM should be restricted to management workstations.

Suggested Fix
Define the Adaptive Security Device Manager (ASDM) ip address using the command

```
no http 0.0.0.0 0.0.0.0 <interface-name>
http <ip-address> <mask> <interface-name>
```

Miscellaneous Service

Description
Policies governing miscellaneous TCP(echo, discard, chargen, day time) and UDP(echo, discard, chargen) services on the device.

Applicable Platforms
Cisco IOS Devices
Cisco IOS Devices With BOOTP Capability
Cisco IOS Devices With SCP Capability

References
Payment Card Industry Data Security Standard(PCI). (2.2 of Version 1.1, September, 2006)
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

National Security Agency (NSA) Cisco Router Configuration Guide(Section 8.1(1) Page 274,275, 8.1(7) Page 276, Section 8.1(18) Page 278, Section 4.2.1 Page 70,71,72 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

SANS Router Security Policy(Sections 3.0(1), 3.0(2), 3.0(3))
The SANS (SysAdmin, Audit, Network, Security) Institute publishes security policy to help system administrators with rapid development and implementation of information security policies.

National Security Agency (NSA) Cisco Switch Configuration Guide(Section 6.2.1, Page 16 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.


Information Technology - Code of practice for information security management.

Cisco SAFE Compliance(1.1b)

SAFE: A Security Blueprint for Enterprise Networks

Department of Homeland Security (DHS) Compliance(Section 4.3, Page 22 of Version 2.0)

This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Center for Internet Security, Benchmark for Cisco IOS.(Section 1.2.2.2-1.2.2.4,1.2.2.6, Page: 23 Section 1.2.2.9-1.2.2.11,page:26; section 1.3.1.2,Page:34; Section 2.3.3.3,Page:47 of Version 2.2, Nov 2007)

CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

Rule 1

**Rule**

Disable TCP small servers [IOS]

**Description**

TCP small servers are servers (daemons, in Unix parlan ce) that run in the router which are useful for diagnostics.

The TCP small servers are:

- **Echo**: Echoes back whatever you type through the `telnet x.x.x.x echo` command.
- **Chargen**: Generates a stream of ASCII data. Use the `telnet x.x.x.x chargen` command.
- **Discard**: Throws away whatever you type. Use the `telnet x.x.x.x discard` command.
- **Daytime**: Returns system date and time, if it is correct. It is correct if you run Network Time Protocol (NTP), or have set the date and time manually from the exec level. Use the `telnet x.x.x.x daytime` command.

Replace x.x.x.x with the IP address of your router. Most routers inside Cisco run the small servers.

The TCP small servers are enabled by default on Cisco IOS Software Version 11.2 and earlier. They are disabled by default on Cisco IOS Software Versions 11.3 and later.

**Applicable Platforms**

Cisco IOS Devices
Impact
It is recommended that you do not enable these services unless it is absolutely necessary. These services could be exploited indirectly or directly to gain information about the target system.

Suggested Fix
Disable TCP small servers using the command

```bash
no service tcp-small-servers
```

**Rule 2**

**Rule**
Disable UDP small servers [IOS]

**Description**
UDP small servers are servers (daemons, in Unix parlance) that run in the router which are useful for diagnostics.

- The UDP small servers are:
- **Echo**: Echoes the payload of the datagram you send.
- **Discard**: Silently pitches the datagram you send.
- **Chargen**: Pitches the datagram you send, and responds with a 72-character string of ASCII characters terminated with a CR+LF.

The UDP small servers are enabled by default on Cisco IOS Software Version 11.2 and earlier. They are disabled by default on Cisco IOS Software Versions 11.3 and later.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
It is recommended that you do not enable these services unless it is absolutely necessary. These services could be exploited indirectly or directly to gain information about the target system.

**Suggested Fix**
Disable UDP small servers using the command

```bash
no service udp-small-servers
```

**Rule 3**

**Rule**
Disable Finger server [IOS]
Understanding Compliance and Audit Manager (CAAM) Policies

Chapter 4      Using Compliance and Audit Manager Feature

Rule 4

Rule
Disable BOOTP server [IOS]

Description
BOOTP (BOOTstrap Protocol) was originally created for loading diskless computers. It was later used to allow a host to obtain all the required TCP/IP information to use the Internet. BOOTP allows a host to broadcast a request onto the network, and obtains information required from a BOOTP server. The BOOTP server is a computer that listens for incoming BOOTP requests and generates responses from a configuration database for the BOOTP clients on that network. BOOTP differs from DHCP in that it has no concept of lease or lease expiration. All IP addresses allocated by a BOOTP server are permanent.

Applicable Platforms
Cisco IOS Devices With BOOTP Capability

Impact
This is rarely needed and may open a security hole.

Suggested Fix
Disable BOOTP server using the command

no ip bootp server

Rule 5

Rule
Disable configuration auto-loading from TFTP server [IOS]
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Description
Configuration autoloading enables autoloading of configuration files from a network server.

Applicable Platforms
Cisco IOS Devices

Impact
Can be exploited to load wrong configuration files.

Suggested Fix
Disable configuration autoloading using the command

no service config

Rule 6

Rule
Disable IP Source Routing [IOS]

Description
Source Routing is a technique whereby the sender of a packet can specify the route that a packet should take through the network. Source routing is useful when the default route that a connection will take fails or is suboptimal for some reason, or for network diagnostic purposes.

Applicable Platforms
Cisco IOS Devices

Impact
When used in conjunction with traceroute, an attacker can find all the routes between points on the network.

Also, sometimes machines will be on the Internet, but will not be reachable. (It may be using a private address like 10.0.0.1). However, there may be some other machine that is reachable to both sides that forwards packets. Someone can then reach that private machine from the Internet by source routing through that intermediate machine.

Suggested Fix
Disable IP Source Routing using the command

no ip source-route

Rule 7

Rule
Disable X.25 PAD service [IOS]
Description
Packet assembler/disassembler (PAD) is configured to enable X.25 connections between network devices. A PAD is a device that receives a character stream from one or more terminals, assembles the character stream into packets, and sends the data packets out to a host. A PAD can also do the reverse. It can take data packets from a network host and translate them into a character stream that can be understood by the terminals. A PAD is defined by Recommendations X.3, X.28, and X.29 of the International Telecommunication Union Telecommunication Standardization Sector (ITU-T).

PADs can also be configured to work with a protocol translation application.

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Disable PAD service using the command
no service pad

Rule 8

Rule
Disable Gratuitous ARPs [IOS]

Description
A gratuitous ARP is an ARP broadcast in which the source and destination MAC addresses are the same. It is used primarily by a host to inform the network about its IP address.

Applicable Platforms
Cisco IOS Devices

Impact
A spoofed gratuitous ARP message can cause network mapping information to be stored incorrectly, causing network malfunction.

Suggested Fix
IP gratuitous Address Resolution Protocol (ARP) requests should be disabled whenever possible using the command no ip gratuitous-arps

Rule 9

Rule
Disable Identification service [IOS]

Description
The identification protocol provides a means to determine the identity of a user of a particular TCP connection.
Applicable Platforms
Cisco IOS Devices

Impact
The information revealed about users, entities, objects, or processes might normally be considered private and can be exploited to attack the device.

Suggested Fix
Disable Identification service using the command no ip identd

Rule 10
Rule
Disable MOP (Maintenance Operation Protocol) [IOS]

Description
System utility services on DECnet networks uses MOP protocol. It is enabled by default on Ethernet interfaces.

Applicable Platforms
Cisco IOS Devices

Impact
Unless you are using DECnet, you should disable MOP. MOP enabled when you do not need it only provides another facility that can be attacked.

Suggested Fix
Disable MOP service on the device using the command interface <interface name> no mop enabled

Rule 11
Rule
Disable TFTP server [IOS]

Description
Disable TFTP Server on the device.

Applicable Platforms
Cisco IOS Devices

Impact
The Trivial File Transfer Protocol (TFTP) provides an easy way to transfer files between network devices. However, TFTP is not a secure service and normally should not be running on any device in a secure network.
Suggested Fix
Disable TFTP service on the device using

\textit{no tftp-server}

\textbf{Rule 12}

\textbf{Rule}
Tunnel interfaces should not be configured [IOS]

\textbf{Description}
Check that no tunnel interfaces are defined on the device.

\textbf{Applicable Platforms}
Cisco IOS Devices

\textbf{Impact}
Tunnel interfaces are virtual interfaces on the router. These interfaces can be used by an attacker. Unless absolutely necessary, do not create any tunnel interfaces.

\textbf{Suggested Fix}
Delete a tunnel interface using

\textit{no interface Tunnel}

\textbf{Rule 13}

\textbf{Rule}
Disable DHCP service [IOS]

\textbf{Description}
Check that DHCP service is disabled on the device.

\textbf{Applicable Platforms}
Cisco IOS Devices

\textbf{Impact}
No known impact

\textbf{Suggested Fix}
Disable DHCP service using the command

\textit{no service dhcp}
Rule 14

Rule
Disable Booting from Network Configuration File [IOS]

Description
Check that booting from network configuration file is disabled.

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Enable booting from network configuration file using the command
no boot network

Rule 15

Rule
IP Classless Forwarding must be [IOS]

Description
Check that IP Classless forwarding is configured as required.

Applicable Platforms
Cisco IOS Devices

Impact
No known impact

Suggested Fix
Enable or disable IP classless forwarding using the command
[no] ip classless

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ip Classless State</td>
<td>Whether IP classless forwarding should be enabled or disable</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: true</td>
</tr>
</tbody>
</table>
Rule 16

Rule
Enable SCP server [IOS]

Description
This rule checks that SCP Server is enabled on the device.

Applicable Platforms
Cisco IOS Devices With SCP Capability

Impact
The router administrators can not use the SCP protocol to transfer configuration or image files to and from the router.

Suggested Fix
Enable SCP service on the device using the commands

```
ip scp server enable
```

Rule 17

Rule
Disable FTP server [IOS]

Description
Disable FTP Server on the device.

Applicable Platforms
Cisco IOS Devices

Impact
The File Transfer Protocol (FTP) provides an easy way to transfer files between network devices. However, FTP is not a secure service and normally should not be running on any device in a secure network.

Suggested Fix
Disable FTP service on the device using the command

```
no ftp-server
```

Routing and Forwarding

Description
Policies governing Routing and Forwarding related services on the device.
Applicable Platforms
Cisco IOS Devices
Cisco IOS Devices With SPD Capability

References
Cisco SAFE Compliance
SAFE: A Security Blueprint for Enterprise Networks
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.3.6, Page 95, Section 4.4.7 Page 130 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 8.2, Page 29 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Department of Homeland Security (DHS) Compliance(Section 4.4, Page 31 of Version 2.0)
This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.
Center for Internet Security, Benchmark for Cisco IOS.(Section 2.3.3.1, Page: 46 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

Rule 1

Rule

Description
Check that Selective Packet Discard (SPD) is configured to be desired state.

Applicable Platforms
Cisco IOS Devices With SPD Capability
Impact

Selective Packet Discard (SPD) is a mechanism that manages the process-level input queues on the route processor. The goal of SPD is to provide priority to routing protocol packets and other important traffic control Layer 2 keepalives during periods of process-level queue congestion. Disabling the feature might create routing inconsistencies during periods of high volume traffic.

Suggested Fix

Configure Selective Packet Discard (SPD) using the command `[no] spd enable`

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired SPD State</td>
<td>Desired state of SPD</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>

Rule 2

Rule

Check Minimum SPD Headroom [IOS]

Description

Check that SPD headroom is configured to be at least given number of packets. Even with SPD, the behavior of normal IP packets is not changed; however, routing protocol packets are given higher priority because SPD recognizes routing protocol packets by the IP precedence field. Hence, if the IP precedence is set to 6, then the packet is given priority. SPD prioritizes these packets by allowing the software to enqueue them into the process level input queue above the normal input queue limit. The number of packets allowed in excess of the normal limit is called the spd headroom, the default being 100, which means that a high precedence packet is not dropped if the size of the input hold queue is lower than 175 (input queue default size + spd headroom size).

Applicable Platforms

Cisco IOS Devices With SPD Capability

Impact

Selective Packet Discard (SPD) is a mechanism that manages the process-level input queues on the route processor. The goal of SPD is to provide priority to routing protocol packets and other important traffic control Layer 2 keepalives during periods of process-level queue congestion. Disabling the feature might create routing inconsistencies during periods of high volume traffic.

Suggested Fix

Configure SPD headroom to be the desired value using command `spd headroom`
Rule 3

Rule
Check Minimum SPD Extended Headroom [IOS]

Description
Check that SPD extended headroom is configured to be at least given number of packets. Non-IP packets, such as Connectionless Network Service Intermediate System-to-Intermediate System (CLNS ISIS) packets, Point-to-Point Protocol (PPP) packets, and High-Level Data Link Control (HDLC) keepalives were, until recently, treated as normal priority as a result of being Layer 2 instead of Layer 3. In addition, Interior Gateway Protocols (IGPs) operating at Layer 3 or higher were given priority over normal IP packets, but given the same priority as BGP packets. So, during BGP convergence or during times of very high BGP activity, IGP hellos and keepalives were often dropped, causing IGP adjacencies to go down. Since IGP and link stability are more tenuous and more crucial than BGP stability, such packets are now given the highest priority and are given extended SPD headroom with a default of 10 packets. This means that these packets are not dropped if the size of the input hold queue is lower than 185 (input queue default size + spd headroom size + spd extended headroom).

Applicable Platforms
Cisco IOS Devices With SPD Capability

Impact
Selective Packet Discard (SPD) is a mechanism that manages the process-level input queues on the route processor. The goal of SPD is to provide priority to routing protocol packets and other important traffic control Layer 2 keepalives during periods of process-level queue congestion. Disabling the feature might create routing inconsistencies during periods of high volume traffic.

Suggested Fix
Configure SPD extended headroom to be the desired value using command

```text
spd extended-headroom
```
Rule 4

Rule
Check that Cisco Express Forwarding (CEF) is enabled [IOS]

Description
Check that Cisco Express Forwarding (CEF) or Distributed CEF are enabled whenever they are available.

Applicable Platforms
Cisco IOS Devices

Impact
The CEF switching mode replaces the traditional Cisco routing cache with a data structure that mirrors the entire system routing table. Because there is no need to build cache entries when traffic starts arriving for new destinations, CEF behaves more predictably than other modes when presented with large volumes of traffic addressed to many destinations.

Although most flooding denial of service attacks send all of their traffic to one or a few targets and therefore do not tax the traditional cache maintenance algorithm, many popular SYN flooding attacks use randomized source addresses. The host under attack replies to some fraction of the SYN flood packets, creating traffic for a large number of destinations. Routers configured for CEF therefore perform better under SYN floods (directed at hosts, not at the routers themselves) than do routers using the traditional cache. CEF is recommended when available.

Suggested Fix
Enable CEF or Distributed CEF whenever they are available using the command

`ip cef`

Rule 5

Rule
Check that Unicast Reverse Path Forwarding (RPF) is enabled on interfaces [IOS]
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Description
Check that unicast reverse path forwarding (RPF) is enabled on interfaces.

In almost all Cisco IOS software versions that support Cisco Express Forwarding (CEF), you can have the device check the source address of any packet against the interface through which the packet entered the device. If the input interface is not a feasible path to the source address according to the routing table, the packet is dropped. This look-back feature is called unicast reverse path forwarding (RPF).

You can use unicast RPF in any single-homed environment where there is essentially only one access point out of the network, that is, one upstream connection. Networks having one access point offer the best example of symmetric routing, which means that the interface where a packet enters the network is also the best return path to the source of the IP packet. Unicast RPF is best used at the network perimeter for Internet, intranet, or extranet environments, or in ISP environments for customer network terminations.

Applicable Platforms
Cisco IOS Devices

Impact
Many network attacks rely on an attacker falsifying (spoofing) the source addresses of IP datagrams. Some attacks depend on spoofing, while other attacks are much harder to trace if the attacker can use somebody else's address. Therefore, you should prevent spoofing wherever feasible.

Suggested Fix
Configure RPF check on the interfaces using the command

\textit{ip verify unicast reverse-path}

Rule 6

Rule
Check that Netflow switching for routing is enabled on all interfaces [IOS]

Description
Check that NetFlow switching for routing is enabled on all interfaces.

Applicable Platforms
Cisco IOS Devices

Impact
NetFlow efficiently provides the metering base for a key set of applications, including accounting and billing, network planning, network monitoring, and outbound marketing for both service provider and enterprise users.

NetFlow has two key components: first, the NetFlow cache or data source that stores IP Flow information and second, the NetFlow export or transport mechanism that sends NetFlow data to a network management collector for data reporting.
Suggested Fix
Enable NetFlow switching using the command on all the interfaces.

```
interface <interface name>
ip route-cache flow
```

Rule 7

Rule
Check that the Committed Access Rate (CAR) is configured on all interfaces [IOS]

Description
Check that the committed access rate is configured on all interfaces.

Applicable Platforms
Cisco IOS Devices

Impact
You can use the `rate-limit` command to allocate different traffic rates to selected types of traffic. This can help you reserve part of the interface bandwidth for critical traffic, preventing an attack from overwhelming the interface. You can also use the command during an attack to throttle the attack.

Suggested Fix
Configure committed access rate (CAR) using the command `rate-limit`

```
<interface name>
rate-limit
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check for traffic</td>
<td>Whether it should be checked for incoming traffic or outgoing traffic or both</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 3</td>
</tr>
</tbody>
</table>

Rule 8

Rule
Check filtering of packets with IP options [IOS]

Description
The `ip options` command allows you to filter IP options packets, either to drop or to ignore packets with IP options. Drop and ignore modes are mutually exclusive; that is, if the drop mode is configured and then the ignore mode is configured, the ignore mode will override the drop mode.

Applicable Platforms
Cisco IOS Devices

Impact
This can be used to mitigate the effects of IP options on the router, and on downstream routers and hosts.
**Suggested Fix**  
Configure filtering of IP options packet filtering using the command

\[\text{[no]} \text{ ip options}\]

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Action | Desired behaviour for packets with IP options | Required: true  
Default: 1 |

**Rule 9**

**Rule**  
Check that “scheduler allocate” or “scheduler interval” command is configured [IOS]

**Description**  
When a Cisco router is fast-switching a large number of packets, it is possible for the router to spend so much time responding to interrupts from the network interfaces that no other work gets done. You can reduce this effect by using the scheduler interval or scheduler allocate commands to set aside time for the device to handle process rather than respond to interrupts.

The `scheduler allocate` command is a newer command and is not supported on all Cisco routers. With this command, you can specify a period for running with interrupts enabled, and another period for running with interrupts masked, so that process tasks can be handled. For example, a typical configuration might include the `scheduler allocate 30000 2000` command.

**Applicable Platforms**  
Cisco IOS Devices

**Impact**  
This can be exploited to cause DoS attacks on the device.

**Suggested Fix**  
Configure scheduler parameters using the command

`scheduler interval`

`scheduler allocate`

**SNMP**

**Description**  
The Simple Network Management Protocol (SNMP) is the standard Internet protocol for automated remote monitoring and administration. There are several different versions of SNMP, with different security properties. If a network has a deployed SNMP infrastructure in place for administration, then all routers on that network should be configured to securely participate in it. In the absence of a deployed SNMP scheme, all SNMP facilities on all routers should be disabled. While SNMP is helpful because it allows an administrator to remotely configure the router, it also offers a potentially dangerous conduit into a network.
Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

References
Payment Card Industry Data Security Standard (PCI) (2.3 of Version 1.1, September, 2006)
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

National Security Agency (NSA) Cisco Router Configuration Guide (Section 8.1(8) Page 276, Section 4.2.1 Page 70, Section 4.5.3 Page 152 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Health Insurance Portability and Accountability Act (164.312(a)(1), 164.312(e)(1))
HIPAA (Health Insurance Portability and Accountability Act) is designed to protect confidential healthcare information through improved security standards and federal privacy legislation. It defines requirements for storing patient information before, during and after electronic transmission. Centers for Medicare & Medicaid Services (CMS) has provided a Security Rule (45 CFR Part 160 and 164) which is adopted to implement provisions of the HIPAA.

SANS Router Security Policy (Sections 3.0(4))
The SANS (SysAdmin, Audit, Network, Security) Institute publishes security policy to help system administrators with rapid development and implementation of information security policies.

National Security Agency (NSA) Cisco Switch Configuration Guide (Section 6.2.2, Page 18 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Cisco SAFE Compliance (1.1b)

Information Technology - Code of practice for information security management.

Defence Information System Agency (Section NET0890, NET0894 of Dec 2, 2005)
DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

Department of Homeland Security (DHS) Compliance (Section 4.3, Page 29 of Version 2.0)
This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Center for Internet Security, Benchmark for Cisco PIX/ASA. (Section 1.1.5, Page: 14 of Version 2.0, Nov 2007)

CIS PIX/ASA benchmark recommends the prudent level of minimum due care for operating system security. CIS PIX/ASA benchmark contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All PIX devices should implement these settings.

Center for Internet Security, Benchmark for Cisco IOS. (Section 1.1.5, Page: 17 of Version 2.2, Nov 2007)

CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

### Rule 1

**Rule**
Check the state of SNMP server [IOS, PIX, ASA]

**Description**
Check the state of SNMP server on the device.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
The Simple Network Management Protocol (SNMP) is the standard Internet protocol for automated remote monitoring and administration. There are several different versions of SNMP, with different security properties. If a network has a deployed SNMP infrastructure in place for administration, then all routers on that network should be configured to securely participate in it. In the absence of a deployed SNMP scheme, all SNMP facilities on all routers should be disabled. While SNMP is helpful because it allows an administrator to remotely configure the router, it also offers a potentially dangerous conduit into a network.

**Suggested Fix**
The safest way to ensure that SNMP is really unavailable to an attacker, and will remain so, is to list the established SNMP community strings and explicitly unset all of them. It is also recommended to disable [SNMP trap] and [system shutdown] features and finally disabling SNMP Server on the device using the command

\[
\text{[no] snmp-server \text{ (for IOS)}}
\]

\[
\text{[no] snmp-server enable \text{ (for PIX)}}
\]
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Server Should be</td>
<td>Choose the desired SNMP state</td>
<td>Required: true  Default: false</td>
</tr>
</tbody>
</table>

Rule 2

**Rule**
Check that SNMP Reload is disabled [IOS]

**Description**
Using SNMP packets, a network management tool can send messages to users on virtual terminals and the console. This facility operates in a similar fashion to the [EXEC send] command, however, the SNMP request that causes the message to be issued to the users also specifies the action to be taken after the message is delivered. One possible action is a shutdown request. After a system is shut down, typically it is reloaded.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
This can be exploited by attackers to reload the system.

**Suggested Fix**
Disable SNMP Reload feature using the command

`no snmp-server system-shutdown`

Rule 3

**Rule**
Check that SNMP Traps are disabled [IOS, PIX, ASA]

**Description**
SNMP trap messages are generated by the device for configuration event notifications or security alerts.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
SNMP traps carry information in clear text. This information can be easily captured to retrieve sensitive information.

**Suggested Fix**
Disable SNMP Traps using the command no snmp-server host
Rule 4

Rule
Check that desired servers are configured for receiving SNMP Traps [IOS, PIX, ASA]

Description
SNMP trap messages are generated by the device for configuration event notifications or security alerts. If you use SNMP and enable the network devices to send SNMP traps, you should ensure that the correct trap servers are configured on the devices.

Logging SNMP traps can be useful because Cisco devices can record information about a variety of events, many of which have security significance. Logs can be invaluable in characterizing and responding to security incidents. Logging the messages from devices and analyzing them in real time or offline provides an insight into the network to troubleshoot security issues. A syslog server is an inexpensive and widely available application that stores log entries from network devices. This facility allows you permanent storage for logging information, which is especially valuable when physical access to the network device is impractical. A syslog server also affords greater detail within the logs themselves (less reliance on the device's logging buffer). The level of detail of the syslog server-stored logs is set using the logging trap command. There is minimal performance impact to the device, regardless of the level of logging detail.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
SNMP traps will not be sent to required hosts.

Suggested Fix
Configure SNMP to send traps to required hosts using the command snmp-server host

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included Trap Servers</td>
<td>List of desired servers to receive SNMP Traps. Using Trap Server Editor option, you can add, remove or update Trap Server details. You can also change the order of the server details.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Rule 5

Rule
SNMP should be configured with these community strings [IOS, PIX, ASA]

Description
Make sure SNMP is configured with the given community strings.

Applicable Platforms
Cisco IOS Devices
Impact

Use of the same community string ensures that security of the devices can be easily managed. Users might use a different community string than the standard one for troubleshooting and then forget to turn it off. An attacker gaining access to a device might change the community string and then access the device later. In certain cases, turning off SNMP is not an option since there are applications that use SNMP to manage the device. In order to manage the network using SNMP and yet not compromise on security, it is essential that ACLs be enabled for device access. This will limit the SNMP access to the authorized subnets or hosts.

Suggested Fix

Configure the given community strings using the command

```
snmp-server community
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included Community Strings</td>
<td>Community string that must be included. Using Community String Editor option, you can add, remove or update Community String details. You can also change the order of the server details.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Rule 6

Rule

SNMP should be configured with the community string [PIX, ASA]

Description

Make sure SNMP is configured with the given community string.

Applicable Platforms

Cisco PIX Devices Running >= 7.x and ASA devices

Impact

Use of the same community string ensures that security of the devices can be easily managed. Users might use a different community string than the standard one for troubleshooting and then forget to turn it off. An attacker gaining access to a device might change the community string and then access the device later. In certain cases, turning off SNMP is not an option since there are applications that use SNMP to manage the device. In order to manage the network using SNMP and yet not compromise on security, it is essential that ACLs be enabled for device access. This will limit the SNMP access to the authorized subnets or hosts.

Suggested Fix

Configure the given community strings using the command

```
snmp-server community
```
### Rule 7

**Rule**
SNMP should not be configured with these well known community strings [IOS, PIX, ASA]

**Description**
Make sure SNMP is not configured with the well known community strings like public,private, etc.

**Applicable Platforms**
- Cisco IOS Devices
- Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
Use of well known community strings will make the network vulnerable since attackers can easily gain access to the network information.

**Suggested Fix**
Do not use well known community strings with SNMP like 'public', 'private', etc. Remove the prohibited community strings using the command no snmp-server community

<table>
<thead>
<tr>
<th>Rule Description Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community String Community string that must be configured Using Community String Editor option, you can add, remove or update Community String details. You can also change the order of the server details Required: true</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule Description Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banned Community Strings Well known strings to check for. Using Banned Community Strings Editor option, you can add, remove or update Banned Community Strings details. You can also change the order of the server details Required: true</td>
</tr>
</tbody>
</table>

### Rule 8

**Rule**
Check that writeable community strings are not configured [IOS]

**Description**
Configuring SNMP community strings with write access allows users to change the system state. Care should be taken while doing so.
Understanding Compliance and Audit Manager (CAAM) Policies

Applicable Platforms
Cisco IOS Devices

Impact
While SNMP is helpful because it allows an administrator to remotely configure the router, it also offers a potentially dangerous conduit into a network. Care should be taken while configuring SNMP community strings with write access since an attacker can change the system state.

Suggested Fix
Do not configure write access for SNMP community strings, give 'Read-Only' access. Change them to ReadOnly community strings using the command

```
snmp-server community <community string> ro
```

Rule 9

Rule
Check that SNMP access is restricted with ACLs [IOS]

Description
ACLs can be configured with SNMP community strings to restrict access to SNMP server.

Applicable Platforms
Cisco IOS Devices

Impact
Configuring an SNMP community string with no ACL allows users from any host to access the SNMP server if they know the community string. This can be exploited by an attacker who can change the system state.

Suggested Fix
Configure ACLs for SNMP community strings to allow access from trusted networks/hosts using the command

```
snmp-server community <community string> <ro|rw> <access-list name or number>
```

TCP Parameters

Description
Policies to enforce TCP related parameter values.

Applicable Platforms
Cisco IOS Devices
Cisco IOS Devices With TCP_INTERCEPT Capability
References

National Security Agency (NSA) Cisco Router Configuration Guide(1.1b)

The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Cisco SAFE Compliance(1.1b)

SAFE: A Security Blueprint for Enterprise Networks

National Security Agency (NSA) Cisco Router Configuration Guide(Section 8.1(14) Page 278, Section 4.1.6 Page 66, Section 4.2.1 Page 70, Section 4.3.3 Page 90 of Version 1.1c)

The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

National Security Agency (NSA) Cisco Switch Configuration Guide(Section 12.2, Page 44 of Version 1.0)

The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Department of Homeland Security (DHS) Compliance(Section 4.4, Page 33 of Version 2.0)

This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Center for Internet Security, Benchmark for Cisco IOS.(Section 1.2.2.7-1.2.2.8, Page:25-26 of Version 2.2, Nov 2007)

CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

Rule 1

Rule
TCP keep-alives on incoming network connections [IOS]

Description
Enable/disable generation of TCP keep-alive messages on idle incoming network connections (those initiated by the remote host)
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Applicable Platforms
Cisco IOS Devices Cisco IOS Devices With TCP_INTERCEPT Capability

Impact
The TCP keepalive service allows a router to detect when the host with which it is communicating experiences a system failure, even if data stops being sent (in either direction). This capability is most useful on incoming connections. For example, if a host failure occurs while the router is communicating with a printer, the router might never notice because the printer does not generate any traffic in the opposite direction. If keepalives are enabled, they are sent once every minute on otherwise idle connections. If 5 minutes pass and no keepalives are detected, the connection is closed. The connection is also closed if the host replies to a keepalive packet with a reset packet. This will happen if the host crashes and comes back up again. An unclosed, stale connection might be used by an attacker to gain unauthorized entry into the device.

Suggested Fix
Enable/Disable generation of TCP keep-alive messages on idle incoming network connections using the command

\[[no\] service tcp-keepalives-in

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>State of TCP keep alives on incoming network connections.</td>
<td>Required: true Default: true</td>
</tr>
</tbody>
</table>

Rule 2

Rule
TCP keep-alives on outgoing network connections [IOS]

Description
Enable/disable generation of TCP keep-alive messages on idle outgoing network connections (those initiated by the user on the device).

Applicable Platforms
Cisco IOS Devices Cisco IOS Devices With TCP_INTERCEPT Capability

Impact
The TCP keepalive service allows a router to detect when the host with which it is communicating experiences a system failure, even if data stops being sent (in either direction).

Suggested Fix
Enable/Disable generation of TCP keep-alive messages on idle outgoing network connections using the command \[no\] service tcp-keepalives-out.
## Rule 3

**Rule**
Check maximum TCP SYN wait time [IOS]

**Description**
Establishing a successful TCP connection involves the originator sending a connection request, the receiver sending an acknowledgement and then the originator sending an acceptance of that acknowledgement. This is called a 3-way handshake. Once this three-phase handshake is complete, the connection is complete and data transfer can begin. SYN wait time determines how long a device waits before bringing down the incomplete connections.

**Applicable Platforms**
- Cisco IOS Devices
- Cisco IOS Devices With TCP_INTERCEPT Capability

**Impact**
This can be exploited by a hacker to do a SYN flooding attack on the device. A SYN flooding attack involves sending repeated connection requests to a device but never sending the acceptance of acknowledgements to complete those connections. This creates increasingly more incomplete connections at the device. Since the buffer for incomplete connections is usually smaller than the buffer for completed connections, this can overwhelm and disable the host to receive further incoming connections denying the service for legitimate users.

**Suggested Fix**
Configure syn wait time, so that the device shuts down the incomplete connections, using the command `ip tcp synwait-time`

### Rule Description Constraints

| SYN Wait Time in Seconds | Time (in seconds) the software waits while attempting to establish a TCP connection. | Required: true Default: 10 Min Value: 5 Max Value: 300 |

## Rule 4

**Rule**
Check state of TCP interception [IOS]
### Understanding Compliance and Audit Manager (CAAM) Policies

#### Description
The TCP intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of denial-of-service attack.

A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a web site, accessing e-mail, using FTP service, and so on.

#### Applicable Platforms
Cisco IOS Devices With TCP_INTERCEPT Capability

#### Impact
Enabling TCP intercept feature helps in avoiding DoS attacks on TCP server services.

#### Suggested Fix
Enforce that TCP interception be enabled or disabled using the command `[no] ip tcp intercept`

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| State | State of TCP interception. | Required: true  
Default: true |

#### Rule 5

#### Rule
Check maximum TCP intercept watch-timeout[IOS]

#### Description
The TCP intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of denial-of-service attack.

A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a web site, accessing e-mail, using FTP service, and so on.

#### Applicable Platforms
Cisco IOS Devices With TCP_INTERCEPT Capability.

#### Impact
Enabling TCP intercept feature helps in avoiding DoS attacks on TCP server services.

#### Suggested Fix
Configure TCP intercept Watch Timeout using the command

```bash
ip tcp intercept watch-timeout
```
Rule 6

**Rule**
Check maximum TCP intercept connection-timeout[IOS]

**Description**
The TCP intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of denial-of-service attack.

A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhels the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a web site, accessing e-mail, using FTP service, and so on.

**Applicable Platforms**
Cisco IOS Devices With TCP_INTERCEPT Capability

**Impact**
Enabling TCP intercept feature helps in avoiding DoS attacks on TCP server services.

**Suggested Fix**
Configure TCP intercept Connection Timeout using the command

`ip tcp intercept connection-timeout`

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| TCP intercept watch-timeout in seconds. | Timeout (in seconds) seconds for a watched connection to reach established state before sending a Reset to the server. | Required: true  
Default: 30  
Min Value: 1  
Max Value: 2147483 |

## BGP

**Description**
BGP Related policies

**Applicable Platforms**
Cisco IOS Devices With BGP Routing Capability
References
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.4.5 Page 123 of Version 1.1c)

The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Information Technology - Code of practice for information security management.

Defence Information System Agency(Section NET0400,NET0410 of Dec 2, 2005)

DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

Department of Homeland Security (DHS) Compliance(Section 4.1,4.2, Page 18,20 of Version 2.0)
This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Center for Internet Security, Benchmark for Cisco IOS.(Section 2.3.2.1, Page: 43 of Version 2.2, Nov 2007)

CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

Rule 1

Rule
Check MD5 Authentication [IOS]

Description
This rule checks to make sure that BGP autonomous systems use MD5 authentication. Router neighbor authentication is a mechanism that, when applied correctly, can prevent many routing attacks. Each router accomplishes authentication by the possession of an authentication key. That is, routers connected to the same network segment all use a shared secret key. Each sending router then uses this key to 'sign' each route table update message. The receiving router checks the shared secret to determine whether the message should be accepted.

Applicable Platforms
Cisco IOS Devices With BGP Routing Capability

Impact
This router is vulnerable to various routing attacks by spoofing the route table update messages.
**Suggested Fix**

Configure BGP MD5 Authentication using the command

```
router bgp <AS Number>
neighbor <Peer Group Name or Neighbor Address> password <Authentication Password>
```

**Rule 2**

**Rule**

Check that incoming BGP route filtering is configured [IOS]

**Description**

This rule checks that some kind of route filtering is configured for each BGP neighbor or globally for all interfaces for accepting route updates. BGP Route Filtering can be configured either using access list based filtering (using distribute-list) or using the prefix lists based filtering (prefix-list).

Communications between routers for routing table updates involve routing protocols. These updates provide directions to a router on which way traffic should be routed. You can use access lists to restrict what routes the router will accept (in) or advertise (out) via some routing protocols.

**Applicable Platforms**

Cisco IOS Devices With BGP Routing Capability

**Impact**

Router may accept route update messages from unintended entities.

**Suggested Fix**

Configure route filtering for all BGP neighbors using the commands

```
router bgp <autonomous system number>
distribute-list <acl number> in
neighbor <neighbor address or peer group> distribute-list <acl number> in
distribute-list prefix <prefix-list name> in
neighbor <neighbor address or peer group> prefix-list <prefix-list name> in !
```

**Rule Description Constraints**

<table>
<thead>
<tr>
<th>Route Filter Type</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired route filter type to be enforce</td>
<td>Required: true</td>
<td>Default: dontcare</td>
</tr>
</tbody>
</table>

| ACL to be enforced | Desired ACL to be enforced. Leave blank to enforce no particular ACL ID. | Required: false |
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 3

Rule
Check that outgoing BGP route filtering is configured [IOS]

Description
This rule checks that some kind of route filtering is configured for each BGP neighbor or globally for all interfaces for advertising route updates. BGP Route Filtering can be configured either using access list based filtering (using distribute-list) or using the prefix lists based filtering (prefix-list). Communications between routers for routing table updates involve routing protocols. These updates provide directions to a router on which way traffic should be routed. You can use access lists to restrict what routes the router will accept (in) or advertise (out) via some routing protocols.

Applicable Platforms
Cisco IOS Devices With BGP Routing Capability

Impact
Router may advertise route update messages to unintended entities.

Suggested Fix
Configure route filtering for all BGP neighbors using the commands router bgp <autonomous system number> distribute-list <acl number> out neighbor <neighbor address or peer group> distribute-list <acl number> out distribute-list prefix <prefix-list name> out neighbor <neighbor address or peer group> prefix-list <prefix-list name> out !

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix List to be enforced</td>
<td>Desired prefix-list to be enforced. Leave blank to enforce no particular prefix-list.</td>
<td>Required: true Default: dontcare</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Filter Type</td>
<td>Desired route filter type to be enforced</td>
<td>Required: true Default: dontcare</td>
</tr>
</tbody>
</table>
Rule 4

Check TTL security [IOS]

This rule checks to make sure that BGP autonomous systems use either TTL Security mechanism using ttl-security feature or ebgp-multihop feature. The Generalized TTL Security Mechanism (GTSM), documented in RFC 3682 [32] and introduced in Cisco IOS 12.0(27)S and 12.3(7)T, utilizes the Time-to-Live (TTL) field of the IP header to protect exterior BGP (eBGP) peering sessions from remote attacks. This mechanism uses the TTL value in a received packet and compares it to an administrator defined hop count. If the received IP packet contains a TTL value greater than or equal to the expected TTL value (i.e. 255 minus an administrator defined hop count), then the packet is processed. Otherwise, the packet is silently discarded. Since remote attacks originate multiple router hops away from an intended target, limiting the hop count to the actual number of hops between eBGP peers will help prevent attacks initiated on any network that does not lie between the peers.

This feature protects the eBGP peering session by comparing the value in the TTL field of received IP packets against a hop count that is configured locally for each eBGP peering session. If the value in the TTL field of the incoming IP packet is greater than or equal to the locally configured value, the IP packet is accepted and processed normally. If the TTL value in the IP packet is less than the locally configured value, the packet is silently discarded and no ICMP message is generated. This is designed behavior; a response to a forged packet is unnecessary.

Applicable Platforms
Cisco IOS Devices With BGP Routing Capability

Impact
Router may be vulnerable to CPU utilization-based attacks. These types of attacks are typically brute force Denial of Service (DoS) attacks that attempt to disable the network by flooding the network with IP packets that contain forged source and destination IP addresses.
Rule 5

Rule
Check BGP Dampening is configured [IOS]

Description
This rule checks to make sure BGP dampening is configured. Route flap dampening is a method that may be used to provide router CPU and network stability while BGP routes are converging. Damping controls the effect of route flapping which occurs when a route constantly transitions from an up-to-down or down-to-up state. These transitions cause excessive BGP route update messages (i.e. add/withdraw routes) to propagate through the network. ISPs and other backbone providers may configure BGP dampening to mitigate route flapping.

Applicable Platforms
Cisco IOS Devices With BGP Routing Capability

Impact
Too many BGP route flaps may effect CPU and network stability.

Suggested Fix
Configure BGP dampening using the command

```
router bgp <AS Number>
bgp dampening !
```

EIGRP

Description
EIGRP Related policies

Applicable Platforms
Cisco IOS Devices With EIGRP Routing Capability

References
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.3.2 Page 88, Section 4.4.3 Page 111 of Version 1.1c)
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Information Technology - Code of practice for information security management.

Defence Information System Agency(Section NET0400.NET0425 of Dec 2, 2005)

DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

Department of Homeland Security (DHS) Compliance(Section 4.1, Page 19 of Version 2.0)
This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Center for Internet Security, Benchmark for Cisco IOS.(Section 2.3.2.2, Page: 44 of Version 2.2, Nov 2007)

CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

Rule 1

Rule
Check all participating interfaces use MD5 authentication [IOS]

Description
This rule checks to make sure that all the interfaces in all the EIGRP autonomous systems use MD5 authentication. Router neighbor authentication is a mechanism that, when applied correctly, can prevent many routing attacks. Each router accomplishes authentication by the possession of an authentication key. That is, routers connected to the same network segment all use a shared secret key. Each sending router then uses this key to 'sign' each route table update message. The receiving router checks the shared secret to determine whether the message should be accepted.

Applicable Platforms
Cisco IOS Devices With EIGRP Routing Capability

Impact
This router is vulnerable to various routing attacks by spoofing the route table update messages.

Suggested Fix
Configure EIGRP MD5 Authentication using the command

```
interface <interface name>

ip authentication mode eigrp <autonomous system number> md5
```


Rule 2

Rule
Check interface state of EIGRP routing updates [IOS]

Description
This rule checks that all the given interfaces are blocked/allowed from participating in EIGRP routing updates. It goes through for every network in every EIGRP autonomous system, and then gets a list of interfaces that belong to that network. It checks to see that if the given interfaces belong to the list above. If so, The interface is checked to see if it is passive or active interface and compared against the given policy. The passive-interface command is used to prevent other routers on the network from learning about routes dynamically. It can also be used to keep any unnecessary parties from learning about the existence of certain routes or routing protocols used. It is typically used when the wildcard specification on the network router configuration command configures more interfaces than desirable.

Applicable Platforms
Cisco IOS Devices With EIGRP Routing Capability

Impact
This interface may receive and transmit in EIGRP routing updates, which means, unnecessary parties may learn about the existence of certain routes or routing protocols used. This also leads to higher chance of spoofed routing update attacks.

Suggested Fix
Configure the interface as a passive/active interface using the commands

```
router eigrp <autonomous system number>
[no] passive-interface <interface name> !
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Group</td>
<td>List of interface groups to apply this policy. Using Interface Group Editor option, you can add, remove or update Interface Group details. You can also change the order of the server details</td>
<td>Required: true</td>
</tr>
<tr>
<td>EIGRP State</td>
<td>Desired EIGRP State of this interface Using EIGRP State Editor option, you can add, remove or update EIGRP State details. You can also change the order of the server details</td>
<td>Required: true Default: dontcare</td>
</tr>
</tbody>
</table>

Rule 3

Rule
Check that EIGRP incoming distribute-list is configured [IOS]
Description
This rule checks that ip distribute-list is configured for each EIGRP autonomous system for accepting route updates. Communications between routers for routing table updates involve routing protocols. These updates provide directions to a router on which way traffic should be routed. You can use access lists to restrict what routes the router will accept (in) or advertise (out) via some routing protocols. The distribute-list acl-num out command is used to restrict routes that get distributed in routing updates, while the distribute-list acl-num in command may be used to filter routes that will be accepted from incoming routing updates.

Applicable Platforms
Cisco IOS Devices With EIGRP Routing Capability

Impact
Router may accept route update messages from unintended entities.

Suggested Fix
Configure distribute-list for all EIGRP autonomous systems using the commands

\[
\text{router eigrp <autonomous system number>}
\]
\[
distribute-list <acl number> in !
\]

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL to be enforced</td>
<td>Desired ACL to be enforced. Leave blank to enforce no particular ACL ID</td>
<td>Required: false</td>
</tr>
</tbody>
</table>

Rule 4

Rule
Check that EIGRP outgoing distribute-list is configured [IOS]

Description
This rule checks that ip distribute-list is configured for each EIGRP autonomous system for advertising route updates. Communications between routers for routing table updates involve routing protocols. These updates provide directions to a router on which way traffic should be routed. You can use access lists to restrict what routes the router will accept (in) or advertise (out) via some routing protocols. The distribute-list acl-num out command is used to restrict routes that get distributed in routing updates, while the distribute-list acl-num in command may be used to filter routes that will be accepted from incoming routing updates.

Applicable Platforms
Cisco IOS Devices With EIGRP Routing Capability

Impact
Router may advertise route update messages to unintended entities.

Suggested Fix
Configure distribute-list for all EIGRP autonomous systems using the commands

\[
\text{router eigrp <autonomous system number>}
\]
\[
distribute-list <acl number> out !
\]
**OSPF**

**Description**
OSPF Related policies

**Applicable Platforms**
Cisco IOS Devices With OSPF Capability

**References**
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.4.3 Page 106 of Version 1.1c)

The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Cisco SAFE Compliance(Appendix A, Page 39 of A Security Blueprint for Enterprise Networks)
SAFE: A Security Blueprint for Enterprise Networks


Information Technology - Code of practice for information security management.

Defence Information System Agency(Section NET0400 of Dec 2, 2005)

DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

Department of Homeland Security (DHS) Compliance(Section 4.1, Page 19 of Version 2.0)

This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Center for Internet Security, Benchmark for Cisco IOS.(Section 2.3.2.3, Page: 44 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

**Rule 1**

**Rule**
Check MD5 Authentication [IOS]

**Description**
This rule checks to make sure that all the areas defined in all the OSPF processes use MD5 authentication. Router neighbor authentication is a mechanism that, when applied correctly, can prevent many routing attacks. Each router accomplishes authentication by the possession of an authentication key. That is, routers connected to the same network segment all use a shared secret key. Each sending router then uses this key to 'sign' each route table update message. The receiving router checks the shared secret to determine whether the message should be accepted.

**Applicable Platforms**
Cisco IOS Devices With OSPF Capability

**Impact**
This router is vulnerable to various routing attacks by spoofing the route table update messages.

**Suggested Fix**
Configure OSPF MD5 Authentication using the command

```
router ospf <process ID>
area <Area ID> authentication message-digest
```

**Rule 2**

**Rule**
Check interface state of OSPF routing updates [IOS]

**Description**
This rule checks that all the given interfaces are blocked/allowed from participating in OSPF routing updates. It goes through for every network in every OSPF process, and then gets a list of interfaces that belong to that network. It checks to see that if the given interfaces belong to the list above. If so, The interface is checked to see if it is passive or active interface and compared against the given policy. The passive-interface command is used to prevent other routers on the network from learning about routes dynamically. It can also be used to keep any unnecessary parties from learning about the existence of certain routes or routing protocols used. It is typically used when the wildcard specification on the network router configuration command configures more interfaces than desirable.

**Applicable Platforms**
Cisco IOS Devices With OSPF Capability
**Impact**
This interface may receive and transmit in OSPF routing updates, which means, unnecessary parties may learn about the existence of certain routes or routing protocols used. This also leads to higher chance of spoofed routing update attacks.

**Suggested Fix**
Configure the interface as a passive/active interface using the commands

```
router ospf <process ID>
[no] passive-interface <interface name> !
```

---

### Rule 3

**Rule**
Check that OSPF incoming distribute-list is configured [IOS]

**Description**
This rule checks that ip distribute-list is configured for each OSPF process for accepting route updates. Communications between routers for routing table updates involve routing protocols. These updates provide directions to a router on which way traffic should be routed. You can use access lists to restrict what routes the router will accept (in) or advertise (out) via some routing protocols. The distribute-list acl-num out command is used to restrict routes that get distributed in routing updates, while the distribute-list acl-num in command may be used to filter routes that will be accepted from incoming routing updates.

**Applicable Platforms**
Cisco IOS Devices With OSPF Capability

**Impact**
Router may accept route update messages from unintended entities.
Suggested Fix
Configure distribute-list for all OSPF processes using the commands

\[ \text{router ospf <process ID>} \]
\[ \text{distribute-list <acl number> in} \]

Rule 4

Rule
Check that OSPF outgoing distribute-list is configured [IOS]

Description
This rule checks that ip distribute-list is configured for each OSPF process for advertising route updates. Communications between routers for routing table updates involve routing protocols. These updates provide directions to a router on which way traffic should be routed. You can use access lists to restrict what routes the router will accept (in) or advertise (out) via some routing protocols. The distribute-list acl-num out command is used to restrict routes that get distributed in routing updates, while the distribute-list acl-num in command may be used to filter routes that will be accepted from incoming routing updates.

Applicable Platforms
Cisco IOS Devices With OSPF Capability

Impact
Router may advertise route update messages to unintended entities.

Suggested Fix
Configure distribute-list for all OSPF processes using the commands

\[ \text{router ospf <process ID>} \]
\[ \text{distribute-list <acl number> out} \]

Note
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.
RIP

Description
Routing Information Protocol (RIP) Related policies

Applicable Platforms
Cisco IOS Devices With RIP Routing Capability

References
Information Technology - Code of practice for information security management.
National Security Agency (NSA) Cisco Router Configuration Guide (Section 4.4.3 Page 110, Section 4.4.4 Page 121 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
Defence Information System Agency (Section NET0425 of Dec 2, 2005)
DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.
Center for Internet Security, Benchmark for Cisco IOS. (Section 2.3.2.4, Page: 45 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

Rule 1

Rule
Check State of RIP [IOS]

Description
This rule checks if RIP is enabled/disabled on the router based on the given policy.

Applicable Platforms
Cisco IOS Devices With RIP Routing Capability

Impact
None
**Suggested Fix**
Enable/Disable RIP using the commands

```plaintext
router rip
network <ip address>
```

**Rule 2**

**Rule**
Check global version of RIP [IOS]

**Description**
This Rule checks that the RIP is enabled with correct version. Note that this rule does not check the per interface override of the RIP version. By default, the software receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets. You can configure the software to receive and send only Version 1 packets. Alternatively, you can configure the software to receive and send only Version 2 packets.

**Applicable Platforms**
Cisco IOS Devices With RIP Routing Capability

**Impact**
None

**Suggested Fix**
Configure required version of RIP using the commands

```plaintext
router rip
version <RIP version>
```

**Rule 3**

**Rule**
Check all participating interfaces use MD5 Authentication [IOS]
Description
This Rule checks all interfaces that receive/transmit RIP information are configured with version 2 AND are configured with MD5 authentication. Router neighbor authentication is a mechanism that, when applied correctly, can prevent many routing attacks. Each router accomplishes authentication by the possession of an authentication key. That is, routers connected to the same network segment all use a shared secret key. Each sending router then uses this key to 'sign' each route table update message. The receiving router checks the shared secret to determine whether the message should be accepted.

Applicable Platforms
Cisco IOS Devices With RIP Routing Capability

Impact
This router is vulnerable to various routing attacks by spoofing the route table update messages.

Suggested Fix
Configure interface to use MD5 authentication for RIP communications the commands

```
router rip
version 2
interface <interface name >
ip rip receive version 2
ip rip send version 2
ip rip authentication mode md5
```

Rule 4

Rule
Check that RIP incoming distribute-list is configured

Description
This rule checks that ip distribute-list is configured in RIP for accepting route updates. Communications between routers for routing table updates involve routing protocols. These updates provide directions to a router on which way traffic should be routed. You can use access lists to restrict what routes the router will accept (in) or advertise (out) via some routing protocols. The distribute-list acl-num out command is used to restrict routes that get distributed in routing updates, while the distribute-list acl-num in command may be used to filter routes that will be accepted from incoming routing updates.

Applicable Platforms
Cisco IOS Devices With RIP Routing Capability

Impact
Router may accept route update messages from unintended entities.

Suggested Fix
Configure distribute-list for RIP using the commands

```
router rip  distribute-list <acl number> in
```
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 5

Rule
Check that RIP outgoing distribute-list is configured

Description
This rule checks that ip distribute-list is configured in RIP for advertising route updates. Communications between routers for routing table updates involve routing protocols. These updates provide directions to a router on which way traffic should be routed. You can use access lists to restrict what routes the router will accept (in) or advertise (out) via some routing protocols. The distribute-list acl-num out command is used to restrict routes that get distributed in routing updates, while the distribute-list acl-num in command may be used to filter routes that will be accepted from incoming routing updates.

Applicable Platforms
Cisco IOS Devices With RIP Routing Capability

Impact
Router may advertise route update messages to unintended entities.

Suggested Fix
Configure distribute-list for RIP using the commands

```bash
router rip
distribute-list <acl number> out
```

Rule 6

Rule
Check interface state of RIP routing updates [IOS]

Description
This rule checks that all the given interfaces are blocked/allowed from participating in RIP routing updates. It goes through for every network in RIP process, and then gets a list of interfaces that belong to that network. It checks to see that if the given interfaces belong to the list above. If so, The interface is checked to see if it is passive or active interface and compared against the given policy. The passive-interface command is used to prevent other routers on the network from learning about routes allowed.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL to be enforced</td>
<td>Desired ACL to be enforced. Leave blank to enforce no particular ACL ID</td>
<td>Required: false</td>
</tr>
</tbody>
</table>
Understanding Compliance and Audit Manager (CAAM) Policies

It can also be used to keep any unnecessary parties from learning about the existence of certain routes or routing protocols used. It is typically used when the wildcard specification on the network router configuration command configures more interfaces than desirable.

**Applicable Platforms**
Cisco IOS Devices With RIP Routing Capability

**Impact**
This interface may receive and transmit in RIP routing updates, which means, unnecessary parties may learn about the existence of certain routes or routing protocols used. This also leads to higher chance of spoofed routing update attacks.

**Suggested Fix**
Configure the interface as a passive/active interface using the commands

```bash
router RIP
[no] passive-interface <interface name>
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Group</td>
<td>List of interface groups to apply this policy.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td>Using Interface Group Editor option, you can add, remove or update Interface Group details. You can also change the order of the server details</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP State</td>
<td>List of interface groups to apply this policy.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td>Using RIP State Editor option, you can add, remove or update RIP State details. You can also change the order of the server details</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

**ACLs**

**Description**
Policies related to Access Control List Configurations.

**Applicable Platforms**
Cisco IOS Devices  
Cisco IOS Devices With RECEIVE_ACL Capability  
Cisco IOS Devices With TURBO_ACL Capability
Rule 1

Rule
Check if all ACLs have established keywords [IOS]

Description
This rule will check to make sure that all extended ACLs, that are used on any interface, has at least one Access Entry that permits traffic with TCP 'established' (ack or rst) flag. This will help in blocking packets from an external network that have only the SYN flag set. Thus, it allows traffic from TCP connections that were established from the internal network, and it denies anyone coming from any external network from starting any TCP connection. This is one of the ways to prevent TCP SYN attack, which involves transmitting a volume of connections that cannot be completed at the destination. This attack causes the connection queues to fill up, thereby denying service to legitimate TCP users.

Applicable Platforms
Cisco IOS Devices

Impact
This device may be vulnerable to TCP SYN attack originated from external network devices.

Suggested Fix
Modify the ACL by adding 'established' TCP flag for the permitted traffic in the access-list commands

```
access-list <number/name> <deny/permit> tcp <source> <destination> established
```

Rule 2

Rule
Check if Turbo ACLs are used [IOS]

Description
This rule checks if Turbo ACL feature is enabled on the device. The Turbo ACL feature compiles the ACLs into a set of lookup tables, while maintaining the first match requirements. Packet headers are used to access these tables in a small, fixed number of lookups, independently of the existing number of ACL entries.

Applicable Platforms
Cisco IOS Devices With TURBO_ACL Capability
Impact
Device performance can be improved by making use of this Turbo ACL feature

Suggested Fix
Enable Turbo ACL feature by using the command `access-list compiled`

Rule 3

Rule
ACL logging should not be turned on [IOS]

Description
ACL logging should not be turned on.

Applicable Platforms
Cisco IOS Devices

Impact
Turning on ACL logging can severely impact the system performance.

Suggested Fix
Do not turn on ACL logging in the access-list commands

```
ip access-list ... [log]
```

Rule 4

Rule
Check for Recieve ACL [IOS]

Description
IP Receive ACL can be used to restrict traffic that is destined to the router

Applicable Platforms
Cisco IOS Devices With RECEIVE_ACL Capability

Impact
No known impact.

Suggested Fix
Configure a receive ACL using the command:

```
ip receive access-list
```
Chapter 4 Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 5

Rule
Recieve ACL should not have entries with “any” source address [IOS]

Description
IP Receive ACL can be used to restrict traffic that is destined to the router.

Applicable Platforms
Cisco IOS Devices With RECEIVE_ACL Capability

Impact
If any of the ACL entry has source address as any, the device accepts traffic from all the sources defeating the purpose of having Receive ACL.

Suggested Fix
Configure a receive ACL using ip receive access-list and make sure that none of the ACL entries has any as the source address.

```
ip receive access-list <ACL>
```

CDP

Description
Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Applicable Platforms
Cisco IOS Devices

References
National Security Agency (NSA) Cisco Router Configuration Guide(Section 8.1(1) Page 274, 4.2.1 Page 70,72 of Version 1.1c)

The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
Understanding Compliance and Audit Manager (CAAM) Policies

Cisco SAFE Compliance(1.1b)
SAFE: A Security Blueprint for Enterprise Networks

National Security Agency (NSA) Cisco Switch Configuration Guide(Section 6.2.2, Page 18 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.

Department of Homeland Security (DHS) Compliance(section 4.2, Page 22 of Version 2.0)
This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.

Center for Internet Security, Benchmark for Cisco IOS.(Section 1.2.2.1, Page: 22 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

Rule 1

Rule
Check for CDP protocol state [IOS]

Description
The Cisco Discovery Protocol is a proprietary protocol that Cisco devices use to identify each other on a LAN segment. It is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Applicable Platforms
Cisco IOS Devices

Impact
CDP is useful only in specialized situations, and is considered deleterious to security.

Suggested Fix
To turn off CDP entirely, use the global configuration command no cdp run. In the unlikely event that CDP is needed for part of a network, it can be enabled and disabled for each interface. To enable CDP use the cdp run command in global configuration mode, and then disable it on each interface where it is not needed using the no cdp enable command in interface configuration mode. To enable/disable CDP globally, use the command: [no] cdp run
Rule 2

Rule

Check for CDP protocol state on the interface [IOS]

Description
The Cisco Discovery Protocol is a proprietary protocol that Cisco devices use to identify each other on a LAN segment. It is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Applicable Platforms
Cisco IOS Devices

Impact
CDP is useful only in specialized situations, and is considered deleterious to security.

Suggested Fix
To turn off CDP entirely, use the global configuration command no cdp run. In the unlikely event that CDP is needed for part of a network, it can be enabled and disabled for each interface. To enable CDP use the cdp run command in global configuration mode, and then disable it on each interface where it is not needed using the command:

```
interface <interface name>
[no] cdp enable
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>CDP protocol state on the device</td>
<td>Required: true, Default: false</td>
</tr>
<tr>
<td>Interface</td>
<td>CDP protocol state on the selected interfaces</td>
<td>Required: true, Default: false</td>
</tr>
<tr>
<td>Interfaces</td>
<td>List of interfaces or interface groups that should carry management traffic. Example valid Values: 'Any', 'AnyEthernet', 'FastEthernet', 'GigabitEthernet', 'FastEthernet0/1', 'FastEthernet0/.*' etc.</td>
<td>Required: true, Default: [Any]</td>
</tr>
</tbody>
</table>
Note

If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

Clock

Description
Clock and time zone related policies.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

References
Cisco SAFE Compliance(Clock of none)
SAFE: A Security Blueprint for Enterprise Networks
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 12.2, Page 47 of Version 1.0)

The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Cisco SAFE Compliance(1.1b)
SAFE: A Security Blueprint for Enterprise Networks

Rule 1

Rule
Summer time should not be configured [IOS, PIX, ASA]

Description
Check that summer time clock is not configured

Applicable Platforms
Cisco IOS Devices Cisco PIX Devices Running >= 7.x and ASA devices

Impact
Log files time-stamped with different time zones are difficult to correlate. This difficulty increases if the time stamps of individual logs need to be adjusted for summer time clock settings. These time-stamp adjustments can lead to errors when you correlate logs for several devices during root cause analysis in case of an attack on the network. If you are not using the local time zone on a device (that is, you are using UTC time zone across your network), do not use the summer time clock.
Suggested Fix
Disable summer time using the command

\texttt{no clock summer-time}

Rule 2

Rule
Check the configured Summer time [IOS, PIX, ASA]

Description
Check that the user defined summer time clock is configured.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
If you use local time zones, you should also configure the clock for summer time settings so that you can more easily compare log file entries with your current time.

Suggested Fix
Configure time zone and summer time mode setting using the command \texttt{clock summer-time}

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone Name</td>
<td>The name of the time zone (for example, PDT for Pacific Daylight Time) to be displayed when summer time is in effect.</td>
<td>Required: false</td>
</tr>
<tr>
<td>Mode</td>
<td>Whether the change to summer time is defined by a recurring rule that applies each year (Recurring), or by specific dates just for a single year (By Date).</td>
<td>Required: false</td>
</tr>
</tbody>
</table>

Rule 3

Rule
Check the configured time zone [IOS, PIX, ASA]

Description
Check that the device is configured to use the required time zone for the clock.
Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
Log files time-stamped with different time zones are difficult to correlate. This difficulty increases if the time stamps of individual logs need to be adjusted for different time zone settings. These time-stamp adjustments can lead to errors when you correlate logs for several devices during root cause analysis in case of an attack on the network. If you manage devices in more than one time zone, consider using a single time zone for the clock.

Suggested Fix
Configure timezone using the command

\textit{clock timezone}

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone Name</td>
<td>The name of the time zone; The default is UTC</td>
<td>Required: false</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offset, in hours, from UTC</td>
<td>The offset, in hours, from UTC. The default is 0</td>
<td>Required: false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min Value: -23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max Value: 23</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offset, in minutes</td>
<td>Offset, in minutes. The default is 0.</td>
<td>Required: false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min Value: 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max Value: 59</td>
</tr>
</tbody>
</table>

Miscellaneous Services On Firewalls

Description
Miscellaneous policies specific to Firewall devices.

Applicable Platforms
Cisco PIX Devices Running >= 7.x and ASA device

References
Cisco SAFE Compliance
SAFE: A Security Blueprint for Enterprise Networks
Center for Internet Security, Benchmark for Cisco PIX/ASA.(Section 1.2.2.1, Page: 19; Section 1.3.1.3, Section 1.3.1.4, Page: 27 ; Section 1.3.1.7, Page: 29; Section 1.3.3.1, Page: 33 of Version 2.0, Nov 2007)
CIS PIX/ASA benchmark recommends the prudent level of minimum due care for operating system security. CIS PIX/ASA benchmark contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All PIX devices should implement these settings.

### Rule 1

**Rule**
Check that DHCP server is not configured [PIX. ASA]

**Description**
The Dynamic Host Configuration Protocol (DHCP) server supplies automatic configuration parameters to Internet hosts.

**Applicable Platforms**
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
DHCP provides a service that can be used for denial-of-service (DoS) attacks.

**Suggested Fix**
Use a dedicated server to provide DHCP services instead of the firewall. Disable dhcp server using the command: no dhcpd enable <interface>

### Rule 2

**Rule**
Check maximum NAT translation timeout [PIX. ASA]

**Description**
Check that the specified address translation slot timeout value is configured on the device.

**Applicable Platforms**
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
Cisco PIX Devices Running >= 7.x and ASA devices

**Suggested Fix**
Configure the NAT Translation Slot Timeout with the desired value using the command:

```bash
timeout xlate```

**Rule 3**

**Rule**
Check maximum allowed packet fragments [PIX, ASA]

**Description**
By default, the PIX Firewall accepts up to 24 fragments to reconstruct a full IP packet. Based on your network security policy, consider configuring the PIX Firewall to prevent fragmented packets from traversing the firewall

**Applicable Platforms**
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
Fragmented packets are often used as Denial-of-Service attacks

**Suggested Fix**
Configure fragment chain command on each interface to allow desired number of packet fragments. Select a value of 1 to prevent receiving packet fragments.

```
fragment chain 1 <interface name>
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Translation Slot Timeout (minutes)</td>
<td>The length of time used to identify the translation slot as idle.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Max Packet Fragments Allowed</td>
<td>Maximum number of packets fragments allowed on an interface. A value of 1 indicates that fragments are not allowed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Rule 4**

**Rule**
Check that Unicast Reverse Path Forwarding (RPF) is enabled on interfaces [PIX, ASA]

**Description**
Check that unicast reverse path forwarding (RPF) is enabled on interfaces.

**Applicable Platforms**
Cisco PIX Devices Running >= 7.x and ASA devices
Impact
Many network attacks rely on an attacker falsifying (spoofing) the source addresses of IP datagrams. Some attacks depend on spoofing, while other attacks are much harder to trace if the attacker can use somebody else's address. Therefore, you should prevent spoofing wherever feasible.

Suggested Fix
Configure RPF check on the interfaces using command:

\textit{ip verify reverse-path interface <interface name>}

Rule 5

Rule
Check maximum timeout for idle session [PIX, ASA]

Description
Check that the specified timeout for idle sessions is configured on the device.

Applicable Platforms
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
This timeout command sets the idle time for connection slots. If the slot has not been used for the idle time specified, the resource is returned to the free pool. This reduces the risk of someone from accessing an already established but idle connection.

Suggested Fix
Configure the Idle Session Timeout with the desired value using the command:

\textit{timeout conn}

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Idle Session Timeout(Minutes) | The length of time used to identify the session as idle. | Required: true  
Default: 60  
Value: 1 Max  
Value: 71580 |

NTP Configuration

Description
The Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP is designed to make time synchronization automatic and efficient across all devices in the network. Having accurate time is important for security, especially for intrusion and forensic analysis.
Applicable Platforms
Cisco IOS Devices With SNTP Capability
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

References
Payment Card Industry Data Security Standard(PCI).(10.4 of Version 1.1, September, 2006)
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.2.1 Page 71, Section 4.5.2 Page 149 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
Information Technology - Code of practice for information security management.
National Security Agency (NSA) Cisco Switch Configuration Guide(Section 12.2, Page 46 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (e.g., switches) which are part of their computer networks.
Cisco SAFE Compliance(1.1b)
SAFE: A Security Blueprint for Enterprise Networks
Defence Information System Agency(Section NET0810 of Dec 2, 2005)
DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.
Department of Homeland Security (DHS) Compliance(Section 3.2, Page 16 of Version 2.0)
This document is being distributed to provide Department of Homeland Security (DHS) Cisco Router systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when an existing Cisco Router is being installed or configured. All settings and parameters presented in this document are the baseline security which all Cisco Router systems must meet.
Center for Internet Security, Benchmark for Cisco IOS.(Section 1.2.4, Page: 31 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

### Rule 1

**Rule**
Check device state as NTP server [IOS]

**Description**
All devices in the network should be configured to synchronize their times with an authoritative NTP Server. It is recommended that the border router be configured to synchronize time from at least two reliable NTP servers and all the devices in the protected network can be configured as clients to this border router.

**Applicable Platforms**
Cisco IOS Devices With NTP_SERVER Capability

**Impact**
Unless all the devices are properly configured to synchronize the time, the event logs coming from different devices would have different time stamps. This makes it very hard to analyze the logs in terms of intrusion detection and forensics.

**Suggested Fix**
Configure ntp server using the command

\[
\text{[no] ntp master}
\]

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server</td>
<td>Desired state of the NTP server configuration</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>

### Rule 2

**Rule**
Check device state as NTP/SNTP Client [IOS]

**Description**
All devices in the network should be configured to synchronize their times with an authoritative NTP Server. It is recommended that the border router be configured to synchronize time from at least two reliable NTP servers and all the devices in the protected network can be configured as clients to this border router.
Applicable Platforms
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With SNTP Capability
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
Unless all the devices are properly configured to synchronize the time, the event logs coming from different devices would have different time stamps. This makes it very hard to analyze the logs in terms of intrusion detection and forensics.

Suggested Fix
Configure ntp client using the commands

[no] ntp server

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP Client</td>
<td>Desired state of the NTP client configuration</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: true</td>
</tr>
</tbody>
</table>

Rule 3

Rule
Check to allow NTP only from these interfaces [IOS]

Description
This rule checks whether all the interfaces that should not participate in NTP communications, are blocked from receiving any NTP packets. Please note that it does not check whether given interfaces are enabled/disabled to receive NTP packets, but checks to make sure all other interfaces are blocked.

Applicable Platforms
Cisco IOS Devices With NTP_CLIENT Capability

Impact
Non-necessary interfaces will be participating in NTP communications and will act as NTP servers.

Suggested Fix
Disable NTP on the interface using the commands interface

<interface name> ntp disable
Rule 4

Rule
Check if NTP servers are configured [IOS, PIX, ASA]

Description
All devices in the network should be configured to synchronize their times with an authoritative NTP Server. It is recommended that the border router be configured to synchronize time from at least two reliable NTP servers and all the devices in the protected network can be configured as clients to this border router.

Applicable Platforms
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With SNTP Capability
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
Unless all the devices are properly configured to synchronize the time, event logs coming from different devices would have different time stamps. This makes it very hard to analyze the logs in terms of intrusion detection and forensics.

Suggested Fix
Configure the device to synchronize clock from the desired NTP servers using the command

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Groups</td>
<td>Desired list of interfaces to make sure all other interfaces are blocked from using NTP. (Empty list means all interfaces should be blocked from using NTP). Using Interface Groups Editor option, you can add, or remove Interface Groups details. You can also change the order of the server details.</td>
<td>Required: false</td>
</tr>
</tbody>
</table>

Rule 5

Rule
Check if configured number of NTP servers is at least [IOS, PIX, ASA]

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>IP Address(es) of desired NTP Server(s). Using Servers Editor option, you can add, remove or update Servers details. You can also change the order of the server details</td>
<td>Required: true</td>
</tr>
</tbody>
</table>
Description
All devices in the network should be configured to synchronize their times with an authoritative NTP Server. It is recommended that the border router be configured to synchronize time from at least two reliable NTP servers and all the devices in the protected network can be configured as clients to this border router.

Applicable Platforms
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With SNTP Capability
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
Unless all the devices are properly configured to synchronize the time, event logs coming from different devices would have different time stamps. This makes it very hard to analyze the logs in terms of intrusion detection and forensics.

Suggested Fix
Configure the device to synchronize clock from the desired NTP servers using the command

\texttt{ntp server}

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Minimum number of NTP servers | Minumim number of NTP servers | Required: true  
Min Value: 1  
Max Value: 2147483647 |

Rule 6

Rule
Make sure NTP packets are authenticated[IOS, PIX, ASA]

Description
Whenever possible, all the packets should be configured to be authenticated.

Applicable Platforms
Cisco IOS Devices With NTP_CLIENT Capability Cisco PIX Devices Running >= 7.x and ASA devices

Impact
NTP packets are not authenticated

Suggested Fix
Configure the device to use authentication of NTP packets using the command ntp authenticate
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 7

Rule
Check NTP Server Access is restricted [IOS, PIX, ASA]

Description
Make sure that NTP server access is controlled.

Applicable Platforms
Cisco IOS Devices With NTP_SERVER Capability

Impact
NTP packets are not controlled.

Suggested Fix
Configure the device to control the NTP packets using the command
ntp access-group (peer | serve | server-only | query-only) <acl-number>

Note
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

Device Version Checks

Description
This policy verifies the operating system versions on the devices and make sure they are as per the defined requirements.

Applicable Platforms
NA

References
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.1.2, Page 57 of Version 1.1c)

The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Center for Internet Security, Benchmark for Cisco PIX/ASA.(Section 1.3.1.2, Page: 26 of Version 2.0, Nov 2007)

CIS PIX/ASA benchmark recommends the prudent level of minimum due care for operating system security. CIS PIX/ASA benchmark contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All PIX devices should implement these settings.
Rule 1

**Rule**
Check for Required OS Versions

**Description**
This rule checks that all selected devices are running accepted OS versions

**Impact**
No known impact.

**Suggested Fix**
Change the OS version of the device by loading one of the accepted versions.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System Type</td>
<td>Type of Operating System. Using Operating System Type Editor option, you can add, remove or update Operating System Type details. You can also change the order of the server details</td>
<td>Required: true</td>
</tr>
<tr>
<td>Match Condition Type</td>
<td>Select whether all the version expressions should match or at least one of the version expression should match in order for the validation to be successful. Using Match Condition Type Editor option, you can add, remove or update Match Condition Type details. You can also change the order of the server details</td>
<td>Required: true, Default: false</td>
</tr>
<tr>
<td>Accepted Version Expressions</td>
<td>List of OS Version Expressions that are acceptable. A &quot;Version Expression&quot; is an operator followed by version string. Valid operators are &quot;=&quot; (equals), &quot;!=&quot; (Not Equals), &quot;&gt;&quot; (Greater Than), &quot;&gt;=&quot; (Greater Than Or Equals), &quot;&lt;&quot; (Less Than), &quot;=&lt;&quot; (Less Than Or Equals), &quot;<del>&quot; (Matches a regular expression), &quot;!</del>&quot; (Does not match a regular expression). Using Accepted Version Expressions Editor option, you can add, remove or update Accepted Version Expressions details. You can also change the order of the server details</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

Configuration Management with Cisco Prime LAN Management Solution 4.2
Devices Running outdated OS Versions

Description
This policy verifies if any of the devices selected are running outdated operating systems as per the End Of Life/End Of Sales Announcements by vendors.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CATOS Devices

References
Cisco End Of Life/End Of Sales Announcements
Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology.

Rule 1

Rule
Verify that software is not announced to be End Of Life [IOS, PIX, ASA, CatOS]

Description
Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CATOS Devices

Impact
If the device is not upgraded to the next version of operating system, the support of this device may end soon.

Suggested Fix
Upgrade to next available version of software as soon as possible

Rule 2

Rule
Verify that software has not reached End Of Sale [IOS, PIX, ASA, CatOS]
Description
Software running on this device has reached End of Sale milestone. The software release may no longer be ordered. Releases which reach this milestone are still available for customers under maintenance contract or for Customer Service Engineering (CSE) support until they reach the "End-of-Life" milestone. Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CATOS Devices

Impact
If the device is not upgraded to the next version of operating system, the support of this device may end soon.

Suggested Fix
Upgrade to next available version of software as soon as possible

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time in years.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Right Now</td>
</tr>
</tbody>
</table>

Rule 3

Rule
Verify that software has not reached End Of Engineering Maintenance [IOS, PIX, ASA, CatOS]

Description
Software running on this device has reached End of Engineering milestone. After this milestone, no scheduled maintenance releases will be produced for the major release. Releases which reach this milestone are still available for customers under maintenance contract or for CSE support until they reach the "End-of-Life" milestone. Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
Cisco IOS Devices Cisco PIX and ASA Firewalls Cisco CATOS Devices
Impact
If the device is not upgraded to the next version of operating system, the support of this device may end soon.

Suggested Fix
Upgrade to next available version of software as soon as possible

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time in years.</td>
<td>Required: true; Default: Right Now</td>
</tr>
</tbody>
</table>

Rule 4

Rule
Verify that software has not reached End Of Contract Renewal Maintenance [IOS, PIX, ASA, CatOS]

Description
This software has reached End of Contract Renewal milestone. After this milestone, service contracts are no longer renewed

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CATOS Devices

Impact
If the device is not upgraded to the next family of devices, the support of this device may end soon.

Suggested Fix
*Upgrade to next available family of devices as soon as possible*

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time in years.</td>
<td>Required: true; Default: Right Now</td>
</tr>
</tbody>
</table>

Rule 5

Rule
Verify that software has not reached End Of Life (Support) [IOS, PIX, ASA, CatOS]

Description
Software running on this device has reached End of Life milestone. After this milestone date, the software release is no longer officially supported by the vendor. Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are
replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CATOS Devices

Impact
If the device is not upgraded to the next version of operating system, the support of this device may end soon.

Suggested Fix
Upgrade to next available version of software as soon as possible

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time in years.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Right Now</td>
</tr>
</tbody>
</table>

Devices with outdated modules

Description
This policy verifies if any of the devices selected are installed with outdated modules as per the End Of Life/End Of Sales Announcements by vendors.

Applicable Platforms
Cisco IOS Devices Cisco PIX and ASA Firewalls Cisco CATOS Devices

References
Cisco End Of Life/End Of Sales Announcements

Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology.

Rule 1

Rule
Verify that none of the modules are announced to be End Of Life [IOS, PIX, ASA, CatOS]

Description
Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.
Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CATOS Devices

Impact
If the device is not migrated to the prescribed modules, the support of these modules may end soon.

Suggested Fix
Migrate to the prescribed modules.

Rule 2

Rule
Verify that none of the modules have reached End Of Sale [IOS, PIX, ASA, CatOS]

Description
This device has modules that reached End of Sale milestone. The hardware may no longer be ordered. Modules which reach this milestone are still available for customers under maintenance contract or for Customer Service Engineering (CSE) support until they reach the "End-of-Life" milestone. Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CATOS Devices

Impact
If the device is not migrated to the prescribed modules, the support of these modules may end soon.

Suggested Fix
Migrate to the prescribed modules.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time in years.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Right Now</td>
</tr>
</tbody>
</table>
Rule 3

Rule
Verify that none of the modules have reached End Of Engineering Maintenance [IOS, PIX, ASA, CatOS]

Description
This device has modules that reached End Of Engineering milestone. The hardware may no longer be ordered. After this milestone, no scheduled maintenance releases will be produced for the major release. Modules which reach this milestone are still available for customers under maintenance contract or for CSE support until they reach the "End-of-Life" milestone. Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CATOS Devices

Impact
If the device is not migrated to the prescribed modules, the support of these modules may end soon.

Suggested Fix
Migrate to the prescribed modules.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time in years.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Right Now</td>
</tr>
</tbody>
</table>

Rule 4

Rule
Verify that none of the modules have reached End Of Contract Renewal Maintenance [IOS, PIX, ASA, CatOS]

Description
This device has modules that have reached End of Contract Renewal milestone. After this milestone, service contracts are no longer renewed

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CATOS Devices
Impact
If the device is not upgraded to the prescribed modules, the support of these modules may end soon.

Suggested Fix
Upgrade to prescribed modules as soon as possible

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time in years.</td>
<td>Required: true, Default: Right Now</td>
</tr>
</tbody>
</table>

Rule 5

Rule
Verify that none of the modules reached End Of Life (Support) [IOS, PIX, ASA, CatO]

Description
This device has modules that reached End of Life milestone. After this milestone date, the modules are no longer officially supported by the vendor. Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CATOS Devices

Impact
If the device is not upgraded to the prescribed modules, the support of these modules may end soon.

Suggested Fix
Upgrade to prescribed modules as soon as possible

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time in years.</td>
<td>Required: true, Default: Right Now</td>
</tr>
</tbody>
</table>
Outdated Devices As Per Vendor Specific EOL/EOS Announcement

Description
This policy verifies if any of the devices selected are outdated as per the Cisco Hardware End Of Life/End Of Sales Announcements.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CatOS Devices

References
Cisco End Of Life/End Of Sales Announcements

Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology.

Rule 1

Rule
Verify that device is announced to be End Of Life [IOS, PIX, ASA, CatOS]

Description
Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CatOS Devices

Impact
If the device is not upgraded to the next family of devices, the support of this device may end soon.

Suggested Fix
Upgrade to next available family of devices as soon as possible

Rule 2

Rule
Verify that device has not reached to be End Of Sale [IOS, PIX, ASA, CatOS]
Chapter 4 Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Description
This device has reached End of Sale milestone. The hardware may no longer be ordered. Devices which reach this milestone are still available for customers under maintenance contract or for Customer Service Engineering (CSE) support until they reach the "End-of-Life" milestone. Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
- Cisco IOS Devices
- Cisco PIX and ASA Firewalls
- Cisco CatOS Devices

Impact
If the device is not upgraded to the next family of devices, the support of this device may end soon.

Suggested Fix
Upgrade to next available family of devices as soon as possible

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time in years.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Right Now</td>
</tr>
</tbody>
</table>

Rule 3

Rule
Verify that device has not reached End Of Engineering Maintenance [IOS, PIX, ASA, CatOS]

Description
This device has reached End of Engineering milestone. After this milestone, no scheduled maintenance releases will be produced for the major release. Upgrades and releases for devices which reach this milestone are still available for customers under maintenance contract or for CSE support until they reach the "End-of-Life" milestone. Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
- Cisco IOS Devices
- Cisco PIX and ASA Firewalls
- Cisco CatOS Devices
Impact
If the device is not upgraded to the next family of devices, the support of this device may end soon.

Suggested Fix
Upgrade to next available family of devices as soon as possible

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time in years.</td>
<td>Required: true Default: Right Now</td>
</tr>
</tbody>
</table>

Rule 4

Rule
Verify that device has not reached End Of Contract Renewal Maintenance [IOS, PIX, ASA, CatOS]

Description
This device has reached End of Contract Renewal milestone. After this milestone, service contracts are no longer renewed

Applicable Platforms
Cisco IOS Devices Cisco PIX and ASA Firewalls Cisco CatOS Devices

Impact
If the device is not upgraded to the next family of devices, the support of this device may end soon.

Suggested Fix
Upgrade to next available family of devices as soon as possible

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time in years.</td>
<td>Required: true Default: Right Now</td>
</tr>
</tbody>
</table>

Rule 5

Rule
Verify that device has not reached End Of Life (Support)[IOS, PIX, ASA, CatOS]

Description
This device has reached End of Life milestone. After this milestone date, the device is no longer officially supported by the vendor. Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CatOS Devices

**Impact**
If the device is not upgraded to the next family of devices, the support of this device may end soon.

**Suggested Fix**
Upgrade to next available family of devices as soon as possible

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time in years.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Right Now</td>
</tr>
</tbody>
</table>

**IEEE 802.1X Port-Based Authentication**

**Description**
The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port and assigns the port to a VLAN before making available any services offered by the switch or the LAN. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

**Applicable Platforms**
Cisco IOS Switches With DOT1X Capability

**References**
National Security Agency (NSA) Cisco Switch Configuration Guide (Section 13.2 Page 52 of Version 1.0)

The Cisco IOS Switch Security Configuration Guide from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (for example, switches) which are part of their computer networks.

**Rule 1**

**Rule**
Check global state of IEEE 802.1X Port-Based Authentication state [IOS]
Description
This check will make sure IEEE 802.1X Port-Based Authentication state on the device to required state as per the policy.

Applicable Platforms
Cisco IOS Switches With DOT1X Capability

Impact
Any device connected to an unused port on the switch can start receiving/transmitting packets from/to the switch.

Suggested Fix
Configure dot1x authentication on the device globally using the command:

\[ \text{no} \text{ dot1x system-auth-control} \]

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired state of 802.1X Authentication</td>
<td>Desired state of 802.1X Authentication</td>
<td>Required: true Default: false</td>
</tr>
</tbody>
</table>

Rule 2

Rule
Check state of IEEE 802.1X Port-Based Authentication state on given interfaces [IOS].

Description
This check will make sure IEEE 802.1X Port-Based Authentication state on the given interfaces to required state as per the policy.

Applicable Platforms
Cisco IOS Switches With DOT1X Capability

Impact
Any device connected to an unused port on the switch can start receiving/transmitting packets from/to the switch.

Suggested Fix
Configure dot1x authentication on the device globally and/or on specific interfaces using the commands:

\[ \text{no} \text{ dot1x system-auth-control} \]

\[ \text{interface <interface name>} \]

\[ \text{dot1x port-control} \]

Note You can add or remove the interface group and authentication state. You can also change the order of the details.
Note
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

---

**IOS Software SIP DoS Vulnerability - 112248**

**Description**

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

**Applicable Platforms**

Cisco IOS Devices

**References**

CISCO PSIRT Advisories and Notices (112248 of 1.1)

Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PSIRT - 112248: Verify IOS Software SIP DoS Vulnerability [IOS].

**Description**

Cisco devices are affected when they are running affected Cisco IOS Software and Cisco IOS XE Software versions that are configured to process SIP messages.

Recent versions of Cisco IOS Software do not process SIP messages by default. Creating a dial peer by issuing the dial-peer voice configuration command will start the SIP processes, causing the Cisco IOS device to process SIP messages. In addition, several features within Cisco Unified Communications Manager Express, such as ePhones, will also automatically start the SIP process when they are configured, causing the device to start processing SIP messages.
An example of an affected configuration follows:

dial-peer voice <Voice dial-peer tag> voip

In addition to inspecting the Cisco IOS device configuration for a `dial-peer` command that causes the device to process SIP messages, administrators can also use the `show processes | include SIP` command to determine whether Cisco IOS Software is running the processes that handle SIP messages. In the following example, the presence of the processes `CCSIP_UDP_SOCKET` or `CCSIP_TCP_SOCKET` indicates that the Cisco IOS device will process SIP messages:

```
Router# show processes | include SIP
149 Mwe 40F48254  4  1  400023108/24000  0 CCSIP_UDP_SOCKET
150 Mwe 40F48034  4  1  400023388/24000  0 CCSIP_TCP_SOCKET
```

Note
Because there are several ways a device running Cisco IOS Software can start processing SIP messages, it is recommended that the `show processes | include SIP` command be used to determine whether the device is processing SIP messages instead of relying on the presence of specific configuration commands.

Cisco Unified Border Element images are also affected by two of these vulnerabilities.

Note
The Cisco Unified Border Element feature (CUBE – previously known as the Cisco Multiservice IP-to-IP Gateway) is a special Cisco IOS Software image that runs on Cisco multiservice gateway platforms. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking.

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the `show version` command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to Cisco Internetwork Operating System Software or Cisco IOS Software. The image name displays in parentheses, followed by Version and the Cisco IOS Software release name. Other Cisco devices do not have the `show version` command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 15.0(1)M1 with an installed image name of C3900-UNIVERSALK9-M:

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team

--- output truncated
```


Cisco IOS XE Software is affected by these vulnerabilities.

Note
Cisco Unified Communications Manager is affected by one of the vulnerabilities described in this advisor. A separate Cisco Security Advisory has been published to disclose the vulnerability that affects the Cisco Unified Communications Manager at the following location:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-cucm
Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerabilities in this advisory may result in system instabilities or a reload of an affected device. Repeated exploitation could result in a sustained denial of service condition.

Suggested Fix
If the affected Cisco IOS device requires SIP for VoIP services, SIP cannot be disabled, and no workarounds are available. Users are advised to apply mitigation techniques to help limit exposure to the vulnerabilities. Mitigation consists of allowing only legitimate devices to connect to affected devices. To increase effectiveness, the mitigation must be coupled with anti-spoofing measures on the network edge. This action is required because SIP can use UDP as the transport protocol.

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco Voice Products.

Disabling SIP Listening Ports
For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. Some versions of Cisco IOS Software allow administrators to disable SIP with the following commands:

```plaintext
sip-ua
  no transport udp
  no transport tcp
  no transport tcp tls
```

Warning
When applying this workaround to devices that are processing Media Gateway Control Protocol (MGCP) or H.323 calls, the device will not stop SIP processing while active calls are being processed. Under these circumstances, this workaround should be implemented during a maintenance window when active calls can be briefly stopped.

The `show udp connections`, `show tcp brief all`, and `show processes | include SIP` commands can be used to confirm that the SIP UDP and TCP ports are closed after applying this workaround.

Depending on the Cisco IOS Software version in use, when SIP is disabled the output from the `show ip sockets` command may still show the SIP ports open, but sending traffic to them will cause the SIP process to emit the following message:

```plaintext
*Jun 2 11:36:47.691: sip_udp_sock_process_read: SIP UDP Listener is DISABLED
```

Control Plane Policing
For devices that need to offer SIP services, it is possible to use Control Plane Policing (CoPP) to block SIP traffic to the device from untrusted sources. Cisco IOS Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations.
The following example can be adapted to specific network configurations:

```plaintext
!-- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.
!-- Everything else is not trusted. The following access list is used
!-- to determine what traffic needs to be dropped by a control plane
!-- policy (the CoPP feature): if the access list matches (permit)
!-- then traffic will be dropped and if the access list does not
!-- match (deny) then traffic will be processed by the router.
access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5061
access-list 100 deny udp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5061
access-list 100 permit udp any any eq 5060
access-list 100 permit tcp any any eq 5060
access-list 100 permit tcp any any eq 5061

!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices.
!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature.
class-map match-all drop-sip-class
   match access-group 100

!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.
policy-map control-plane-policy
class drop-sip-class
drop

!-- Apply the Policy-Map to the Control-Plane of the
!-- device.
control-plane
  service-policy input control-plane-policy
```

**Note** Because SIP can use UDP as a transport protocol, it is possible to spoof the source address of an IP packet, which may bypass access control lists that permit communication to these ports from trusted IP addresses.

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the permit action result in these packets being discarded by the policy-map drop function, while packets that match the deny action (not shown) are not affected by the policy-map drop function. Additional information on the configuration and use of the CoPP feature can be found at [http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html](http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html) and [http://www.cisco.com/en/US/docs/ios/redirect/eol.html](http://www.cisco.com/en/US/docs/ios/redirect/eol.html).

**Management VLAN**

**Description**
Management VLAN allows out-of-band management of network devices separating management traffic from user traffic.

**Applicable Platforms**
Cisco IOS Switches
References

National Security Agency (NSA) Cisco Switch Configuration Guide (Section 9.2 Page 32 of Version 1.0)

The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (for example, switches) which are part of their computer networks.

Rule 1

Rule

Check management VLAN is configured [IOS].

Description

This check will make sure there is a designated VLAN is configured for management and that the policy requirements given in other rules in the policy are satisfied for this management VLAN. It is a good practice to separate the management VLAN from the user or server VLAN. With this separation, any broadcast/packet storm that occurs in the user or server VLAN does not affect the management of switches. Do not use VLAN 1 for management. All ports in Cisco switches default to VLAN 1, and any devices that connect to nonconfigured ports are in VLAN 1. The use of VLAN 1 for management can cause potential issues for the management of switches, as the first tip explains.

Applicable Platforms

Cisco IOS Switches

Impact

None

Suggested Fix

Separate the management VLAN from the user or server VLAN. With this separation, any broadcast/packet storm that occurs in the user or server VLAN does not affect the management of switches. Do not use VLAN 1 for management. To provide network-based, out-of-band management, dedicate a physical switch port and VLAN on each switch for management use. Create a Switch Virtual Interface (SVI) Layer Three interface for that VLAN, and connect the VLAN to a dedicated switch and communications path back to the management hosts. Do not allow the operational VLANs access to the management VLAN. Also, do not trunk the management VLAN off the switch. To configure a management VLAN interface on the switch, use the command:

```
interface vlan<management vlan ID>
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designated Management VLAN</td>
<td>VLAN number designated as a management VLAN</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min Value: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max Value: 4094</td>
</tr>
</tbody>
</table>
Rule 2

Rule
Check management traffic allowed only on these interfaces/interface groups [IOS].

Description
This check will make sure that only designated management interfaces allow the management traffic.

Applicable Platforms
Cisco IOS Switches

Impact
Management traffic will be allowed by interfaces that are not designated to receive it.

Suggested Fix
Remove management VLAN from non-management interfaces using the command:

```
interface <interface name>
switchport access vlan
```
or

```
switchport trunk allowed vlan remove <management vlan ID>
```

<table>
<thead>
<tr>
<th>Rule Description Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management interfaces</td>
</tr>
<tr>
<td>List of interfaces or interface groups that should carry management traffic.</td>
</tr>
<tr>
<td>Valid Values—Any, AnyEthernet, FastEthernet, GigabitEthernet, FastEthernet0/1, FastEthernet0/.* and so on.</td>
</tr>
<tr>
<td>Required: true</td>
</tr>
</tbody>
</table>

Rule 3

Rule
Check management VLAN access is restricted using an Access Control List [IOS].

Description
This check will make sure that management VLAN access is restricted with a given access control.

Applicable Platforms
Cisco IOS Switches

Impact
Management VLAN access is not restricted and could be exploited.
Suggested Fix
Restrict management VLAN with an access control list using the command:

```plaintext
interface vlan<management vlan ID>
ip access-group <access list number or name> in
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control List</td>
<td>Access Control List to restrict the management</td>
<td>Required: true</td>
</tr>
<tr>
<td>traffic.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note**
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

**IOS Software IPv6 DoS Vulnerability - 112252**

**Description**
Cisco IOS Software contains a vulnerability in the IP version 6 (IPv6) protocol stack implementation that could allow an unauthenticated, remote attacker to cause a reload of an affected device that has IPv6 operation enabled. The vulnerability is triggered when an affected device processes a malformed IPv6 packet.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices (112252 of 1.1)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT - 112252: Verify IOS Software IPv6 DoS Vulnerability [IOS]

**Description**
Cisco devices that are running an affected version of Cisco IOS Software and configured for IPv6 operation are affected. A device that is running Cisco IOS Software and that has IPv6 enabled will show some interfaces with assigned IPv6 addresses when the `show ipv6 interface brief` command is executed.

The `show ipv6 interface brief` command will produce an error message if the running version of Cisco IOS Software does not support IPv6, or will not show any interfaces with IPv6 address if IPv6 is disabled. The system is not vulnerable in either of these scenarios.

Sample output of the `show ipv6 interface brief` command on a system that is configured for IPv6 operation follows:

```plaintext
router>show ipv6 interface brief
FastEthernet0/0 [up/up]
```
Understanding Compliance and Audit Manager (CAAM) Policies

Alternatively, the IPv6 protocol is enabled if the interface configuration command `ipv6 address <IPv6 address>` or `ipv6 enable` is present in the configuration. Both may be present, which the vulnerable configuration in the following example shows:

```
interface FastEthernet0/1
  ipv6 address 2001:0DB8:C18:1::/64 eui-64
!
interface FastEthernet0/2
  ipv6 enable
```

A device that is running Cisco IOS Software and has IPv6 enabled on a physical or logical interface is vulnerable even if `ipv6 unicast-routing` is globally disabled (that is, the device is not routing IPv6 packets). FIXME—Remove this since it is at the top. Administrators can use the `show ipv6 interface brief` command to determine whether IPv6 is enabled on any interface.

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the `show version` command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to Cisco Internetwork Operating System Software or Cisco IOS Software. The image name displays in parentheses, followed by Version and the Cisco IOS Software release name. Other Cisco devices do not have the `show version` command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 15.0(1)M1 with an installed image name of C3900-UNIVERSALK9-M:

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team

--- output truncated
```

Additional information about Cisco IOS Software release naming conventions is available in the white paper Cisco IOS and NX-OS Software Reference Guide.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability that is described in this advisory may cause a reload of an affected device. Repeated exploitation could result in a sustained denial of service condition.

Suggested Fix
There are no workarounds for this vulnerability if IPv6 configuration is required.
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

IOS Software Data Link Switching Vulnerability - 112254

Description
Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (112254 of 1.1)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 112254: Verify IOS Software Data Link Switching Vulnerability [IOS].

Description
Cisco IOS devices with the DLSw promiscuous feature enabled are affected by the vulnerability described in this advisory. Devices with the DLSw promiscuous feature enabled contain a line in the configuration defining a local DLSw peer with the promiscuous keyword. This configuration can be observed by issuing the command `show running-config`. Systems configured with the DLSw promiscuous feature enabled contain a line similar to one of the following:

```
dlsw local-peer promiscuous
```

or

```
dlsw local-peer peer-id <IP address> promiscuous
```

To determine the software that runs on a Cisco IOS device, log in to the device and issue the show version command to display the system banner. Cisco IOS Software identifies itself as Cisco Internetwork Operating System Software or Cisco IOS Software. Other Cisco devices do not have the `show version` command or give different output.

The following example shows output from a device running IOS version 15.0(1)M1:

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod rel team
```

Additional information about Cisco IOS Software release naming conventions is available in the white paper `Cisco IOS and NX-OS Software Reference Guide` at:

```
http://www.cisco.com/web/about/security/intelligence/ios-ref.html
```

Applicable Platforms
Cisco IOS Devices
Impact

Successful exploitation of the vulnerability may result in a memory leak that can lead to a denial of service condition. Memory exhaustion can cause an affected Cisco IOS device to reload or become unresponsive; a power cycle might be required to recover from the condition.

To identify the memory leak caused by this vulnerability, issue the `show dlsw peers | include FST.*DISCONN` command; a monotonically increasing list of FST peers that remain in the DISCONN state indicates that memory is being held, as shown in the following example:

```
Router> show dlsw peers | include FST.*DISCONN
FST 176.74.146.194  DISCONN          1         0  prom      0    -   -        -
FST 9.180.128.186   DISCONN          1         0  prom      0    -   -        -
FST 139.71.105.39   DISCONN          1         0  prom      0    -   -        -
FST 138.150.39.18   DISCONN          1         0  prom      0    -   -        -
FST 253.240.220.167 DISCONN          1         0  prom      0    -   -        -
FST 252.186.119.224 DISCONN          1         0  prom      0    -   -        -
FST 41.255.172.252  DISCONN          1         0  prom      0    -   -        -
! --- Output truncated
Router>
```

Suggested Fix

This vulnerability can be mitigated by using Control Plane Policing (CoPP) to only allow IP Protocol 91 packets sent by valid peers.

Mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.

Control Plane Policing

Control Plane Policing (CoPP) can be used to block untrusted IP Protocol 91 packets sent to the affected device. Cisco IOS Software Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting, and if configured, rate-limiting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations.
The following example, which uses 192.168.100.1 to represent a trusted host, can be adapted to your network.

```plaintext
!-- Deny FST traffic on IP protocol 91 from trusted
!-- hosts to all IP addresses configured on all interfaces of the affected device
!-- so that it will be allowed by the CoPP feature

access-list 111 deny 91 host 192.168.100.1 any

!-- Permit all other FST traffic on IP protocol 91
!-- sent to all IP addresses configured on all interfaces of the affected
!-- device so that it will be policed and dropped by the CoPP feature

access-list 111 permit 91 any any

!-- Permit (Police or Drop)/Deny (Allow) all other Layer3
!-- and Layer4 traffic in accordance with existing security
!-- policies and configurations for traffic that is authorized
!-- to be sent to infrastructure devices

!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature

class-map match-all drop-fst-91-class
  match access-group 111

!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.

policy-map input-CoPP-policy
  class drop-fst-91-class
    drop

!-- Apply the Policy-Map to the Control-Plane of the
!-- device

control-plane
  service-policy input input-CoPP-policy
```

In the above CoP example, the access control list entries (ACEs) that match the potential exploit packets with the permit action result in these packets being discarded by the policy map drop function, while packets that match the deny action (not shown) are not affected by the policy-map drop function. Note that in the 12.2S and 12.0S Cisco IOS trains the policy-map syntax is different, as shown in the following example:

```plaintext
policy-map input-CoPP-policy
  class drop-fst-91-class
    police 32000 1500 1500 conform-action drop exceed-action drop
```

Additional information on the CoPP feature is available at:

Control Plane Policing Implementation Best Practices
Cisco 10000 Series DoS Vulnerability - 113032

Description
The Cisco 10000 Series Router is affected by a denial of service (DoS) vulnerability where an attacker could cause a device reload by sending a series of ICMP packets.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (113032 of 1.1)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 113032: Verify Cisco 10000 Series DoS Vulnerability [IOS].

Description
Cisco 10000 Series Routers that are running an affected version of Cisco IOS are affected.
To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the `show version` command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to Cisco Internetwork Operating System Software or Cisco IOS Software. The image name displays in parentheses, followed by Version and the Cisco IOS Software release name. Other Cisco devices do not have the `show version` command or may provide different output.
The following example identifies a Cisco product that is running Cisco IOS Software Release 15.0(1)M1 with an installed image name of C3900-UNIVERSALK9-M:

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team

!--- output truncated
```


Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of this vulnerability could cause an affected device to reload. Repeated exploitation could result in a sustained DoS condition.
Suggested Fix
Traffic destined to the device or transit traffic could trigger the effects of this vulnerability. Subsequently, the only workaround available is to block ICMP packets destined to the affected device and all ICMP transit traffic.

IOS Software NAT H.323 Vulnerability - 112253

Description
The Cisco IOS Software network address translation (NAT) feature:
- H.323 protocol
Cisco has released free software updates that address these vulnerabilities.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (112253 of 1.1)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 112253: Verify IOS Software NAT H.323 Vulnerability [IOS].

Description
NAT of H.323 Packets DoS Vulnerability
Transit crafted H.323 packets on TCP port 1720 could cause a reload of the vulnerable device.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of these vulnerability can cause the device to reload or become unresponsive.

Suggested Fix
NAT for Crafted H.323 Packets DoS Vulnerability Mitigation
Mitigation for this vulnerability consists of disabling NAT for H.323 and H.225.0 using the **no ip nat service h225** global configuration command.
Multiple SSH Vulnerabilities - 8118

Description
Four different Cisco product lines are susceptible to multiple vulnerabilities discovered in the Secure Shell (SSH) protocol version 1.5. These issues have been addressed, and fixes have been integrated into the Cisco products that support this protocol.

By exploiting the weakness in the SSH protocol, it is possible to insert arbitrary commands into an established SSH session, collect information that may help in brute force key recovery, or brute force a session key.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (8118 of 1.6)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 8118: Verify Multiple SSH Vulnerabilities [IOS].

Description
An implementation of SSH in multiple Cisco products are vulnerable to three different vulnerabilities. These vulnerabilities are:

**CRC-32 integrity check vulnerability**—This vulnerability has been described in a CORE SDI S.A. paper entitled *An attack on CRC-32 integrity checks of encrypted channels using CBC and CFB modes*. In order for this attack to succeed, an attacker must possess one or two known ciphertext/plaintext pairs. This should not be difficult since every session starts with a greeting screen which is fixed and which can be determined. This also implies that an attacker must be somewhere along the session path in order to be able to sniff the session and collect corresponding ciphertext.

While fixing this vulnerability, we have not made the implementation mistake described by VU#945216 (see http://www.kb.cert.org/vuls/id/945216) which is being actively exploited.

**Traffic analysis**—This issue has been described in an analysis jointly made by Dug Song and Solar Designer. It can be found at http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt, and is entitled *Passive Analysis of SSH (Secure Shell) Traffic*. To exploit this vulnerability, an attacker must be able to capture packets. When sending a packet using the SSH protocol, it is padded to the next 8-byte boundary, but the exact length of the data (without the padding) is sent unencrypted. The timing between packets may yield additional information, such as the relative position of a letter on the keyboard, but that depends on overall jitter in the network and the typing habits of the person. For additional information, see http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt.

**Key recovery in SSH protocol 1.5**—This has been discovered by CORE SDI S.A. and the paper describing it can be viewed at http://www.securityfocus.com/archive/1/161150. The subject line is SSH protocol 1.5 session key recovery vulnerability. In order to exploit this vulnerability, an attacker must be able to sniff the SSH session and be able to establish a connection to the SSH server. In order to recover
the server key, an attacker must perform an additional $2^{20}+2^{19}=1572864$ connections. Since the key has a lifespan of about an hour, this means that an attacker must perform around 400 connections per second. For further details, see http://www.securityfocus.com/archive/1/161150.

Applicable Platforms
Cisco IOS Devices

Impact

**CRC-32 integrity check vulnerability**—By exploiting this protocol weakness, the attacker can insert arbitrary commands in the session after the session has been established.

**Traffic analysis**—This vulnerability exposes the exact lengths of the passwords used for login authentication. This is only applicable to an interactive session that is being established over the tunnel protected by SSH. This can significantly help an attacker in guessing the password using the brute force attack.

**Key recovery in SSH protocol 1.5**—This vulnerability may lead to the compromise of the session key. Once the session key is determined, the attacker can proceed to decrypt the stored session using any implementation of the crypto algorithm used. This will reveal all information in an unencrypted form.

Suggested Fix
There are no workarounds for these vulnerabilities.

**IOS Software Smart Install Vulnerability - 113030**

**Description**
A vulnerability exists in the Smart Install feature of Cisco Catalyst Switches running Cisco IOS Software that could allow an unauthenticated, remote attacker to perform remote code execution on the affected device.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices (113030 of 1.2)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT - 113030: Verify IOS Software Smart Install Vulnerability [IOS]

**Description**
Devices configured as a Smart Install client or director are affected by this vulnerability. To display Smart Install information, use the `show vstack config` privileged EXEC command on the Smart Install director or client. The outputs of the show commands are different when entered on the director or on the client. The following is the output of the `show vstack config` in a Cisco Catalyst Switch configured as a Smart Install client:
The following is the output of the `show vstack config` in a Cisco Catalyst Switch configured as a Smart Install director:

**Director# show vstack config**

Role: Director  
Vstack Director IP address: 10.1.1.163  
Vstack Mode: Basic  
Vstack default management vlan: 1  
Vstack management Vlans: none  
Vstack Config file: tftp://10.1.1.100/default-config.txt  
Vstack Image file: tftp://10.1.1.100/c3750e-universalk9-tar.122-  
Join Window Details:  
  Window: Open (default)  
  Operation Mode: auto (default)  
Vstack Backup Details:  
  Mode: On (default)  
  Repository: flash:/vstack (default)

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the `show version` command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the `show version` command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 15.0(1)M1 with an installed image name of C3900-UNIVERSALK9-M:

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team

--- output truncated
```

Additional information about Cisco IOS Software release naming conventions is available in the white paper Cisco IOS and NX-OS Software Reference Guide available at:  
http://www.cisco.com/web/about/security/intelligence/ios-ref.html

### Applicable Platforms
Cisco IOS Devices

### Impact
Successful exploitation could allow an unauthenticated, remote attacker to perform remote code execution on the affected device.

### Suggested Fix
There are no workarounds available to mitigate this vulnerability other than disabling the Smart Install feature. The Smart Install Feature is enabled by default in client switches. No configuration is needed in client switches.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.
SSH Parameters

Description
Policies to enforce SSH related parameters.

Applicable Platforms
Cisco IOS Devices With SSH Capability

References
Control Objectives for Information and Related Technology (DS5.8 of 4.0)
COBIT (Control Objectives for Information and Related Technology) is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT is a de-facto standard used by most of the auditors when auditing for IT section of Sarbanes-Oxley (SOX) Compliance.

National Security Agency (NSA) Cisco Router Configuration Guide (Section 5.3.1 Page 228 of 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Cisco SAFE Compliance
SAFE: A Security Blueprint for Enterprise Networks

National Security Agency (NSA) Cisco Switch Configuration Guide (Section 6.2.2, Page 18 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (for example, switches) which are part of their computer networks.

Information Technology – Code of practice for information security management.
Defence Information System Agency (Section NET0681, NET0682 of Dec 2, 2005)
DISA Checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

Center for Internet Security, Benchmark for Cisco IOS (Section 1.1.2.2, Page: 9 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

Rule 1

Rule
Check the state of SSH server [IOS].

Description
Check the state of SSH server on the device. SSH provides secure access to the device.

Applicable Platforms
Cisco IOS Devices With SSH Capability

Impact
Using unsecured access to the device like telnet is not suggested since the communication is not encrypted.

Suggested Fix
Enable SSH server on the device for secure access of the device using the commands:

crypto key generate

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>SSH server state</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: true</td>
</tr>
</tbody>
</table>

Rule 2

Rule
Check maximum number of SSH authentication retries [IOS].

Description
Maximum number of authentication retries for SSH before the session is reset.

Applicable Platforms
Cisco IOS Devices With SSH Capability
Impact
If not limited, an unauthorized user may keep retrying to gain access to the device by guessing different username/passwords.

Suggested Fix
Limit the number of retires before the session is reset using the command:

\textit{ip ssh authentication-retries}

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Max Authentication Retries  | The number of attempts after which the session is reset. | Required: true
|                             |                                    | Default: 3
|                             |                                    | Min Value: 0
|                             |                                    | Max Value: 5

Rule 3

Rule
Check maximum Time-out interval for SSH negotiations [IOS].

Description
The time interval that the router waits for the SSH client to respond. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.

Applicable Platforms
Cisco IOS Devices With SSH Capability

Impact
None.

Suggested Fix
Configure desired time-out value using the command:

\textit{ip ssh time-out}

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Max timeout in seconds      | The time interval (in seconds) that the router waits for the SSH client to respond. | Required: true
|                             |                                                                            | Default: 120
|                             |                                                                            | Min Value: 1
|                             |                                                                            | Max Value: 120
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

**IOS Software IPv6 over Multiprotocol Label Switching Vulnerability - 113058**

**Description**
Cisco IOS Software is affected by Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain.
- Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices (113058 of 1.2)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT - 113058: Verify IOS Software IPv6 over Multiprotocol Label Switching Vulnerability [IOS].

**Description**
Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
A crafted IPv6 packet may cause the device to crash when the packet is processed by Cisco IOS Software because the MPLS TTL has expired. The crafted packet used to exploit this vulnerability would be silently discarded in Cisco IOS Software if received on an interface where the packet did not have an MPLS label.

Cisco IOS Software or Cisco IOS XE Software devices (hereafter both referenced as Cisco IOS Software in this document) that are running vulnerable versions of Cisco IOS Software and configured for MPLS are affected by two vulnerabilities related to IPv6 traffic that traverses an MPLS domain. The two vulnerabilities are independent of each other.

**Note**
IPv6 does not need to be configured on the affected devices themselves. The vulnerabilities do require the MPLS label switched packets to have specific IPv6 payloads to be exploited.

To determine whether a device is configured for MPLS, log in to the device and issue the command-line interface (CLI) command `show mpls interface`. If the IP state is Yes, the device is vulnerable. The following example shows a device that has MPLS configured on interface Ethernet0/0:

```
Router#show mpls interface
Interface           IP     Tunnel  BGP  Static  Operational
Ethernet0/0  Yes (ldp)  No   No  No       Yes
Router#
```
The following two examples show responses from a device with MPLS forwarding disabled. The first example shows a return of no interfaces:

```
router#show mpls interface  
<table>
<thead>
<tr>
<th>Interface</th>
<th>IP</th>
<th>Tunnel</th>
<th>BGP Static</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>routers#</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

In the second example, the device provides a message indicating that MPLS forwarding is not configured:

```
router#show mpls interface  
no MPLS apps enabled or MPLS not enabled on any interfaces
router#
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the `show version` command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the `show version` command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 15.0(1)M1 with an installed image name of C3900-UNIVERSALK9-M:

```
Router> show version  
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1,  
RELEASE SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2009 by Cisco Systems, Inc.  
Compiled Wed 02-Dec-09 17:17 by prod_rel_team  
!--- output truncated
```

Additional information about Cisco IOS Software release naming conventions is available in the white paper Cisco IOS and NX-OS Software Reference Guide at: 

**Applicable Platforms**
Cisco IOS Devices

**Impact**
Successful exploitation of these vulnerabilities may cause the device to reload. Repeated exploitation could result in a sustained denial of service condition.

**Suggested Fix**
For both vulnerabilities the following workaround applies:

**Disabling MPLS TTL Propagation**
Disabling MPLS TTL propagation will prevent exploitation of these vulnerabilities. MPLS TTL propagation will have to be disabled on all PE routers in the MPLS domain. To disable MPLS TTL propagation, enter the global configuration command `no mpls ip propagate-ttl`. If only `no mpls ip propagate-ttl forward` is configured, the vulnerabilities could still be exploited from within the MPLS domain.

IOS Software ICMPv6 over Multiprotocol Label Switching Vulnerability - 113058

Description
Cisco IOS Software is affected by Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain.

- ICMPv6 Packet May Cause MPLS-Configured Device to Reload

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (113058 of 1.2)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 113058: Verify IOS Software ICMPv6 over Multiprotocol Label Switching Vulnerability [IOS].

Description
ICMPv6 Packet May Cause MPLS-Configured Device to Reload

A valid ICMPv6 packet may cause the device to crash when the packet is processed by Cisco IOS Software because the MPLS TTL has expired. The packet used to exploit this vulnerability would not affect Cisco IOS Software if received on an interface where the packet did not have an MPLS label.

Cisco IOS Software or Cisco IOS XE Software devices (hereafter both referenced as Cisco IOS Software in this document) that are running vulnerable versions of Cisco IOS Software and configured for MPLS are affected by two vulnerabilities related to IPv6 traffic that traverses an MPLS domain. The two vulnerabilities are independent of each other.

Note
IPv6 does not need to be configured on the affected devices themselves. The vulnerabilities do require the MPLS label switched packets to have specific IPv6 payloads to be exploited.

To determine whether a device is configured for MPLS, log in to the device and issue the command-line interface (CLI) command show mpls interface. If the IP state is Yes, the device is vulnerable. The following example shows a device that has MPLS configured on interface Ethernet0/0:

Router#show mpls interface
Interface IP Tunnel BGP Static Operational
Ethernet0/0 Yes (ldp) No No No Yes
Router#
The following two examples show responses from a device with MPLS forwarding disabled. The first example shows a return of no interfaces:

```
router#show mpls interface
  Interface              IP            Tunnel   BGP Static Operational
  routers#
```

In the second example, the device provides a message indicating that MPLS forwarding is not configured:

```
router#show mpls interface
  no MPLS apps enabled or MPLS not enabled on any interfaces
  router#
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the show version command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the show version command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 15.0(1)M1 with an installed image name of C3900-UNIVERSALK9-M:

```
Router> show version
  Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1,
  RELEASE SOFTWARE (fc1)
  Technical Support: http://www.cisco.com/techsupport
  Copyright (c) 1986-2009 by Cisco Systems, Inc.
  Compiled Wed 02-Dec-09 17:17 by prod_rel_team
  !--- output truncated
```

Additional information about Cisco IOS Software release naming conventions is available in the white paper Cisco IOS and NX-OS Software Reference Guide at:


**Applicable Platforms**

Cisco IOS Devices

**Impact**

Successful exploitation of these vulnerabilities may cause the device to reload. Repeated exploitation could result in a sustained denial of service condition.

**Suggested Fix**

**Disabling MPLS TTL Propagation**

Disabling MPLS TTL propagation will prevent exploitation of these vulnerabilities. MPLS TTL propagation will have to be disabled on all PE routers in the MPLS domain. To disable MPLS TTL propagation, enter the global configuration command `no mpls ip propagate-ttl`. If only `no mpls ip propagate-ttl forward` is configured, the vulnerabilities could still be exploited from within the MPLS domain.

For more information about the MPLS TTL propagation command, see the configuration guide at:

FTP

Description
Policies to enforce FTP related parameter values.

Applicable Platforms
Cisco IOS Devices

References
None

Rule 1

Rule
Check FTP username configured [IOS].

Description
Check FTP username configured.

Applicable Platforms
Cisco IOS Devices

Impact
None

Suggested Fix
Configure FTP username using the command:

```
ip ftp username
```

Rule 2

Rule
Check FTP password is configured [IOS].

Description
Check that FTP password is configured.

Applicable Platforms
Cisco IOS Devices

Impact
None

Suggested Fix
Configure FTP password using the command:

```
ip ftp password
```
Cisco ASA Internet Locator Service Inspection DoS vulnerability - 113097

Description
Cisco ASA 5500 Series Adaptive Security Appliances:
  • Internet Locator Service (ILS) Inspection Denial of Service vulnerability

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices (113097 of 1.1)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 113097: Verify ASA Internet Locator Service Inspection DoS vulnerability [ASA].

Description
ILS Inspection Denial of Service Vulnerability
The ILS inspection engine provides NAT support for Microsoft NetMeeting, SiteServer, and Active Directory products that use LDAP to exchange directory information with an ILS server.
A DoS vulnerability affects the ILS inspection feature of Cisco ASA 5500 Series Adaptive Security Appliances. During successful exploitation, an unauthenticated attacker could cause the affected device to reload and may result in a sustained DoS condition.

Applicable Platforms
Cisco ASA Devices

Impact
Successful exploitation of all the DoS vulnerabilities could cause an affected device to reload. Repeated exploitation could result in a sustained DoS condition.

Suggested Fix
ILS Inspection DoS Vulnerability
Administrators can mitigate this vulnerability by disabling ILS inspection if it is not required. Administrators can disable ILS inspection by issuing the no inspect ils command in class configuration sub-mode in the policy map configuration. Disabling ILS inspection may cause ILS traffic to stop through the security appliance.
**IP Phone + Host Ports**

**Description**
Policy to enforce parameters for ports connected to IP Phone AND hosts.

**Applicable Platforms**
Cisco IOS Switches

**References**
National Security Agency (NSA) Cisco Switch Configuration Guide (Section 7.2 Page26 of Version 1.0)

The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (for example, switches) which are part of their computer networks.

**Rule 1**

**Rule**
Check configuration on IP Phone ports that are connected to Host as well [IOS].

**Description**
This check makes sure configuration on IP Phone ports is according to the policy.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
None

**Suggested Fix**
Make sure all the IP Phone ports are configured as switch ports in access mode using the command:

```
interface <interface name>
switchport
switchport mode access
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Phone Ports</td>
<td>Group of ports to make sure unused port configuration is enforced. Example valid values: 'Any', 'AnyEthernet', 'FastEthernet', 'GigabitEthernet', 'FastEthernet0/1', 'FastEthernet0/.*', and so on.</td>
<td>Required: true Default: [Voice and Hosts]</td>
</tr>
</tbody>
</table>

Using IP Phone Ports Editor option, you can add, or remove IP Phone Ports details. You can also change the order of the port details.
Rule 2

Rule
Check all IP Phone ports are assigned to voice VLAN [IOS].

Description
This check makes sure all IP Phone ports are assigned to a voice VLAN.

Applicable Platforms
Cisco IOS Switches

Impact
None

Suggested Fix
Assign all IP Phone ports to a specific voice VLAN using the command:

```
interface <interface name>
switchport voice vlan <vlan number>
```

<table>
<thead>
<tr>
<th>Rule Description Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice VLAN</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Rule 3

Rule
Check the Access VLAN [IOS].

Description
This check makes sure all IP Phone + host ports are assigned to an access VLAN.

Applicable Platforms
Cisco IOS Switches

Impact
None

Suggested Fix
Assign all IP Phone + host ports to a specific access VLAN using the command:

```
interface <interface name>
switchport access vlan <vlan number>
```
Rule 4

Rule
Check all IP Phone ports block unknown multicast frames [IOS].

Description
This check will make sure all IP Phone ports are configured to block unknown multicast frames.

Applicable Platforms
Cisco IOS Switches

Impact
By default, a switch floods packets with unknown destination MAC addresses to all ports. If unknown unicast and multicast traffic is forwarded to a switch port, there might be security issues. To prevent forwarding such traffic, you can configure a port to block unknown unicast or multicast packets.

Suggested Fix
Configure IP Phone ports to block unknown multicast packets using the command:

```
interface <interface name>
switchport block multicast
```

Rule 5

Rule
Check all IP Phone ports block unknown unicast frames [IOS].

Description
This check will make sure all IP Phone ports are configured to block unknown unicast frames.

Applicable Platforms
Cisco IOS Switches

Impact
By default, a switch floods packets with unknown destination MAC addresses to all ports. If unknown unicast and multicast traffic is forwarded to a switch port, there might be security issues. To prevent forwarding such traffic, you can configure a port to block unknown unicast or multicast packets.
Suggested Fix
Configure IP Phone ports to block unknown unicast packets using the command:

\[
\text{interface <interface name>}
\]
\[
\text{switchport block unicast}
\]

Rule 6

Rule
Check all IP Phone ports are enabled with port security [IOS].

Description
This check will make sure all IP Phone ports are configured port security to block devices with unknown MAC addresses to be connected.

Applicable Platforms
Cisco IOS Switches

Impact
None

Suggested Fix
Configure IP Phone ports with port security using the command:

\[
\text{interface <interface name>}
\]
\[
\text{switchport port-security}
\]

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Maximum MAC addresses allowed | Maximum MAC addresses allowed to be connected to this port. Please note that each IP Phone may require 2 entries. | Required: false  
Default: 3  
Min Value: 1  
Max Value: 5120 |

Rule 7

Rule
Check all IP Phone ports are configured not to override COS of incoming packets [IOS].

Description
This check will make sure the IP Phone ports are configured not to override Class Of Service of packets with default cos.

Applicable Platforms
Cisco IOS Switches
Impact

All the incoming packets will be overwritten with a default class of service replacing the original class of service in the packet. This will cause the voice traffic to share the same queues as data coming from PC and hence may cause degradation in voice quality.

Suggested Fix

Configure IP Phone ports not to override cos using the command:

```
interface <interface name>
no mls qos cos override
```

Rule 8

Rule

Check all IP Phone ports are configured to trust priority fields [IOS].

Description

This check will make sure the IP Phone ports are configured to trust the priority fields of an incoming packet when classifying a packet for QoS purposes.

Applicable Platforms

Cisco IOS Switches

Impact

None

Suggested Fix

Configure IP Phone ports to trust DSCP bits/COS bits/IP Precedence bits using the command:

```
interface <interface name>
mls qos trust
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification Based On</td>
<td>Field in the packet to be used for classifying packets.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DSCP bits</td>
</tr>
</tbody>
</table>

Rule 9

Rule

Check all IP Phone ports have CDP enabled [IOS].

Description

In a typical network, you connect a Cisco IP Phone. Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the CoS 3-bit field, which determines the priority of the packet. For most Cisco IP Phone configurations, the traffic sent from the telephone to the switch is trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the mls qos trust cos interface
configuration command, you can configure the switch port to which the telephone is connected to trust the CoS labels of all traffic received on that port. However, if a user bypasses the telephone and connects the PC directly to the switch, the CoS labels generated by the PC are trusted by the switch (because of the trusted CoS setting) and can allow misuse of high-priority queues. The trusted boundary feature solves this problem by using the CDP to detect the presence of a Cisco IP Phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue.

Applicable Platforms
Cisco IOS Switches

Impact
It may not be possible to recognize a voice phone connected to the switch port and this may cause quality of service issues.

Suggested Fix
Configure IP Phone ports to use CDP using the command:

```
interface <interface name>
cdp enable
```

Rule 10

Rule
Check all IP Phone ports are configured to trust Cisco IP Phones [IOS].

Description
Switch port uses CDP to detect an IP Phone connected to it. So, it is required to CDP to be enabled on the switch port. In a typical network, you connect a Cisco IP Phone. Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the CoS 3-bit field, which determines the priority of the packet. For most Cisco IP Phone configurations, the traffic sent from the telephone to the switch is trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the mls qos trust cos interface configuration command, you can configure the switch port to which the telephone is connected to trust the CoS labels of all traffic received on that port. However, if a user bypasses the telephone and connects the PC directly to the switch, the CoS labels generated by the PC are trusted by the switch (because of the trusted CoS setting) and can allow misuse of high-priority queues. The trusted boundary feature solves this problem by using the CDP to detect the presence of a Cisco IP Phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue.

Applicable Platforms
Cisco IOS Switches

Impact
If a PC is connected directly to a Voice port, the switch will trust the priority coming from the PC, which may cause the LAN Quality of service to mis-behave.
Suggested Fix
Configure IP Phone ports to trust Cisco IP Phones using the command:

```
interface <interface name>
mis qos trust device cisco-phone
```

Rule 11

Rule
Check all IP Phone ports configured to set COS value for attached device [IOS].

Description
This check will make sure the IP Phone + Host ports are configured properly to instruct IP Phones to rewrite the PC traffic with a given COS.

Applicable Platforms
Cisco IOS Switches

Impact
Host may generate frames with higher cos value there by disrupting quality of service on the port.

Suggested Fix
Configure switch IP Phone + Host port to overwrite PC traffic using the command:

```
interface <interface name>
switchport priority extend cos
```
Applicable Platforms
Cisco IOS Switches

References
National Security Agency (NSA) Cisco Switch Configuration Guide (Section 7.2 Page 24 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (for example, switches) which are part of their computer networks.

Rule 1

Description
This check makes sure the state and configuration of port security is as per the required policy. Port security limits the number of valid MAC addresses allowed on a port. All switch ports or interfaces should be secured before the switch is deployed. In this way the security features are set or removed as required instead of adding and strengthening features randomly or as the result of a security incident. Please note that Since IP phones may use both untagged packets (e.g., Layer 2 CDP protocol) and Voice VLAN tagged packets, the IP phone's MAC address will be seen on both the native VLAN and the Voice VLAN. Therefore it will be counted twice. Set the maximum MAC count for a port connected to an IP phone to account for this plus the number of computers attached to the IP phone. Computers that legitimately transmit using multiple MAC address (for example, Network Load Balancing protocol) must also be taken into account.

Applicable Platforms
Cisco IOS Switches

Impact
A switch that does not provide port security allows an attacker to attach a system to an unused, enabled port and to perform information gathering or attacks. A switch can be configured to act like a hub, which means that every system connected to the switch can potentially view all network traffic passing through the switch to all systems connected to the switch. Thus, an attacker could collect traffic that contains usernames, passwords or configuration information about the systems on the network.

Suggested Fix
Configure Port security on given interfaces using the command:

```
interface <interface name>
   switchport port-security
   switchport port-security maximum
   switchport port-security violation
```

You can add, remove, or update the port security details. You can also change the order of the port security details.
Chapter 4 Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Note
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

ASA SCCP Inspection DoS Vulnerability - 112881

Description
Cisco ASA 5500 Series Adaptive Security Appliances are affected by the:

- Skinny Client Control Protocol (SCCP) Inspection Denial of Service Vulnerability

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices (112881 of 1.0)

Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 112881: Verify SCCP Inspection DoS Vulnerability [ASA].

Description
SCCP Inspection Denial of Service Vulnerability

A denial of service vulnerability affects the SCCP inspection feature of Cisco ASA 5500 Series Adaptive Security Appliances.

Administrators can determine if SCCP inspection is enabled by issuing the `show service-policy | include skinny` command and confirming that output, such as what is displayed in the following example, is returned.

```
ciscoasa# show service-policy | include skinny
Inspect: skinny, packet 0, drop 0, reset-drop 0
```

Alternatively, a device that has SCCP inspection enabled has a configuration similar to the following:

```
class-map inspection_default
  match default-inspection-traffic
 /

policy-map global_policy
  class inspection_default
    ...
    inspect skinny
    ...
 /
  service-policy global_policy global
```

Note
The service policy could also be applied to a specific interface instead of globally, which is displayed in the previous example.
SCCP inspection is enabled by default.

**Applicable Platforms**
Cisco ASA Devices

**Impact**
Successful exploitation of this vulnerability could cause a reload of the affected device. Repeated exploitation may result in a sustained denial of service condition.

**Suggested Fix**
Administrators can mitigate this vulnerability by disabling SCCP inspection if it is not required. Administrators can disable SCCP inspection by issuing the `no inspect skinny` command in class configuration submode in the policy map configuration.

---

**Password Rules**

**Description**
Default user name should not configured.

**Applicable Platforms**
Cisco Wireless LAN Controller (WLC) Devices

**References**
User Defined

**Rule 1**

**Rule**
Check default username should not be configured (WLC).

**Description**
Default user should not be configured.

**Applicable Platforms**
Cisco Wireless LAN Controller (WLC) Devices.

**Impact**
Default user name vulnerable.

**Suggested Fix**
Default user can delete using command:

```
mgmtuser delete admin
```

---

**ASA Unauthorized File System Access Vulnerability - 112881**

**Description**
Cisco ASA 5500 Series Adaptive Security Appliances are affected by the:
• Unauthorized File System Access Vulnerability

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices (112881 of 1.0)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 112881: Verify Unauthorized File System Access Vulnerability [ASA].

Description
An unauthorized file system access vulnerability affects Cisco ASA 5500 Series Adaptive Security Appliances when a security appliance is configured as a local Certificate Authority (CA). An affected configuration consists of the following minimum commands:

```
crypto ca trustpoint <trustpoint name>
keypair <keypair name>
crl configure
crypto ca server
crypto ca certificate chain <trustpoint name>
certificate ca 01
...
http server enable
```

The local CA server is not enabled by default.

Applicable Platforms
Cisco ASA Devices

Impact
Successful exploitation of this vulnerability could allow unauthorized, unauthenticated users to retrieve files that are stored in an affected appliance's file system, which may contain sensitive information.

Suggested Fix
There are no workarounds for this vulnerability.

IOS Software IPS and Zone Based Firewall Memory Leak Vulnerability - 113057

Description
Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features.

• Memory leak in Cisco IOS Software

Applicable Platforms
Cisco IOS Devices
References
CISCO PSIRT Advisories and Notices (113057 of 1.2)

Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 113057: Verify IOS Software IPS and Zone Based Firewall Memory Leak Vulnerability [IOS].

Description
Cisco IOS devices running vulnerable versions of Cisco IOS Software are affected by two vulnerabilities in Cisco IOS IPS and Cisco IOS Zone-Based Firewall. The two vulnerabilities are independent of each other. Details to confirm affected configurations are provided below.

• Memory leak in Cisco IOS Software

A device that is configured for either Cisco IOS IPS or Cisco IOS Zone-Based Firewall (or both), may experience a memory leak under high rates of new session creation flows through the device.

To determine if a device is configured with Cisco IOS IPS, log into the device and issue the `show ip ips interfaces` CLI command. If the output shows an IPS rule either in the inbound or outbound direction set, then the device is vulnerable. This example, shows a device with an IPS rule set on Interface Gigabit Ethernet 0/0 in the inbound direction:

```
Router#show ip ips interfaces
Interface Configuration
    Interface GigabitEthernet0/0
    Inbound IPS rule is example_ips_rule
    Outgoing IPS rule is not set
Router#
```

A device that is not configured for Cisco IOS IPS will return a blank line. The following example shows a device on which Cisco IOS IPS is not configured:

```
Router#show ip ips interfaces

Router#
```

To determine whether a device is configured with Zone-Based Firewall, log into the device and issue the `show zone security` CLI command. If the output shows a member interface under a zone name, then the device is vulnerable. This example, shows a device with Zone-Based Firewall rules configured on both GigabitEthernet0/0 and GigabitEthernet0/1

```
Router#show zone security
    zone self
        Description: System defined zone
    zone inside
        Description: *** Inside Network ***
        Member Interfaces:
            GigabitEthernet0/0
    zone outside
        Description: *** Outside Network ***
        Member Interfaces:
            GigabitEthernet0/1
Router#
```
Chapter 4  Using Compliance and Audit Manager Feature

Note
The device is vulnerable if configured with Zone-Based Firewall, regardless of the type of packet inspection being performed.

Applicable Platforms
Cisco IOS Devices

Impact
Memory leak in Cisco IOS Software The device may run out of memory resulting in instability or the device crashing.

Suggested Fix
There are no workarounds available.

ASA Transparent Firewall Packet Buffer Exhaustion Vulnerability - 112881

Description
Cisco ASA 5500 Series Adaptive Security Appliances are affected by the:
- Transparent Firewall Packet Buffer Exhaustion Vulnerability.

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices (112881 of 1.0)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 112881: Verify Cisco Transparent Firewall Packet Buffer Exhaustion Vulnerability [ASA].

Description
Transparent Firewall Packet Buffer Exhaustion Vulnerability
A packet buffer exhaustion vulnerability affects multiple versions of Cisco ASA Software when a security appliance is configured to operate in the transparent firewall mode. Transparent firewall mode is enabled on the appliance if the command firewall transparent is present in the configuration. The default firewall mode is routed, not transparent. The show firewall command can also be used to determine the firewall operation mode:

```
ciscoasa# show firewall
Firewall mode: Transparent
```

Applicable Platforms
Cisco ASA Devices
Impact
Successful exploitation of this vulnerability could cause a decrease in the number of available packet buffers. Repeated exploitation could eventually deplete all available packet buffers, which may cause an appliance to stop forwarding traffic.

Suggested Fix
There is no workaround for this vulnerability.

IP Phone Ports

Description
Policy to enforce parameters for ports connected to IP Phone.

Applicable Platforms
Cisco IOS Switches

References
National Security Agency (NSA) Cisco Switch Configuration Guide (Section 7.2 Page26 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (for example, switches) which are part of their computer networks.

Rule 1

Rule
Check configuration on IP Phone ports [IOS].

Description
This check makes sure configuration on IP Phone ports is according to the policy.

Applicable Platforms
Cisco IOS Switches

Impact
None

Suggested Fix
Make sure all the IP Phone ports are configured as switch ports in access mode using the command:

```
interface <interface name>
switchport
switchport mode access
```
Chapter 4      Using Compliance and Audit Manager Feature

Using IP Phone Ports Editor option, you can add, or remove IP Phone Ports details. You can also change the order of the port details.

Rule 2

Rule
Check all IP Phone ports are assigned to voice VLAN [IOS].

Description
This check makes sure all IP Phone ports are assigned to a voice VLAN.

Applicable Platforms
Cisco IOS Switches

Impact
None

Suggested Fix
Assign all IP Phone ports to a specific voice VLAN using the command:

```plaintext
interface <interface name>
switchport voice vlan <vlan number>
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Voice VLAN       | VLAN assigned to carry IP Phone traffic in the network.                     | Required: true
|                  |                                                                             | Min Value: 1
|                  |                                                                             | Max Value: 4094

Rule 3

Rule
Check all IP Phone ports block unknown multicast frames [IOS].

Description
This check will make sure all IP Phone ports are configured to block unknown multicast frames.

Applicable Platforms
Cisco IOS Switches
Impact
By default, a switch floods packets with unknown destination MAC addresses to all ports. If unknown unicast and multicast traffic is forwarded to a switch port, there might be security issues. To prevent forwarding such traffic, you can configure a port to block unknown unicast or multicast packets.

Suggested Fix
Configure IP Phone ports to block unknown multicast packets using the command:

interface <interface name>
switchport block multicast

Rule 4

Rule
Check all IP Phone ports block unknown unicast frames [IOS].

Description
This check will make sure all IP Phone ports are configured to block unknown unicast frames.

Applicable Platforms
Cisco IOS Switches

Impact
By default, a switch floods packets with unknown destination MAC addresses to all ports. If unknown unicast and multicast traffic is forwarded to a switch port, there might be security issues. To prevent forwarding such traffic, you can configure a port to block unknown unicast or multicast packets.
Suggested Fix
Configure IP Phone ports to block unknown unicast packets using the command:

interface <interface name>
switchport block unicast

Rule 5

Rule
Check all IP Phone ports are enabled with port security [IOS].

Description
This check will make sure all IP Phone ports are configured port security to block devices with unknown MAC addresses to be connected.

Applicable Platforms
Cisco IOS Switches

Impact
None

Suggested Fix
Configure IP Phone ports with port security using the command:

interface <interface name>
switchport port-security

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum MAC addresses allowed</td>
<td>Maximum MAC addresses allowed to be connected to this port. Please note that each IP Phone may require 2 entries.</td>
<td>Required: false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min Value: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max Value: 5120</td>
</tr>
</tbody>
</table>

Rule 6

Rule
Check all IP Phone ports are configured not to override COS of incoming packets [IOS].

Description
This check will make sure the IP Phone ports are configured not to override Class Of Service of packets with default cos.

Applicable Platforms
Cisco IOS Switches
Impact
All the incoming packets will be overwritten with a default class of service replacing the original class of service in the packet. This will cause the voice traffic to share the same queues as data coming from PC and hence may cause degradation in voice quality.

Suggested Fix
Configure IP Phone ports not to override cos using the command:

interface <interface name>
no mls qos cos override

Rule 7

Rule
Check all IP Phone ports are configured to trust priority fields [IOS].

Description
This check will make sure the IP Phone ports are configured to trust the priority fields of an incoming packet when classifying a packet for QoS purposes.

Applicable Platforms
Cisco IOS Switches

Impact
None

Suggested Fix
Configure IP Phone ports to trust DSCP bits/COS bits/IP Precedence bits using the command:

interface <interface name>
mls qos trust

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification Based On</td>
<td>Field in the packet to be used for classifying packets.</td>
<td>Required: true Default: DSCP bits</td>
</tr>
</tbody>
</table>

Rule 8

Rule
Check all IP Phone ports have CDP enabled [IOS].

Description
In a typical network, you connect a Cisco IP Phone. Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the CoS 3-bit field, which determines the priority of the packet. For most Cisco IP Phone configurations, the traffic sent from the telephone to the switch is trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the mls qos trust cos interface
configuration command, you can configure the switch port to which the telephone is connected to trust the CoS labels of all traffic received on that port. However, if a user bypasses the telephone and connects the PC directly to the switch, the CoS labels generated by the PC are trusted by the switch (because of the trusted CoS setting) and can allow misuse of high-priority queues. The trusted boundary feature solves this problem by using the CDP to detect the presence of a Cisco IP Phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
It may not be possible to recognize a voice phone connected to the switch port and this may cause quality of service issues.

**Suggested Fix**
Configure IP Phone ports to use CDP using the command:

```
interface <interface name>
cdp enable
```

**Rule 9**

**Rule**
Check all IP Phone ports are configured to trust Cisco IP Phones [IOS].

**Description**
Switch port uses CDP to detect an IP Phone connected to it. So, it is required to CDP to be enabled on the switch port. In a typical network, you connect a Cisco IP Phone. Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the CoS 3-bit field, which determines the priority of the packet. For most Cisco IP Phone configurations, the traffic sent from the telephone to the switch is trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the mls qos trust cos interface configuration command, you can configure the switch port to which the telephone is connected to trust the CoS labels of all traffic received on that port. However, if a user bypasses the telephone and connects the PC directly to the switch, the CoS labels generated by the PC are trusted by the switch (because of the trusted CoS setting) and can allow misuse of high-priority queues. The trusted boundary feature solves this problem by using the CDP to detect the presence of a Cisco IP Phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
If a PC is connected directly to a Voice port, the switch will trust the priority coming from the PC, which may cause the LAN Quality of service to mis-behave.
Suggested Fix

Configure IP Phone ports to trust Cisco IP Phones using the command:

```
interface <interface name>
mls qos trust device cisco-phone
```

Note

If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

ASA Routing Information Protocol DoS Vulnerability - 112881

Description

Cisco ASA 5500 Series Adaptive Security Appliances are affected by the:

- Routing Information Protocol (RIP) Denial of Service Vulnerability

Applicable Platforms

Cisco ASA Devices

References

CISCO PSIRT Advisories and Notices (112881 of 1.0)

Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule

PSIRT - 112881: Verify Routing Information Protocol DoS Vulnerability [ASA].

Description

RIP Denial of Service Vulnerability

A denial of service vulnerability affects the RIP implementation in Cisco ASA 5500 Series Adaptive Security Appliances when both RIP and the Cisco Phone Proxy feature are enabled on the same device. The following example displays an affected configuration (Cisco ASA Software version 8.0 and 8.1):

```
router rip
...
!
phone-proxy <instance name>
media-termination address <IP address>
...
<Rest of phone proxy feature configuration>
```
Or (Cisco ASA Software version 8.2 and later):

```
router rip

media-termination <instance name>
  address <IP address>

<Rest of phone proxy feature configuration>
```

A security appliance is vulnerable if it is processing RIP messages (`router rip`) and if a global media termination address is configured for the Cisco Phone Proxy feature (refer to previous example). Note that Cisco ASA Software versions 8.0 and 8.1 only allow a global media termination address. However, in Cisco ASA Software version 8.2 and later, it is possible to tie a media termination address to an interface. This configuration, which is accomplished by issuing the command `address <IP address> interface <interface name>` in media termination configuration mode, is not affected.

Neither RIP nor the Cisco Phone Proxy feature is enabled by default.

**Applicable Platforms**
Cisco ASA Devices

**Impact**
Successful exploitation of this vulnerability could cause a reload of the affected device. Repeated exploitation may result in a sustained denial of service condition.

**Suggested Fix**
There are no workarounds for Cisco ASA Software version 8.0 and 8.1. On Cisco ASA Software version 8.2 and later, administrators can configure a non-global media termination address by specifying a termination address that will be tied to a specific interface. For example:

```
router rip

media-termination <instance name>
  address <IP address> interface <interface name>

<Rest of phone proxy feature configuration>
```

**Outdated Devices As Per Vendor Specific EOL/EOS Announcements**

**Description**
This policy verifies if any of the devices selected are outdated as per the Cisco Hardware End Of Life/End Of Sales Announcements.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CatOS Devices
Rule 1

Rule
Verify that device is not announced to be End Of Life (IOS, PIX, ASA, CatOS).

Description
Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CatOS Devices

Impact
If the device is not upgraded to the next family of devices, the support of this device may end soon.

Suggested Fix
Upgrade to next available family of devices as soon as possible.

Rule 2

Rule
Verify that device has not reached to be End Of Sale (IOS, PIX, ASA, CatOS).

Description
This device has reached End of Sale milestone. The hardware may no longer be ordered. Devices which reach this milestone are still available for customers under maintenance contract or for Customer Service Engineering (CSE) support until they reach the "End-of-Life" milestone. Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CatOS Devices
**Rule 3**

**Rule**
Verify that device has not reached to be End Of Engineering Maintenance (IOS, PIX, ASA, CatOS).

**Description**
This device has reached End of Engineering milestone. After this milestone, no scheduled maintenance releases will be produced for the major release. Upgrades and releases for devices which reach this milestone are still available for customers under maintenance contract or for CSE support until they reach the "End-of-Life" milestone. Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to [Cisco End-Of-Life Policy](#) for more details.

**Applicable Platforms**
- Cisco IOS Devices
- Cisco PIX and ASA Firewalls
- Cisco CatOS Devices

**Impact**
If the device is not upgraded to the next family of devices, the support of this device may end soon.

**Suggested Fix**
Upgrade to next available family of devices as soon as possible.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Time | Time in years. | Required: true  
Default: Right Now |

**Rule 4**

**Rule**
Verify that device has not reached to be End Of Contract Renewal Maintenance (IOS, PIX, ASA, CatOS).

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Time | Time in years. | Required: true  
Default: Right Now |
Chapter 4 Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Description
This device has reached End of Contract Renewal milestone. After this milestone, service contracts are no longer renewed.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CatOS Devices

Impact
If the device is not upgraded to the next family of devices, the support of this device may end soon.

Suggested Fix
Upgrade to next available family of devices as soon as possible.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Time | Time in years. | Required: true
|      |             | Default: Right Now |

Rule 5

Rule
Verify that device has not reached to be End Of Life (Support) (IOS, PIX, ASA, CatOS).

Description
This device has reached End of Life milestone. After this milestone date, the device is no longer officially supported by the vendor. Products reach the end of their Product Life Cycle for a number of reasons. These reasons may be due to market demands, technology innovation and development driving changes in the product, or the products simply mature over time and are replaced by functionally richer technology. It is important to make sure all the devices are still supported by the vendor to make sure they be serviced and upgraded whenever needed. Refer to Cisco End-Of-Life Policy for more details.

Applicable Platforms
Cisco IOS Devices
Cisco PIX and ASA Firewalls
Cisco CatOS Devices

Impact
If the device is not upgraded to the next family of devices, the support of this device may end soon.

Suggested Fix
Upgrade to next available family of devices as soon as possible.
Cisco ASA TACACS+ Authentication Bypass vulnerability - 113097

Description
Cisco ASA 5500 Series Adaptive Security Appliances:
• TACACS+ Authentication Bypass vulnerability

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices (113097 of 1.1)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 113097: Verify ASA TACACS+ Authentication Bypass vulnerability [ASA].

Description
TACACS+ Authentication Bypass Vulnerability
An authentication bypass vulnerability affects the TACACS+ implementation of Cisco ASA 5500 Series Adaptive Security Appliances.
In order to enable TACACS+ for authentication, authorization, or accounting (AAA), you must first create at least one AAA server group per AAA protocol and add one or more servers to each group with the `aaa-server` command. You identify AAA server groups by name. The following example shows how a AAA server group is configured for TACACS+ authentication:

```
aaa-server my-tacacs-sever protocol tacacs+
aaa-server my-tacacs-server (inside) host 203.0.113.11
```

Applicable Platforms
Cisco ASA Devices

Impact
Successful exploitation of the TACACS+ authentication bypass vulnerability could allow an attacker to bypass authentication of VPN, firewall and/or administrative sessions.

Suggested Fix
TACACS+ Authentication Bypass Vulnerability
There are no workarounds available for this vulnerability other than using a different authentication protocol such as RADIUS, Active Directory, and so on.

**Content Services Gateway Service policy bypass - 112206**

**Description**
A service policy bypass vulnerability exists in the Cisco Content Services Gateway - Second Generation (CSG2), which runs on the Cisco Service and Application Module for IP (SAMI). Under certain configurations this vulnerability could allow:

- Customers to access sites that would normally match a billing policy to be accessed without being charged to the end customer
- Customers to access sites that would normally be denied based on configured restriction policies

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices (112206 of 1.0)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT - 112206: Verify Cisco Content Services Gateway Service policy bypass Vulnerability [IOS].

**Description**
The service policy bypass vulnerability affects all versions of the Cisco IOS Software for the CSG2 prior to the first fixed release, as indicated in the "Software Versions and Fixes" section of this advisory.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
Successful exploitation of the service policy bypass can allow customers to obtain access to sites that would normally be accounted and billed according to the billing policy without the billing policy being engaged. Additionally, customers could gain access to URLs that are configured in the Cisco CSG2 to be explicitly denied.

**Suggested Fix**
There is no workaround for this vulnerability.

**IOS Software NAT LDAP Vulnerability - 112253**

**Description**
The Cisco IOS Software network address translation (NAT) feature:
Understanding Compliance and Audit Manager (CAAM) Policies

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (112253 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 112253: Verify IOS Software NAT LDAP Vulnerability [IOS].

Description
NAT for NetMeeting Directory (LDAP) Vulnerability
LDAP is a protocol for querying and modifying data of directory services implemented in IP networks. NAT for NetMeeting Directory, also known as the Internet Locator Service (ILS), translates LDAP packets on TCP port 389. The inspected port is not configurable.
This vulnerability is triggered by malformed transit LDAP traffic that needs to be processed by the NAT for NetMeeting Directory feature.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of this vulnerability can cause the device to reload or become unresponsive.

Suggested Fix
NAT LDAP Vulnerability Mitigation
To disable NAT of LDAP, port-based address translation needs to be configured to disable LDAP inspection using the no-payload keyword. This will still allow the NAT of LDAP packets at Layer 3 (non-port specific). Translation of other non-LDAP protocols translation will not be affected. Applications that use embedded IP addresses in LDAP, such as NetMeeting Directory, will be negatively impacted if the embedded IP addresses need to be translated.
The following is an example configuration that includes the mitigation for two NAT rules.

```plaintext
!-- NAT rule for port TCP/389 to disable IP NAT for LDAP translation
!-- Takes precedence over the non-port translation rule.

ip nat outside source static tcp 192.168.0.1 389 192.168.1.1 389 no-payload
ip nat outside source static tcp 192.168.0.3 389 192.168.1.3 389 no-payload

!-- Translation rule for all other protocols

ip nat outside source static 192.168.0.1 192.168.1.1
ip nat outside source static 192.168.0.3 192.168.1.3

interface GigabitEthernet0/0
    ip nat inside
interface GigabitEthernet0/1
    ip nat outside
```

Each NAT translation rule in the configuration will need to be updated to include a per-port rule that disables translation of TCP packets on port 389.

**DHCP**

**Description**
Policies to enforce DHCP related parameter values.

**Applicable Platforms**
Cisco IOS Devices With DHCP_SERVER Capability

**References**
None

**Rule 1**

**Rule**
Check DHCP service on the device [IOS].

**Description**
Enable/disable DHCP service.

**Applicable Platforms**
Cisco IOS Devices With DHCP_SERVER Capability

**Impact**
None

**Suggested Fix**
Enable/Disable DHCP service using the command:

```
[no] service dhcp
```
Chapter 4 Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Rule 2

Rule
Check DHCP lease time should be at least [IOS].

Description
Make sure that DHCP lease time should be at least.

Applicable Platforms
Cisco IOS Devices With DHCP_SERVER Capability

Impact
None

Suggested Fix
Configure DHCP lease time using the command:

```
ip dhcp pool <pool-name>
lease <number>
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP lease time in days</td>
<td>The amount of time (in days) that the assigned ip address is valid.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 1 Min Value: 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max Value: 365</td>
</tr>
</tbody>
</table>

IOS Software IP Service Level Agreement Vulnerability - 113056

Description
The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (113056 of 1.2)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 113056: Verify IOS Software IP Service Level Agreement Vulnerability [IOS].

Description
Cisco devices that are running Cisco IOS Software are vulnerable when they are configured for IP SLA, either as responders or as originators of vulnerable IP SLA operations.

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the `show version` command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the `show version` command or may provide different output.

The following example shows output from a device that runs a Cisco IOS Software image:

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team

!--- output truncated
```

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability described in this document may result in the reload of a vulnerable device. Repeated exploitation could result in a DoS condition.

Suggested Fix
There are no workarounds for this vulnerability, but there are mitigations that can be deployed on a general IP SLA responder to reduce the exposure to this vulnerability.

General IP SLA Responder Mitigation
For devices that are configured as general responders, a mitigation is to restrict IP SLA control packets on UDP port 1967 that are addressed to the vulnerable device to permit only trusted probe originators to open UDP ports that could be exploited. This can be accomplished using techniques such as Infrastructure Access list or Control Plane Protection.

For devices configured as general responders, mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.

IP SLA Permanent Responder Mitigation
For the permanent responder, the mitigation is to filter UDP packets addressed to the configured UDP port of each permanent responder to permit packets from the IP addresses of trusted devices.
IP SLA Source Devices Mitigation
For IP SLA source devices, a mitigation is to allow only UDP packets from trusted devices (that is, devices that are the target of IP SLA operations).

DHCP Status

Description
DHCP server should be disabled.

Applicable Platforms
Cisco Wireless LAN Controller (WLC) Devices

References
User Defined

Rule 1

Rule
DHCP should be disabled (WLC).

Description
Disable DHCP service.

Applicable Platforms
Cisco Wireless LAN Controller (WLC) Device

Impact
None

Suggested Fix
Make sure that no dhcp scopes defined.
Cisco ASA Four SunRPC Inspection Denial of Service vulnerability - 113097

Description
Cisco ASA 5500 Series Adaptive Security Appliances:

- Four SunRPC Inspection Denial of Service vulnerability

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices (113097 of 1.1)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 113097: Verify ASA Four SunRPC Inspection Denial of Service Vulnerability [ASA].

Description
SunRPC Inspection Denial of Service Vulnerabilities

Four DoS vulnerabilities affect the SunRPC inspection feature of Cisco ASA 5500 Series Adaptive Security Appliances.

SunRPC inspection is enabled by default.

To check if SunRPC inspection is enabled, issue the `show service-policy | include sunrpc` command and confirm that output, such as what is displayed in the following example, is returned.

```
ciscoasa# show service-policy | include sunrpc
   Inspect: sunrpc, packet 0, drop 0, reset-drop 0
```

The following configuration commands are used to enable SunRPC inspection in the Cisco ASA.

```
class-map inspection_default
    match default-inspection-traffic

policy-map global_policy
    class inspection_default
        ... inspect sunrpc
        ...
    service-policy global_policy global
```

Applicable Platforms
Cisco ASA Devices

Impact
Successful exploitation of all the DoS vulnerabilities could cause an affected device to reload. Repeated exploitation could result in a sustained DoS condition.
Suggested Fix

SunRPC Inspection DoS Vulnerabilities

Administrators can mitigate this vulnerability by disabling SunRPC inspection if it is not required. Administrators can disable SunRPC inspection by issuing the `no inspect sunrpc` command in class configuration sub-mode in the policy map configuration. Disabling SunRPC inspection may cause SunRPC traffic to stop through the security appliance.

Content Services Gateway DOS Vulnerability - 112206

Description

Cisco IOS Software Release 12.4 (24)MD1 on the Cisco CSG2 contains two vulnerabilities that can be exploited by a remote, unauthenticated attacker to create a denial of service condition that prevents traffic from passing through the CSG2. These vulnerabilities require only a single content service to be active on the Cisco CSG2 and can be exploited via crafted TCP packets. A three-way handshake is not required to exploit either of these vulnerabilities.

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (112206 of 1.0)

Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule

PSIRT - 112206: Verify Cisco Content Services Gateway DOS Vulnerability [IOS].

Description

The Denial of service vulnerabilities only affect Cisco IOS Software Release 12.4 (24) MD1 on the Cisco CSG2. No other Cisco IOS Software releases are affected.

Applicable Platforms

Cisco IOS Devices

Impact

Successful exploitation of either denial of service vulnerability could result in the Cisco CSG2 reloading or potentially hanging.

Suggested Fix

There is no workaround for this vulnerability.
IOS Software IPS and Zone Based Firewall crafted HTTP packets Vulnerability - 113057

Description
Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features.
• Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (113057 of 1.2)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 113057: Verify IOS Software IPS and Zone Based Firewall crafted HTTP packets Vulnerability [IOS].

Description
• Cisco IOS Software Denial of Service when processing specially crafted HTTP packets.
A device is vulnerable if configured under the following circumstances:
• HTTP Layer 7 Application Control and Inspection and Cisco IOS IPS are enabled.
• HTTP Layer 7 Application Control and Inspection with match request arg regex parameter on the HTTP class map. This configuration is affected regardless if Cisco IOS IPS is enabled or not.
The device is not vulnerable under other configurations. A summary of different configurations and their affect by this vulnerability is provided below:

<table>
<thead>
<tr>
<th>Configuration on Device</th>
<th>Affected or not Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only Cisco IOS IPS enabled</td>
<td>Not Affected</td>
</tr>
<tr>
<td>HTTP Layer 4 Stateful Inspection with Cisco IOS IPS enabled</td>
<td>Not Affected</td>
</tr>
<tr>
<td>HTTP Layer 4 Stateful Inspection with Cisco IOS IPS disabled</td>
<td>Not Affected</td>
</tr>
<tr>
<td>HTTP Layer 7 Application Control and Inspection with Cisco IOS IPS enabled</td>
<td>Affected</td>
</tr>
<tr>
<td>HTTP Layer 7 Application Control and Inspection with match arg regex parameter. With or without Cisco IOS IPS enabled.</td>
<td>Affected</td>
</tr>
<tr>
<td>HTTP Layer 7 Application Control and Inspection without match arg regex parameter. With or without Cisco IOS IPS enabled.</td>
<td>Not Affected</td>
</tr>
</tbody>
</table>
The following example shows an affected device configured with HTTP Layer 7 Application Control and Inspection and Cisco IOS IPS enabled:

```plaintext
ip ips name myips
!
ip ips signature-category
category all
  retired true
category ios_ips basic
  retired false
!
class-map type inspect match-any layer4-classmap
  match protocol http
!
class-map type inspect http match-any layer7-classmap
  match request arg length gt 15
!
policy-map type inspect http layer7-policymap
  class type inspect http layer7-classmap
  reset
  log
policy-map type inspect layer4-policymap
  class type inspect layer4-classmap
  inspect
  service-policy http layer7-policymap
  class class-default
  drop
!
zone security inside
description ** Inside Network **
zone security outside
description ** Outside Network **
zone-pair security in2out source inside destination outside
description ** Zone Pair - inside to outside **
  service-policy type inspect layer4-policymap
!
interface GigabitEthernet0/0
  ip address 192.168.0.6 255.255.255.0
  ip ips myips in
  zone-member security inside
!
interface GigabitEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  zone-member security outside
!
```
The following example shows an affected device configured with HTTP Layer 7 Application Control and Inspection with the match request arg regex parameter on the HTTP class map:

```
! parameter-map type regex example
  pattern [^\x00-\x80]
!
class-map type inspect match-any layer4-classmap
  match protocol http
!
class-map type inspect http match-any layer7-classmap
  match request arg regex example
!
!
policy-map type inspect http layer7-policymap
  class type inspect http layer7-classmap
    reset
    log
policy-map type inspect layer4-policymap
  class type inspect layer4-classmap
    inspect
      service-policy http layer7-policymap
  class class-default
    drop
!
zone security inside
  description ** Inside Network **
zone security outside
  description ** Outside Network **
zone-pair security in2out source inside destination outside
  description ** Zone Pair - inside to outside **
  service-policy type inspect layer4-policymap
!
interface GigabitEthernet0/0
  ip address 192.168.0.6 255.255.255.0
  zone-member security inside
!
interface GigabitEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  zone-member security outside
!
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the `show version` command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the `show version` command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 15.0(1)M1 with an installed image name of C3900-UNIVERSALK9-M:

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
!--- output truncated
```

Additional information about Cisco IOS Software release naming conventions is available in the white paper Cisco IOS and NX-OS Software Reference Guide at:

Applicable Platforms
Cisco IOS Devices

Impact
If the device supports and is configured with `scheduler isr-watchdog` then the device will reset and reload if the vulnerability is exploited, rather than just hang. For more information on the `scheduler isr-watchdog` command consult the Cisco IOS Configuration Fundamentals Command Reference at the following link:

Suggested Fix
There are no workarounds available.

Secure Webmode Access

Description
HTTP Server allows web based remote administration of the router. It is useful primarily when intervening routers or firewalls prevent use of Telnet for that purpose. However, it is important to note that both Telnet and web-based remote administration reveal critical passwords in clear text. Further, web-based administration imposes the requirement that users log in at full (level 15) privilege. Therefore, web-based remote administration should be avoided, then it is preferable.

Applicable Platforms
Cisco Wireless LAN Controller (WLC) Devices

References
User Defined

Rule 1

Rule
Check secureweb mode should be disabled (WLC).

Description
HTTP Server allows web based remote administration of the device. It is useful primarily when intervening routers or firewalls prevent use of Telnet for that purpose. However, it is important to note that both Telnet and web-based remote administration reveal critical passwords in clear text. Further, web-based administration imposes the requirement that users log in at full (level 15) privilege. Therefore, web-based remote administration should be avoided, then it is preferable.

Applicable Platforms
Cisco Wireless LAN Controller (WLC) Devices

Impact
Can be exploited to access the device.
**Suggested Fix**
Secure webmode can be disabled using the command:

```
network secureweb disable
```

**Unused Ports**

**Description**
Policy to enforce parameters for unused ports configuration.

**Applicable Platforms**
Cisco IOS Switches

**References**
National Security Agency (NSA) Cisco Switch Configuration Guide (Section 7.2 Page26 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (for example, switches) which are part of their computer networks.

**Rule 1**

**Rule**
Check configuration on unused ports [IOS].

**Description**
This check makes sure configuration on unused ports is according to the policy.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
None

**Suggested Fix**
None

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unused Interfaces</td>
<td>Group of interfaces to make sure unused port configuration is enforced. Example Valid Values: 'Any', 'AnyEthernet', 'FastEthernet', 'GigabitEthernet', 'FastEthernet0/1', 'FastEthernet0/.*', and so on.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>
Using Unused Interfaces Editor option, you can add, or remove the unused interface details. You can also change the order of the interface details.

Rule 2

**Rule**
Check all unused ports are shutdown [IOS].

**Description**
This check makes sure all unused ports are in shutdown state.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
Any device connected to this unused port may have a complete access to the switch and can start receiving/transmitting packets from/to the switch.

**Suggested Fix**
Shutdown unused interfaces using the command:

```
interface <interface name>
shutdown
```

Rule 3

**Rule**
Check all unused ports are configured in access mode [IOS].

**Description**
This check makes sure all unused ports are in access mode.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
None

**Suggested Fix**
Configure unused ports in access mode using the command:

```
interface <interface name>
switchport mode access
```

Rule 4

**Rule**
Check all unused ports are assigned to unused VLAN [IOS].
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

**Rule 5**

**Rule**
Check all unused ports block unknown multicast frames [IOS].

**Description**
This check will make sure all unused ports are configured to block unknown multicast frames.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
By default, a switch floods packets with unknown destination MAC addresses to all ports. If unknown unicast and multicast traffic is forwarded to a switch port, there might be security issues. To prevent forwarding such traffic, you can configure a port to block unknown unicast or multicast packets.

**Suggested Fix**
Configure unused ports to block unknown multicast packets using the command:

```
interface <interface name >
switchport block multicast
```

**Rule 6**

**Rule**
Check all unused ports block unknown unicast frames [IOS].
**Description**
This check will make sure all unused ports are configured to block unknown unicast frames.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
By default, a switch floods packets with unknown destination MAC addresses to all ports. If unknown unicast and multicast traffic is forwarded to a switch port, there might be security issues. To prevent forwarding such traffic, you can configure a port to block unknown unicast or multicast packets.

**Suggested Fix**
Configure unused ports to block unknown unicast packets using the command:

```
interface <interface name >
switchport block unicast
```

**Rule 7**

**Rule**
Check all unused ports are enabled with port security [IOS].

**Description**
This check will make sure all unused ports are configured port security to block devices with unknown MAC addresses to be connected.

**Applicable Platforms**
Cisco IOS Switches

**Impact**
None

**Suggested Fix**
Configure unused ports with port security using the command:

```
interface <interface name >
switchport port-security
```

**Rule 8**

**Rule**
Check all unused ports force devices to be un-authorized [IOS].

**Description**
This check will make sure all unused ports are configured to force all connected devices as unauthorized.

**Applicable Platforms**
Cisco IOS Switches
Impact
Unauthorized clients may use network resources using unused ports.

Suggested Fix
Configured unused ports with IEEE 802.1x port-based authentication using the command:

```
interface <interface name >
dot1x port-control
```

Note
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

Cisco ASA MSN Instant Messenger Inspection DoS vulnerability - 113097

Description
Cisco ASA 5500 Series Adaptive Security Appliances:
- MSN Instant Messenger (IM) Inspection Denial of Service vulnerability.

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices (113097 of 1.1)
Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 113097: Verify ASA MSN IM Inspection DoS vulnerability [ASA].

Description
MSN IM Inspection Denial of Service Vulnerability
The MSN IM inspection feature of Cisco ASA 5500 Series Adaptive Security Appliances is affected by a DoS vulnerability.

MSN IM inspection is not enabled by default.
Understanding Compliance and Audit Manager (CAAM) Policies

Administrators can enable MSN IM inspection and specify actions when a message violates a parameter, create an IM inspection policy map. You can then apply the inspection policy map when you enable IM inspection, as shown in the following example:

```plaintext
class inspection_default
   inspect im MY-MSN-INSPECT

# DHCP Snooping

Description
DHCP snooping is a DHCP security feature that provides security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. An untrusted message is a message that is received from outside the network or firewall and that can cause traffic attacks within your network. DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

Applicable Platforms
Cisco IOS Devices With DHCP_SNOOPING Capability

References
National Security Agency (NSA) Cisco Switch Configuration Guide (Section 7.2 Page24 of Version 1.0)
The "Cisco IOS Switch Security Configuration Guide" from National Security Agency (NSA) provides technical recommendations intended to help network administrators improve the security of their networks. Using the information presented in this document, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic. Also, this guide can assist information security officers by describing the security issues related to critical systems (for example, switches) which are part of their computer networks.
Rule 1

Rule
Check state of DHCP Snooping [IOS].

Description
DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database (also referred to as a DHCP snooping binding table).

To use any DHCP snooping features, you must globally enable DHCP snooping on the switch. DHCP snooping is not active until DHCP snooping is enabled on a VLAN.

Applicable Platforms
Cisco IOS Devices With DHCP_SNOOPING Capability

Impact
DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You can use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

Suggested Fix
Configure DHCP snooping using the command:

\[no\] ip dhcp snooping

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Snooping State</td>
<td>The required state of DHCP Snooping on the switch.</td>
<td>Required: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>

Rule 2

Rule
Check that DHCP Snooping is enabled for the given Vlans [IOS].

Description
This check makes sure that the DHCP snooping is enabled for the given VLANs.

Applicable Platforms
Cisco IOS Devices With DHCP_SNOOPING Capability

Impact
None

Suggested Fix
Enable DHCP snooping for required VLANs using the command:

ip dhcp snooping vlan
### Chapter 4  Using Compliance and Audit Manager Feature

#### Understanding Compliance and Audit Manager (CAAM) Policies

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan List</td>
<td>List of VLANs to enable DHCP snooping.</td>
<td>Required: true</td>
</tr>
</tbody>
</table>

**Rule 3**

**Rule**

Check that DHCP Snooping is enabled to verify MAC addresses [IOS].

**Description**

This check makes sure that the DHCP snooping is enabled to verify MAC addresses.

**Applicable Platforms**

Cisco IOS Devices With DHCP_SNOOPING Capability

**Impact**

None

**Suggested Fix**

Configure DHCP snooping to verify MAC addresses using the command:

```
[no] ip dhcp snooping verify mac-address
```

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify MAC Addresses</td>
<td>Enable or disable MAC address verification.</td>
<td>Required: true Default: false</td>
</tr>
</tbody>
</table>

**IOS Software NAT SIP Vulnerability - 112253**

**Description**

The Cisco IOS Software network address translation (NAT) feature:

- Session Initiation Protocol (Multiple vulnerabilities)

**Applicable Platforms**

Cisco IOS Devices

**References**

CISCO PSIRT Advisories and Notices (112253 of 1.1)

Security Advisories for security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PSIRT - 112253: Verify IOS Software NAT SIP Vulnerability [IOS].
Description

NAT for SIP DoS Vulnerabilities
Four vulnerabilities in the NAT for SIP feature are described in this document:

NAT of SIP over TCP vulnerability
Crafted SIP packets on TCP port 5060 could cause unpredictable results, including the reload of the vulnerable device. Translation of SIP over TCP packets will be disabled by default with the fix for this vulnerability.

Provider edge Multiprotocol Label Switching (MPLS) NAT of SIP over UDP packets DoS vulnerability
A malformed SIP packet on UDP 5060 that transits an MPLS enabled vulnerable device that needs an MPLS tag to be imposed on the malformed packet might reload the device.

NAT of crafted SIP over UDP packets DoS vulnerabilities
There are two DoS vulnerabilities related to similar crafted packets on UDP port 5060 that require SIP translation: the first is a vulnerability that will cause the device to reload and the second will cause a memory leak that could lead to a DoS condition, including reload of the vulnerable device.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of these vulnerability can cause the device to reload or become unresponsive.

Suggested Fix

NAT for SIP over TCP DoS Vulnerability Mitigation
Mitigation for this vulnerability consists of disabling NAT for SIP over the TCP transport by using the no ip nat service sip tcp port 5060 global configuration command.

NAT of Crafted SIP over UDP Packets DoS Vulnerability Mitigation
Mitigation of these vulnerabilities consists of disabling NAT for SIP over the UDP transport by using the no ip nat service sip udp port 5060 global configuration command.

Hot Standby Router Protocol (HSRP)

Description
Policies related to Hot Standby Router Protocol (HSRP) protocol configuration.

Applicable Platforms
Cisco IOS Devices With HSRP Capability

References
None

Rule 1

Rule
Check that HSRP authentication is configured as non-default [IOS].
Understanding Compliance and Audit Manager (CAAM) Policies

Description
Check that HSRP authentication is configured to non-default key.

Applicable Platforms
Cisco IOS Devices With HSRP Capability

Impact
HSRP authentication uses default string which makes it possible for crafted packets to claim to be the primary device and thereby bringing down the HSRP.

Suggested Fix
Configure HSRP authentication using the command:

```
interface <interface name>
standby <groupId> authentication
```

Note
If you select a rule which checks for interface related configuration, compliance check will be done only for the interfaces which are administratively up and configured with an IP address.

AAA Command Authorization By-pass - 68840 [IOS]

Description
A vulnerability exists within Cisco Internetwork Operating System (IOS) Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (Tcl) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Devices not running AAA command authorization feature, or do not support Tcl functionality are not affected by this vulnerability.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(68840 of 2.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Rule 1

Rule
PSIRT-68840: Verify AAA Command Authorization By-pass Vulnerability [IOS]

Description
A vulnerability exists within Cisco Internetwork Operating System (IOS) Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (Tcl) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Devices not running AAA command authorization feature, or do not support Tcl functionality are not affected by this vulnerability.

Applicable Platforms
Cisco IOS Devices

Impact
Devices impacted by this vulnerability, will allow users to execute any IOS EXEC command at the users authenticated privilege level from within the Tcl shell mode.

A separate issue exists that exacerbates this vulnerability. An authenticated user may be placed into Tcl Shell mode automatically (without the evidence of the (tcl) within the router prompt), without any intermediate step of manually entering into Tcl Shell mode via the tclsh command, only if a previous user goes into Tcl Shell mode and terminates the session before leaving the Tcl Shell mode.

If a privileged user initiates a Tcl Shell and exits the Tcl Shell mode without issuing the Tcl Shell command tclquit then the Tcl Shell process will remain active and attached to the corresponding virtual type terminal VTY or teletypewriter (TTY - line). The next authenticated user that accesses the device over the same line will have access to the Tcl Shell process, and may bypass AAA command.

Suggested Fix
Adding IOS configuration command authorization checking with the global configuration command aaa authorization config-commands forces AAA command authorization to occur within Tcl Shell mode.

⚠️ Caution
By enabling IOS configuration command authorization all commands within EXEC configuration mode will be subject to command authorization checks.

ARP Table Overwrite - 13600 [IOS]

Description
It is possible to send an Address Resolution Protocol (ARP) packet on a local broadcast interface (for example, Ethernet, cable, Token Ring, FDDI) which could cause a router or switch running specific versions of Cisco IOS Software Release to stop sending and receiving ARP packets on the local router interface. This will in a short time cause the router and local hosts to be unable to send packets to each other. ARP packets received by the router for the router's own interface address but a different Media Access Control (MAC) address will overwrite the router's MAC address in the ARP table with the one from the received ARP packet. This was demonstrated to attendees of the Black Hat conference and
should be considered to be public knowledge. This attack is only successful against devices on the segment local to the attacker or attacking host. See "Cisco IOS ARP Table Overwrite Vulnerability." at Cisco Security Advisories website.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices (13600 of 1.3)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT-13626: Verify ARP Table Overwrite Vulnerability [IOS]

**Description**
ARP packets, both request and reply, received by the router for the router's own interface address or global Network Address Translation (NAT) entries, but with a different MAC address, will overwrite the router's MAC address in the router's ARP table with the one in the ARP request or reply. Cisco IOS router devices will defend the MAC address of an interface for several attempts, but in an attempt to prevent an ARP storm, the device will accept the incorrect information into the ARP table, which causes the interface to stop accepting new ARP entries, and entries will not be accepted or updated in the ARP table. This behavior has been repaired to properly defend the interface MAC address, with rate limiting the response to avoid an ARP storm on the local network. This attack can only be carried out from the local network. This defect also impacts HSRP virtual interfaces.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
This issue can cause a Cisco Router to be vulnerable to a Denial-of-Service attack, once the ARP table entries time out. This defect does not result in a failure of confidentiality of information stored on the unit, nor does this defect allow hostile code to be loaded onto a Cisco device. This defect may cause a Denial-of-Service on the management functions of a Cisco Layer 2 Switch, but does not affect traffic through the device.

**Suggested Fix**
The workaround for this vulnerability is to enter the router interface MAC address into the arp table with a configuration entry, sometimes known as "hard coding" the ARP table entry.

The syntax for this command for routers and switches running IOS is as follows:

`arp <ip-address> <hardware-address> <type>`

The caveat to this workaround is identified with defect CSCd04366, which will clear all manually entered MAC addresses from the ARP table, when they are the same as the interface MAC address, when the command "clear arp" is issued on the router. This workaround does not survive a reboot of the router, and must be re-written to the configuration after any reload or reboot.
ASA Crafted IKE Message DoS Vulnerability - 111877 [ASA]

Description
Cisco ASA 5500 Series Adaptive Security Appliances are affected with:

- Crafted Internet Key Exchange (IKE) Message Denial of Service Vulnerability

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices(111877 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-111877: Verify ASA Crafted IKE Message DoS Vulnerability [IOS]

Description
IPsec is an IP security feature that provides robust authentication and encryption of IP packets. IKE is a key management protocol standard that is used in conjunction with the IPsec standard. A DoS vulnerability exists in the IKE implementation of the Cisco ASA. During successful exploitation, an unauthenticated attacker may cause an affected device to reload.

Note
Only traffic that is destined to the appliance may trigger this vulnerability when the affected device is configured for IPsec remote access or site-to-site VPNs.

Applicable Platforms
Cisco ASA Devices

Impact
Successful exploitation of this vulnerability cause the affected device to reload. Repeated exploitation could result in a sustained DoS condition.

Suggested Fix
There are no workarounds for this vulnerability apart from disabling IKE on the affected device. The no crypto isakmp enable <interface-name> command can be used to disable IKE on a specific interface.

ASA Crafted IKE Message DoS Vulnerability - 111877

Description
Cisco ASA 5500 Series Adaptive Security Appliances are affected with:

Crafted Internet Key Exchange (IKE) Message Denial of Service Vulnerability
Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices(111877 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-111877: Verify Cisco ASA Crafted IKE Message DoS Vulnerability [ASA]

Description
IPsec is an IP security feature that provides robust authentication and encryption of IP packets. IKE is a key management protocol standard that is used in conjunction with the IPsec standard. A DoS vulnerability exists in the IKE implementation of the Cisco ASA. During successful exploitation, an unauthenticated attacker may cause an affected device to reload.

Note
Only traffic that is destined to the appliance may trigger this vulnerability when the affected device is configured for IPsec remote access or site-to-site VPNs.

Applicable Platforms
Cisco ASA Devices

Impact
Successful exploitation of this vulnerability cause the affected device to reload. Repeated exploitation could result in a sustained DoS condition.

Suggested Fix
There are no workarounds for this vulnerability apart from disabling IKE on the affected device. The no crypto isakmp enable <interface-name> command can be used to disable IKE on a specific interface.

ASA Crafted TCP Segment DoS Vulnerability - 111485 [ASA]

Description
Cisco ASA 5500 Series Adaptive Security Appliances are affected with:

• Crafted TCP Segment Denial of Service Vulnerability

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices(111485 of 1.1)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Rule 1

Rule
PSIRT-111485: Verify ASA Crafted TCP Segment DoS Vulnerability [IOS]

Description
Cisco ASA 5500 Series Adaptive Security Appliances are affected by a vulnerability that may cause an appliance to reload when all of the following conditions are met:
1. A malformed, transit TCP segment is received.
2. The TCP segment matches a static NAT translation that has the "nailed" option configured on it.
3. The TCP segment is also processed by the Cisco AIP-SSM, which is configured for inline mode of operation.
A TCP three-way handshake is not necessary to exploit this vulnerability.

Applicable Platforms
Cisco ASA Devices

Impact
Successful exploitation of this vulnerability may cause a reload of the affected appliance. Repeated exploitation could result in a sustained DoS condition.
Suggested Fix
Possible workarounds for this vulnerability are the following:

- Migrate from "nailed" static NAT entries to TCP-state bypass.
- Use the Cisco AIP-SSM in promiscuous mode. This mode can be configured by issuing the ips promiscuous command in "class" configuration mode.
- Disable IPS inspection for "nailed" static NAT entries.
- If possible, change "nailed" static NAT entries to standard static NAT entries.

ASA Crypto Accelerator Memory Leak Vulnerability - 108009 [ASA]

Description
Crypto Accelerator Memory Leak Vulnerability exists in the Cisco ASA 5500 Series Adaptive Security Appliances.
Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate some of these vulnerabilities are available.

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices(108009 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-108009: Verify ASA Crypto Accelerator Memory Leak Vulnerability [IOS]

Description
Crypto Accelerator Memory Leak Vulnerability
The Cisco ASA security appliances may experience a memory leak triggered by a series of packets. This memory leak occurs in the initialization code for the hardware crypto accelerator.

Note
Only packets destined to the device (not transiting the device) may trigger this vulnerability.

The following Cisco ASA features use the services the crypto accelerator provides, and therefore may be affected by this vulnerability:

- Clientless WebVPN, SSL VPN Client, and AnyConnect Connections
- ASDM (HTTPS) Management Sessions
- Cut-Through Proxy for Network Access
- TLS Proxy for Encrypted Voice Inspection
- IP Security (IPsec) Remote Access and Site-to-site VPNs
• Secure Shell (SSH) Access

Applicable Platforms
Cisco ASA Devices

Impact
Repeated exploitation could result in a sustained DoS condition.

Suggested Fix
There are no workarounds for this vulnerability.

ASA NTLMv1 Authentication Bypass Vulnerability - 111485 [ASA]

Description
Cisco ASA 5500 Series Adaptive Security Appliances are affected with:
• NT LAN Manager version 1 (NTLMv1) Authentication Bypass Vulnerability

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices (111485 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-111485: Verify ASA NTLMv1 Authentication Bypass Vulnerability [IOS]

Description
Cisco ASA 5500 Series Adaptive Security Appliances contain a vulnerability that could result in authentication bypass when the affected appliance is configured to authenticate users against Microsoft Windows servers using the NTLMv1 protocol.

Users can bypass authentication by providing an invalid, crafted username during an authentication request. Any services that use a AAA server group that is configured to use the NTLMv1 authentication protocol is affected. Affected services include:
• Telnet access to the security appliance
• SSH access to the security appliance
• HTTPS access to the security appliance (including Cisco ASDM access)
• Serial console access
• Privileged (enable) mode access
• Cut-through proxy for network access
• VPN access

Applicable Platforms
Cisco ASA Devices

**Impact**
Successful exploitation of this vulnerability could result in unauthorized access to the network or appliance.

**Suggested Fix**
If NTLMv1 authentication is required, there are no workarounds for this vulnerability. If NTLMv1 authentication can be substituted by other authentication protocols (LDAP, RADIUS, TACACS+, etc.), it is possible to mitigate the vulnerability.

### ASA SCCP Inspection DoS Vulnerability - 111485 [ASA]

**Description**
ASA 5500 Series Adaptive Security Appliances are affected with:
- Skinny Client Control Protocol (SCCP) Inspection Denial of Service Vulnerability

**Applicable Platforms**
Cisco ASA Devices

**References**
CISCO PSIRT Advisories and Notices(111485 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT-111485: Verify ASA SCCP Inspection DoS Vulnerability [IOS]

**Description**
> Cisco ASA 5500 Series Adaptive Security Appliances are affected by a vulnerability that may cause the appliance to reload during the processing of malformed skinny control message. Appliances are only vulnerable when SCCP inspection is enabled.

Only transit traffic can trigger this vulnerability; traffic that is destined to the appliance will not trigger the vulnerability.

**Applicable Platforms**
Cisco ASA Devices

**Impact**
Successful exploitation of this vulnerability may cause a reload of the affected appliance. Repeated exploitation could result in a sustained DoS condition.

**Suggested Fix**
This vulnerability can be mitigated by disabling SCCP inspection if it is not required. Administrators can disable SCCP inspection by issuing the no inspect skinny command in class configuration sub-mode within the policy-map configuration.
ASA SIP Inspection DoS Vulnerability - 111485 [ASA]

Description
Cisco ASA 5500 Series Adaptive Security Appliances are affected with:

• SIP Inspection Denial of Service Vulnerabilities

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices(111485 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-111485: Verify ASA SIP Inspection DoS Vulnerability [IOS]

Description
Cisco ASA 5500 Series Adaptive Security Appliances are affected by two denial of service vulnerabilities that may cause an appliance to reload during the processing of SIP messages. Appliances are only vulnerable when SIP inspection is enabled.

Only transit traffic can trigger these vulnerabilities; traffic that is destined to the appliance will not trigger the vulnerabilities.

Applicable Platforms
Cisco ASA Devices

Impact
Successful exploitation of this vulnerability may cause a reload of the affected appliance. Repeated exploitation could result in a sustained DoS condition.
Suggested Fix

SIP Inspection Denial of Service Vulnerabilities

These vulnerabilities can be mitigated by disabling SIP inspection if it is not required. Administrators can disable SIP inspection by issuing the no inspect sip command in class configuration sub-mode within policy-map configuration.

ASA SIP Inspection DoS Vulnerability - 111877 [ASA]

Description
Cisco ASA 5500 Series Adaptive Security Appliances are affected with:
- Session Initiation Protocol (SIP) Inspection Denial of Service Vulnerability

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices(111877 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-111877: Verify Cisco ASA SIP Inspection DoS Vulnerability [IOS]

Description
SIP, as defined by the Internet Engineering Task Force (IETF), enables call handling sessions, particularly two-party audio conferences, or "calls." SIP works with SDP for call signalling. SDP specifies the ports for the media stream. Using SIP, the Cisco ASA can support any SIP VoIP gateways and VoIP proxy servers. To support SIP calls through the Cisco ASA, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected, because while the signaling is sent over a well-known destination port (UDP/TCP 5060), the media streams are dynamically allocated. Also, SIP embeds IP addresses in the user-data portion of the IP packet. SIP inspection applies NAT for these embedded IP addresses.

A DoS vulnerability affects the SIP inspection feature of Cisco ASA 5500 Series Adaptive Security Appliances. SIP inspection is enabled by default. During successful exploitation, an unauthenticated attacker may cause the affected device to reload.

Applicable Platforms
Cisco ASA Devices

Impact
Successful exploitation of this vulnerability cause the affected device to reload. Repeated exploitation could result in a sustained DoS condition.
Suggested Fix
This vulnerability can be mitigated by disabling SIP inspection if it is not required. Administrators can disable SIP inspection by issuing the `no inspect sip` command in class configuration sub-mode within policy-map configuration.

ASA TCP Connection Exhaustion DoS Vulnerability - 111485  [ASA]

Description
ASA 5500 Series Adaptive Security Appliances are affected by the following vulnerabilities:

• TCP Connection Exhaustion Denial of Service Vulnerability

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices(111485 of 1.1)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-111485: Verify Cisco ASA TCP Connection Exhaustion DoS Vulnerability [IOS]

Description
The Cisco ASA 5500 Series Adaptive Security Appliance is a modular platform that provides security and VPN services. It offers firewall, intrusion prevention (IPS), anti-X, and VPN services.

Cisco ASA 5500 Series Adaptive Security Appliances are affected by the following vulnerabilities:

TCP Connection Exhaustion Denial of Service Vulnerability

Cisco ASA 5500 Series Adaptive Security Appliances may experience a TCP connection exhaustion condition (no new TCP connections are accepted) when specific TCP segments are received during the TCP connection termination phase.

This vulnerability is triggered only when specific TCP segments are sent to certain TCP-based services that terminate on the affected appliance. Although exploitation of this vulnerability requires a TCP three-way handshake, authentication is not required.

Applicable Platforms
Cisco ASA Devices

Impact
Successful exploitation of this vulnerability may lead to an exhaustion condition where the affected appliance cannot accept new TCP connections. A reload of the appliance is necessary to recover from the TCP connection exhaustion condition. If a TCP-based protocol is used for device management (like telnet, SSH, or HTTPS), a serial console connection may be needed to access to the appliance.

Suggested Fix
TCP Connection Exhaustion Denial of Service Vulnerability
It is possible to mitigate this vulnerability for TCP-based services that are offered to known clients. For example, it may be possible to restrict SSH, Cisco ASDM/HTTPS, and Telnet administrative access to known hosts or IP subnetworks. For other services like remote access SSL VPN, where clients connect from unknown hosts and networks, no mitigations exist.

ASA Three SunRPC Inspection DoS Vulnerability - 111877 [ASA]

**Description**
Cisco ASA 5500 Series Adaptive Security Appliances are affected with:
- Three SunRPC Inspection Denial of Service Vulnerabilities

**Applicable Platforms**
Cisco ASA Devices

**References**
CISCO PSIRT Advisories and Notices(111877 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT-111877: Verify Cisco ASA Three SunRPC Inspection DoS Vulnerability [IOS]

**Description**
The Sun RPC inspection engine enables or disables application inspection for the Sun RPC protocol. Sun RPC is used by Network File System (NFS) and Network Information Service (NIS). Sun RPC services can run on any port. When a client attempts to access a Sun RPC service on a server, it must learn the port that service is running on. The client does this by querying the port mapper process, usually rpcbind, on the well-known port of 111. Three DoS vulnerabilities affect the SunRPC inspection feature of Cisco ASA 5500 Series Adaptive Security Appliances, in which an unauthenticated attacker may cause the affected device to reload.

**Note**
Only transit traffic can trigger these vulnerabilities; traffic that is destined to the appliance will not trigger the vulnerabilities. These vulnerabilities can be triggered by using UDP packets, not TCP.

**Applicable Platforms**
Cisco ASA Devices

**Impact**
Successful exploitation of this may cause the affected device to reload. Repeated exploitation could result in a sustained DoS condition.

**Suggested Fix**
These vulnerabilities can be mitigated by disabling SunRPC inspection if it is not required. Administrators can disable SunRPC inspection by issuing the no inspect sunrpc command in class configuration sub-mode within policy-map configuration.
ASA Three TLS DoS Vulnerability - 111877 [ASA]

Description
Cisco ASA 5500 Series Adaptive Security Appliances are affected with:
• Three Transport Layer Security (TLS) Denial of Service Vulnerabilities

Applicable Platforms
Cisco ASA Devices

References
CISCO PSIRT Advisories and Notices(111877 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-111877: Verify Cisco ASA Three TLS DoS Vulnerability [IOS]

Description
TLS and its predecessor, SSL, are cryptographic protocols that provide security for communications over IP data networks such as the Internet.
Three vulnerabilities exist on the Cisco ASA security appliances that can be triggered by a series of crafted TLS packets. An unauthenticated attacker may cause the affected device to reload. A Cisco ASA device configured for SSL VPN, TLS Proxy for Encrypted Voice Inspection, or configured to accept ASDM management connections is vulnerable.

Applicable Platforms
Cisco ASA Devices

Impact
Successful exploitation of this may cause the affected device to reload. Repeated exploitation could result in a sustained DoS condition.

Suggested Fix
If SSL VPN (clientless or client-based) is not needed, it can be disabled by issuing the clear configure webvpn command.
Administrators should make sure that ASDM connections are only allowed from trusted hosts.
To identify the IP addresses from which the security appliance accepts HTTPS connections for ASDM, configure the http command for each trusted host address or subnet. The following example, shows how a trusted host with IP address 192.168.1.100 is added to the configuration:

```
hostname(config)# http 192.168.1.100 255.255.255.255
```

The TLS Proxy for Encrypted Voice Inspection feature is affected by these vulnerabilities. This feature can be disabled if it is not needed. Temporarily disabling the feature will mitigate these vulnerabilities.
The Cut-Through Proxy for Network Access feature, when configured for HTTPS, is affected by these vulnerabilities. The only workaround is to disable the feature if not needed. To disable HTTPS Cut-Through Proxy authentication use the `no aaa authentication listener https` command, as shown in the following example:

```
ASA(config)# no aaa authentication listener https inside port 443
```

ASA WebVPN DTLS DoS Vulnerability - 111485 [ASA]

**Description**
ASA 5500 Series Adaptive Security Appliances are affected with:

- WebVPN Datagram Transport Layer Security (DTLS) Denial of Service Vulnerability

**Applicable Platforms**
Cisco ASA Devices

**References**
CISCO PSIRT Advisories and Notices(111485 of 1.1)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT-111485: Verify Cisco ASA WebVPN DTLS DoS Vulnerability [IOS]

**Description**
Cisco ASA 5500 Series Adaptive Security Appliances are affected by a vulnerability that may cause the appliance to reload when a malformed DTLS message is sent to the DTLS port (by default UDP port 443). Appliances are only vulnerable when they are configured for WebVPN and DTLS transport.

This vulnerability is only triggered by traffic that is destined to the appliance; transit traffic will not trigger the vulnerability.

**Applicable Platforms**
Cisco ASA Devices

**Impact**
Successful exploitation of this vulnerability may cause a reload of the affected appliance. Repeated exploitation could result in a sustained DoS condition.

**Suggested Fix**
This vulnerability can be mitigated by disabling DTLS transport for WebVPN. Administrators can disable DTLS by issuing the `no svc dtls enable` command under the "webvpn" attributes section of the corresponding group policy.
Access Point Memory Exhaustion from ARP Attacks - 68715 [IOS]

Description
A vulnerability exists in Cisco Aironet Wireless Access Points (AP) running IOS which may allow a malicious user to send a crafted attack via IP address Resolution Protocol (ARP) to the Access point which will cause the device to stop passing traffic and/or drop user connections. Repeated exploitation of this vulnerability will create a sustained DoS (denial of service).
See "Access Point Memory Exhaustion from ARP Attacks" at Cisco Security Advisories website for more information.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(68715 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-68715: Verify Access Point Memory Exhaustion from ARP Attacks Vulnerability [IOS]

Description
The Address Resolution Protocol (ARP) is used to dynamically map physical hardware addresses to an IP address. Network devices and workstations maintain internal tables in which these mappings are stored for some period of time.
An attacker, who has successfully associated with a Cisco IOS Wireless Access Point, may be able to spoof ARP messages to the management interface on the Access Point. The attacker could add entries to the ARP table on the device until physical memory has been completely exhausted. This will leave the device in a state where it is unable to pass traffic until the device has been reloaded by cycling the power.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of this vulnerability may result in a denial of service (DoS) impacting the availability of the Wireless Access Point. Management and packet forwarding services will be unavailable.

Suggested Fix
After upgrading the Access Point (see Software Versions and Fixes), add the command L2-FILTER BLOCK-ARP to each radio interface. For example:

```
! interface Dot11Radio0 l2-filter block-arp !
```
Access Point Web-browser Interface - 70567 [IOS]

Description
The Cisco web-browser interface for Cisco access points contains a vulnerability that could, under certain circumstances, remove the default security configuration from the managed access point and allow administrative access without validation of administrative user credentials. Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of this vulnerability.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(70567 of 1.2)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-70567: Access Point Web-browser Interface Vulnerability [IOS]

Description
The web-browser interface contains management pages that are used to change the wireless device settings, upgrade firmware, and monitor and configure other wireless devices on the network. The web-browser interface is enabled by default, and is indicated by the configuration command `ip http server` or `ip http secure-server`.

An access point running a default configuration will use the default enable secret password for administrative access. This can be modified via the web-browser interface tab `Security > Admin Access` or via the CLI with the configuration command `enable secret [new_secret]`.

Local User List Only (Individual Passwords) allows administrators of the access points to define a local unique username/password database for their administrators, so that a common global password is not shared.

A vulnerability exists in the access point web-browser interface when `Security > Admin Access` is changed from `Default Authentication (Global Password)` to `Local User List Only (Individual Passwords)`. This results in the access point being re-configured with no security, either Global Password or Individual Passwords, enabled. This allows for open access to the access point via the web-browser interface or via the console port with no validation of user credentials.

Access points configured for `Local User List Only (Individual Passwords)` and running non-vulnerable versions of Cisco IOS which are subsequently upgraded to a vulnerable version of IOS are not affected by this vulnerability as long as the configuration is not altered after the upgrade.

Applicable Platforms
Cisco IOS Devices
Impact
Successful exploitation of this vulnerability will result in unauthorized administrative access to the access point via the web management interface or via the console port.

Suggested Fix
Either of the following workarounds and mitigations may be used to help mitigate the effects of this vulnerability:

- **Disable Web-Based Management**
  To prevent the use of the web-browser interface via:
  - Web-Based Management—Select the Disable Web-Based Management check box on the Services > HTTP-Web Server page and click Apply.
  - CLI—Log into the device and issue these configuration commands (save the configuration upon exiting):

```bash
ap(config)#no ip http server
ap(config)#no ip http secure-server
ap(config)#exit
```

- **Configure via CLI**
  Enabling **Local User List Only (Individual Passwords)** via the CLI rather than the web-browser interface will provide the access point with the desired protected configuration. Log into the device and issue these configuration commands (save the configuration upon exiting):

```bash
ap#configure terminal
!--- Setup the username password pair first.
ap(config)#username test privilege 15 password test!
!--- Enable AAA.
ap(config)#aaa new-model
!--- Enable aaa authentication to the local database.
ap(config)#aaa authentication login default local
!--- Enable aaa authorization to the local database.
ap(config)#aaa authorization exec default local
!--- Enable http authentication to AAA.
ap(config)#ip http authentication aaa
ap(config)#exit
```

- **Configure RADIUS/TACACS Server first**
  Via the web-browser interface enabling any RADIUS/TACACS+ server within **Security > Server Manager > Corporate Servers** and then performing the option of **Security > Admin Access** as **Local User List Only (Individual Passwords)** will provide a workaround to this vulnerability.
Auth Proxy Buffer Overflow - 66269 [IOS]

Description
The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition. Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected. Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected. Only devices running certain versions of Cisco IOS are affected. See "Cisco IOS Firewall Authentication Proxy for FTP and Telnet Sessions Buffer Overflow." at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(66269 of 1.3)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-66269: Verify Firewall Authentication Proxy for FTP and TELNET Sessions Buffer Overflow [IOS]

Description
The Cisco IOS Firewall Authentication Proxy feature allows network administrators to apply specific security policies on a per-user basis. With the Firewall Authentication Proxy for FTP and/or Telnet Sessions feature, users can log into the network services via FTP and/or Telnet, and their specific access profiles are automatically retrieved and applied from a Remote Authentication Dial In User Service (RADIUS), or Terminal Access Controller Access Control System Plus (TACACS+) authentication server.

Cisco IOS Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack when processing the user authentication credentials from an Authentication Proxy Telnet/FTP session. To exploit this vulnerability an attacker must first complete a TCP connection to the IOS device running affected software and receive an auth-proxy authentication prompt.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability on Cisco IOS may result in a reload of the device or execution of arbitrary code. Repeated exploitation could result in a sustained DoS attack or execution of arbitrary code on Cisco IOS devices.

Suggested Fix
In networks where Cisco IOS Firewall Authentication Proxy feature for Telnet/FTP sessions is not required but enabled, disabling the feature on an IOS device will eliminate exposure to this vulnerability.
Configure the device with Cisco IOS Firewall Authentication Proxy feature for HTTP and/or HTTPS sessions and allow the Telnet and FTP services within the per-user TACACS+/RADIUS profile. Disable Authentication proxy for Telnet/FTP sessions to eliminate exposure.

**Authentication Proxy Vulnerability - 110478 [IOS]**

**Description**
Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices(110478 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT-110478: Verify Authentication Proxy Vulnerability [IOS]

**Description**
Devices running affected versions of Cisco IOS Software and configured with Authentication Proxy for HTTP(S) or Web Authentication or the consent feature are vulnerable.

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log into the device and issue the `show version` command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the `show version` command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright © 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih
<output truncated>
```
Understanding Compliance and Audit Manager (CAAM) Policies

The following example shows a product that is running Cisco IOS Software release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```bash
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
```


To determine if your device is configured with either Authentication Proxy for HTTP(S), Web Authentication or the consent feature, log into the device and issue the `show running-config` command.

The following example identifies firewall authentication proxy services using the `ip auth-proxy` under the proxy rule name `example_auth_proxy_name`:

```bash
Router#show running-config
```

```bash
! Set up the aaa new model to use the authentication proxy.
!

aaa authorization auth-proxy default group
!

! Apply a name to the authentication proxy configuration rule.
!

ip auth-proxy name example_auth_proxy_name http
!

! Apply the authentication proxy rule at an interface.
!

interface e0
ip auth-proxy example_auth_proxy_name
!
```

<output truncated>
The following example identifies firewall authentication proxy services running for HTTP under the proxy rule name `example_auth_proxy_name`, using the `ip admission` commands. This is the same configuration as Web Authentication:

```
Router#show running-config
<output truncated>
!
! Set up the aaa new model to use the authentication proxy.
!

aaa authorization auth-proxy default group
!
! Apply a name to the authentication proxy configuration rule.
!

ip admission name example_auth_proxy_name proxy http inactivity-time 60
!
! Apply the authentication proxy rule at an interface.
!

interface FastEthernet0/1
  ip admission example_auth_proxy_name
!

<output truncated>
```

The following example identifies a device configured with the consent feature under the consent rule name `example_consent_rule`:

```
Router#show running-config
<output truncated>
!
! Apply a name to the consent configuration rule.
!

ip admission name example_consent_rule consent
!
! Apply the consent rule at an interface.
!

interface FastEthernet 0/0
```
Understanding Compliance and Audit Manager (CAAM) Policies

Chapter 4  Using Compliance and Audit Manager Feature

Chapter 4  Using Compliance and Audit Manager Feature

ip admission consent-rule_rule
!

<output truncated>

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability may result in an unauthenticated and unauthorized user bypassing the authentication proxy services offered in Cisco IOS Authentication Proxy for HTTP(S) and/or bypassing the consent accept webpage.

Suggested Fix
There are no workarounds for this vulnerability.

BGP Attribute Corruption - 10935  [IOS]

Description
A Border Gateway Protocol (BGP) UPDATE contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. An unrecognized transitive attribute can cause failures in Cisco IOS routers, ranging from a crash upon receipt of the unrecognized transitive attribute, to a later failure upon attempt to clear the unrecognized transitive attribute. Specific but common configurations are affected, and described below. The failure was discovered because of a malfunction in the BGP implementation of another vendor. There is no workaround. Affected customers are urged to upgrade to fixed code.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(10935 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-10935: Verify BGP Attribute Corruption Vulnerability [IOS]

Description
A Border Gateway Protocol (BGP) UPDATE contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. Each path attribute is a type, length, value (TLV) object. This failure occurs as a result of memory corruption and only in configurations using specific inbound route filtering. The failure was discovered because of a malfunction in the BGP implementation of another vendor.

Applicable Platforms
Cisco IOS Devices

Impact
The vulnerability can be exercised repeatedly, affecting core routers, creating widespread network outages. This vulnerability can only be exercised in configurations that include both BGP and inbound route filtering on affected software.

Suggested Fix
There are no known workarounds for this vulnerability. Please upgrade to fixed versions.

BGP Logging - 63845  [IOS]

Description
A Cisco device running IOS Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with either the command bgp log-neighbor-changes configured or the command snmp-server enable traps bgp are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

This issue is tracked by CERT/CC VU#689326.

See "Cisco IOS Misformed BGP Packet Causes Reload" at Cisco Security Advisories website for more information.

Applicable Platforms
Cisco IOS Devices
CISCO PSIRT Advisories and Notices(63845 of 1.5)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-63845: Verify Misformed BGP Packet Causes Reload Vulnerability [IOS]

Description
A Cisco device running IOS Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with either the command bgp log-neighbor-changes configured or the command snmp-server enable traps bgp are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

This issue is tracked by CERT/CC VU#689326.

See "Cisco IOS Misformed BGP Packet Causes Reload" at Cisco Security Advisories website for more information.

Applicable Platforms
Cisco IOS Devices
Impact
Successful exploitation of this vulnerability on an IOS device results in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

Suggested Fix
Under normal circumstances, due to inherent security factors in the TCP protocol, such as sequence number checks, it is difficult, but possible to forge an appropriate packet to exploit this problem. Configuring your Cisco IOS device for BGP MD5 authentication greatly increases the work necessary to forge a valid packet from a remote peer. This will not protect your peering session if a valid BGP peer generates an invalid packet.

BGP Long AS path Vulnerability - 110457 [IOS]

Description
Affect only devices running Cisco IOS Software with support for four-octet AS number space (here after referred to as 4-byte AS number) and BGP routing configured.

This vulnerability could cause an affected device to reload when processing a BGP update that contains autonomous system (AS) path segments made up of more than one thousand autonomous systems.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(110457 of 1.2)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-110457 : Verify BGP Long AS path Vulnerability [IOS]

Description
This vulnerability affects only devices running Cisco IOS and Cisco IOS XE Software (here after both referred to as simply Cisco IOS) with support for RFC4893 and that have been configured for BGP routing.

BGP is configured in Cisco IOS Software with the configuration command `router bgp [AS Number]`.

The device is vulnerable if it is running affected Cisco IOS version and has BGP configured, regardless of whether the device is configured with a 2 or 4 byte AS number under the `router bgp` configuration command.

A Cisco IOS software version that has support for RFC4893 will allow configuration of AS numbers using 4 Bytes. The following example identifies a Cisco device that has 4 byte AS number support:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp ?
<1-65535> Autonomous system number
```
<1.0-XX.YY> 4 Octets Autonomous system number

Or:

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp ?
  <1-4294967295> Autonomous system number
  <1.0-XX.YY> Autonomous system number

The following example identifies a Cisco device that has 2 byte AS number support:

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp ?
  <1-65535> Autonomous system number

A router that is running the BGP process will contain a line in the configuration that defines the autonomous system number (AS number), which can be seen by issuing the command line interface (CLI) command "show running-config".

The canonical textual representation of four byte AS Numbers is standardized by the IETF through RFC5396 (Textual Representation of Autonomous System (AS) Numbers). Two major ways for textual representation have been defined as ASDOT and ASPLAIN. Cisco IOS routers support both textual representations of AS numbers. For further information about textual representation of four byte AS numbers in Cisco IOS Software consult the document "Explaining 4-Byte Autonomous System (AS) ASPLAIN and ASDOT Notation for Cisco IOS" at the following link:

Cisco IOS Software with support for RFC4893 is affected by both vulnerabilities if BGP routing is configured using either ASPLAIN or ASDOT notation, regardless if the AS Number is a 2 byte or 4 byte number.

The following example identifies a Cisco device that is configured for BGP using ASPLAIN notation:
router bgp 65536

The following example identifies a Cisco device that is configured for BGP using ASDOT notation:
router bgp 1.0

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability described in this document may result in a reload of the device. The issue could result in repeated exploitation to cause an extended DoS condition.
Suggested Fix
For this vulnerability, there are no workarounds on the affected device. Neighbors could be configured to discard routes that have more than one thousand AS numbers in the AS-path segments. This configuration will help prevent the further propagation of BGP updates with the AS path segments made up of greater than one thousand AS numbers.

Note
Configuring "bgp maxas-limit [value]" on the affected device does not mitigate this vulnerability.

BGP Packet - 53021  [IOS]

Description
A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

(See "Cisco IOS Malformed BGP Packet Causes Reload" at Cisco Security Advisories website for more information.)

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (53021 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-53021: Verify Malformed BGP Packet Causes Reload Vulnerability [IOS]

Description
A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

(See "Cisco IOS Malformed BGP Packet Causes Reload" at Cisco Security Advisories website for more information.)

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of this vulnerability results in a reload of the device. Repeated exploitation could result in a sustained DoS attack.
Suggested Fix
Under normal circumstances, due to inherent security factors in the TCP protocol such as sequence number checks, it is difficult but possible to forge an appropriate packet to exploit this problem. Configuring your Cisco IOS device for BGP MD5 authentication is a valid workaround to protect the vulnerable device.

BGP Update Message Vulnerability - 110457 [IOS]

Description
Affect only devices running Cisco IOS Software with support for four-octet AS number space (hereafter referred to as 4-byte AS number) and BGP routing configured.
This vulnerability could cause an affected device to reload when the affected device processes a malformed BGP update that has been crafted to trigger the issue.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(110457 of 1.2)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-110457: Verify BGP Update Message Vulnerability [IOS]

Description
These vulnerabilities affect only devices running Cisco IOS and Cisco IOS XE Software (hereafter both referred to as simply Cisco IOS) with support for RFC4893 and that have been configured for BGP routing.
BGP is configured in Cisco IOS Software with the configuration command `router bgp [AS Number]`. The device is vulnerable if it is running affected Cisco IOS version and has BGP configured, regardless of whether the device is configured with a 2 or 4 byte AS number under the `router bgp` configuration command.
A Cisco IOS software version that has support for RFC4893 will allow configuration of AS numbers using 4 Bytes. The following example identifies a Cisco device that has 4 byte AS number support:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp ?
<1-65535>  Autonomous system number
<1.0-XX.YY>  4 Octets Autonomous system number
```

Or:
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#router bgp ?
<1-4294967295>  Autonomous system number
<1.0-XX.YY>     Autonomous system number

The following example identifies a Cisco device that has 2 byte AS number support:

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#router bgp ?
<1-65535>  Autonomous system number

A router that is running the BGP process will contain a line in the configuration that defines the autonomous system number (AS number), which can be seen by issuing the command line interface (CLI) command "show running-config".

The canonical textual representation of four byte AS Numbers is standardized by the IETF through RFC5396 (Textual Representation of Autonomous System (AS) Numbers). Two major ways for textual representation have been defined as ASDOT and ASPLAIN. Cisco IOS routers support both textual representations of AS numbers. For further information about textual representation of four byte AS numbers in Cisco IOS Software consult the document "Explaining 4-Byte Autonomous System (AS) ASPLAIN and ASDOT Notation for Cisco IOS" at the following link:

Cisco IOS Software with support for RFC4893 is affected by both vulnerabilities if BGP routing is configured using either ASPLAIN or ASDOT notation, regardless if the AS Number is a 2 byte or 4 byte number.

The following example identifies a Cisco device that is configured for BGP using ASPLAIN notation:
router bgp 65536

The following example identifies a Cisco device that is configured for BGP using ASDOT notation:
router bgp 1.0

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerabilities described in this document may result in a reload of the device. The issue could result in repeated exploitation to cause an extended DoS condition

Suggested Fix
For this vulnerability, configuring "bgp maxas-limit [value]" on the affected device does mitigate this vulnerability. Cisco is recommends using a conservative value of 100 to mitigate this vulnerability.

Consult the document "Protecting Border Gateway Protocol for the Enterprise" at the following link for additional best practices on protecting BGP infrastructures:
http://www.cisco.com/web/about/security/intelligence/protecting_bgp.html
CEF Data Leak - 20640 [IOS]

Description
Excluding Cisco 12000 Series Internet Routers, all Cisco devices running Cisco IOS software that have Cisco Express Forwarding (CEF) enabled can leak information from previous packets that have been handled by the device. This can happen if the packet length described in the IP header is bigger than the physical packet size. Packets like these will be expanded to fit the IP length and, during that expansion, an information leak may occur. Please note that an attacker can only collect parts of some packets but not the whole session. See "Data Leak with Cisco Express Forwarding Enabled." at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(20640 of 1.3)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-20640: Verify CEF Data Leak with CEF Vulnerability [IOS]

Description
When a router receives a packet where MAC level packet length is shorter than is indicated by the IP level, the router will "extend" the packet to the size indicated by the IP level. This extension will be done by padding the packet with arbitrary data. The issue here is that padding may contain data from a previous packet that has not been erased.

Although it is possible to trigger this vulnerability on command, it is not possible to predict what information would be collected this way. It is not possible for an attacker to selectively capture desired packets (for example, packets with username and password combination).

This vulnerability is specific to CEF. Fast switching is not affected by it.

Applicable Platforms
Cisco IOS Devices

Impact
By sending malformed packets, and capturing them after they have been processed by CEF, an attacker may find remnants of previous packets in them. The remnant data may contain whatever the previous packet has carried. That may be parts of a document, mail or any other content.

Suggested Fix
The workaround is to disable CEF on a router.
Call Processing Solutions - 63708  [IOS]

Description
Cisco Internetwork Operating System (IOS) Software release trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for the Cisco IOS Telephony Service (ITS), Cisco CallManager Express (CME) or Survivable Remote Site Telephony (SRST) may contain a vulnerability in processing certain malformed control protocol messages.

See "Vulnerability in Cisco IOS Embedded Call Processing Solutions" at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(63708 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-63708: Verify Vulnerabilities in Cisco IOS Embedded Call Processing Solutions Vulnerability [IOS]

Description
ITS, CME and SRST are features that allow a Cisco device running IOS to control IP Phones using the Skinny Call Control Protocol (SCCP). SCCP is the Cisco CallManager native signaling protocol. Certain malformed packets sent to the SCCP port on an IOS device configured for ITS, CME or SRST may cause the target device to reload.

More information about Cisco's IOS Telephony Service (ITS) and Cisco CallManager Express (CME) can be found here:

More information on Cisco's Survivable Remote Site Telephony (SRST) can be found here:

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability may result in a device reload. Repeated exploitation could result in a Denial of Service (DoS) attack.

Suggested Fix
Affected devices that must run ITS, CME or SRST are vulnerable, and there are not any specific configurations that can be used to protect them. Applying access lists on interfaces that should not accept ITS, CME or SRST traffic and putting firewalls in strategic locations may greatly reduce exposure until an upgrade can be performed.
The IP Telephony Security in Depth SAFE paper at the URL below discusses a variety of best practices that should keep your voice network isolated from the Internet. These best practices may help to reduce the risk of exposure, although attacks from within the local network should always be considered a potential risk.

**CatOS Catalyst 5000 Series 802.1x Vulnerability - 13617 [CatOS]**

**Description**
When an 802.1x frame is received by an affected Catalyst 5000 series switch on a STP blocked port it is forwarded in that VLAN instead of being dropped. This causes a performance impacting 802.1x frames network storm in that part of the network, which is made up of the affected Catalyst 5000 series switches. This network storm only subsides when the source of the 802.1x frames is removed or one of the workarounds in the workaround section is applied. This vulnerability can be exploited to produce a denial of service (DoS) attack.

**Applicable Platforms**
Cisco CATOS Devices

**References**
CISCO PSIRT Advisories and Notices (13617 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
CATOS PSIRT-13617: Verify Catalyst 5000 Series 802.1x Vulnerability [IOS]

**Description**
When an 802.1x (IEEE standard for port based network access control) frame is received by an affected Catalyst 5000 series switch on a STP (Spanning Tree Protocol) blocked port it is forwarded in that VLAN (Virtual Local Area Network) instead of being dropped. This causes a performance impacting 802.1x frames network storm in that part of the network, which is made up of the affected Catalyst 5000 series switches. This network storm only subsides when the source of the 802.1x frames is removed or one of the workarounds in the workaround section is applied.

**Applicable Platforms**
Cisco CATOS Devices

**Impact**
When an affected Catalyst 5000 series switch network receives an 802.1x frame it causes an 802.1x frames network storm. This network storm degrades the performance of the network. Slower ports on the affected Catalyst 5000 series switches may stop passing user data. The affected Catalyst 5000 series switches may not respond to any management inquiries via SNMP, Telnet or HTTP. However, management via the console port on the switches is still possible and can be used to apply the workarounds.
**Suggested Fix**

The following workarounds will prevent the 802.1x frames from causing an 802.1x frames network storm in an affected Catalyst 5000 series switch network.

These workarounds can also be applied to a network experiencing an 802.1x frames network storm.

1. Configure permanent MAC address entries for the entire reserved STP range 01-80-c2-00-00-02 to 01-80-c2-00-00-0f to be directed out an unused port for each VLAN on each affected switch in the network. The commands to configure are given below.

   ```
   set cam permanent 01-80-c2-00-00-02 <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-03 <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-04 <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-05 <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-06 <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-07 <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-08 <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-09 <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-0a <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-0b <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-0c <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-0d <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-0e <mod#>/<port#> <VLAN>
   set cam permanent 01-80-c2-00-00-0f <mod#>/<port#> <VLAN>
   ```

2. Break the STP loop by either
   - Disabling the redundant (STP blocked ports) or
   - Disconnecting the cable from these ports

   Remove all the sources of 802.1x frames before re-enabling the ports or reconnecting the cables.

3. Power down the Catalyst 5000 switch(es) that create the spanning-tree loop (any switch with STP blocked ports).

   Remove all the sources of 802.1x frames before powering up the switches.
**CatOS Denial-of-Service of TCP-based services - 43864 [CatOS]**

**Description**
After receiving eight TCP connection attempts using a non-standard TCP flags combination, a Catalyst switch will stop responding to further TCP connections to that particular service. In order to re-establish functionality of that service, the switch must be rebooted. There is no workaround. This vulnerability affects only CatOS. No other Cisco products are affected.

**Applicable Platforms**
Cisco CATOS Devices

**References**
CISCO PSIRT Advisories and Notices(43864 of 1.5)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
CATOS PSIRT-43864: Verify Denial-of-Service of TCP-based services Vulnerability [IOS]

**Description**
After receiving eight connection attempts on any TCP service, the switch will stop responding to any further connection attempts to that service. These attempts must use a non-standard combination of TCP flags. The switch will continue to pass other switched traffic normally and the console is also not affected. Only the service to which connections were made will become unresponsive. Standard TCP services include HTTP, Telnet, and SSH.

**Applicable Platforms**
Cisco CATOS Devices

**Impact**
By exploiting this vulnerability, an attacker can prevent further use of the specified TCP-based service. Depending on the configuration of the device, if SSH or Telnet are enabled and exploited, the availability of those services could be affected, possibly resulting in a loss of management capability using those same services. However, UDP-based services such as Simple Network Management Protocol (SNMP) would still be available and unaffected.

**Suggested Fix**
There is no workaround. In order to continue using an affected TCP service, the switch must be rebooted. It is possible to mitigate the exposure by configuring VLAN Access Control Lists (VACLs) on the switch (where they are supported) that will allow only legitimate hosts to connect to the desired services. This must be combined with Unicast Reverse Path Forwarding (uRPF), or some other anti-spoofing technique, on the network edge to protect against spoofed packets from the outside of the network.
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

CatOS DoS using Telnet, HTTP and SSH - 52781  [CatOS]

Description
Cisco CatOS is susceptible to a TCP-ACK Denial of Service (DoS) attack on the Telnet, HTTP and SSH service. If exploited, the vulnerability causes the Cisco CatOS running device to stop functioning and reload.

Applicable Platforms
Cisco CATOS Devices

References
CISCO PSIRT Advisories and Notices(52781 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
CATOS PSIRT-52781: Verify Telnet, HTTP, and SSH Vulnerability [IOS]

Description
Cisco CatOS is susceptible to a TCP-ACK Denial of Service (DoS) attack on the Telnet, HTTP and SSH service. If exploited, the vulnerability causes the Cisco CatOS running device to stop functioning and reload.

A TCP-ACK DoS attack is conducted by not sending the regular final ACK required for a 3-way TCP handshake to complete, and instead sending an invalid response to move the connection to an invalid TCP state. This attack can be initiated from a remote spoofed source.

This vulnerability is currently known to be exploitable only if you have the Telnet, HTTP or SSH service configured on a device which is running Cisco CatOS.

Applicable Platforms
Cisco CATOS Devices

Impact
When exploited, the vulnerability causes the Cisco CatOS running device to stop functioning and reload.

Suggested Fix
Implement the best practice of assigning all switch management interfaces to a dedicated VLAN and apply appropriate access controls on routers switching between the switch management interface VLAN and the rest of the network.

Apply ACLs on routers / switches / firewalls in front of the vulnerable switches such that traffic destined for the Telnet TCP port 23, HTTP TCP port 80 and SSH TCP port 22 on the vulnerable switches is only allowed from the network management workstations. Refer to http://www.cisco.com/warp/public/707/iacl.html for examples on how to apply access control lists (ACLs) on Cisco routers.

On the Catalyst 6000 series switches, if the VLAN Access Control List (VACL) feature is available in the code base, you can use VACLs to enable Telnet, HTTP and SSH access to the switch's management interface only from the network management workstations.
Please note, these workarounds will not prevent spoofed IP packets with the source IP address set to that of the network management station from reaching the switch's management interface. For more information on anti-spoofing refer to


#sec_ip

http://www.ietf.org/rfc/rfc2827.txt

The Unicast Reverse Path Forwarding (Unicast RPF) feature helps to mitigate problems that are caused by malformed or forged IP source addresses that are passing through a router.

IP Permit Lists will not provide any mitigation against this vulnerability.

The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code.

---

**CatOS Embedded HTTP Server Buffer Overflow - 27962 [CatOS]**

**Description**
Cisco Catalyst switches running specific versions of Cisco CatOS software are vulnerable to a buffer overflow in an embedded HTTP server. Only CatOS versions from 5.4 up to and including 7.3 which contain a "cv" in the image name are affected. If the HTTP server is enabled a buffer overflow can be remotely exploited which will cause the switch to fail and reload. The vulnerability can be exploited repeatedly and result in a denial of service.

Workarounds are available that limit the ability to exploit the vulnerability.

**Applicable Platforms**
Cisco CATOS Devices

**References**
CISCO PSIRT Advisories and Notices(27962 of 1.1)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

---

**Rule 1**

**Rule**
CATOS PSIRT-27962: Verify Embedded HTTP Server Buffer Overflow Vulnerability [IOS]

**Description**
If the HTTP server is enabled on a Cisco Catalyst switch running an affected CiscoView image, an overly long HTTP query can be received by the embedded HTTP server that will cause a buffer overflow and result in a software reset of the switch. Once the switch has recovered and has resumed normal processing it is vulnerable again. It remains vulnerable until the HTTP server is disabled, HTTP queries to the switch management port are blocked, or the switch's software has been upgraded to a fixed version.

The HTTP server is disabled by default. It is typically enabled to allow web based management of the switch using CiscoView. Only a small subset of CatOS images contain this embedded HTTP server.

**Applicable Platforms**
Cisco CATOS Devices
Impact
The exploitation of this issue can result in a software forced reset of this device. Repeated exploitation may lead to a denial of service until the workaround for this vulnerability has been implemented or a fixed version of software has been loaded onto the device.

Suggested Fix
The HTTP server can be disabled on the Cisco switch.
This example shows how to disable the HTTP server:

```
Console (enable) set ip http server disable
HTTP server disabled.
```

The default setting for the HTTP server is disabled.
You may also choose to block access to port 80 for your Cisco switch. This can be done with any device with traffic filtering capabilities.

CatOS Enable Password Bypass Vulnerability - 13619 [CatOS]

Description
Cisco Catalyst software permits unauthorized access to the enable mode in the 5.4(1) release. Once initial access is granted, access can be obtained for the higher level "enable" mode without a password. This problem is resolved in version 5.4(2). Customers with vulnerable releases are urged to upgrade as soon as possible.

Applicable Platforms
Cisco CATOS Devices
Rule 1

CATOS PSIRT-13619: Verify Enable Password Bypass Vulnerability [IOS]

Description
Cisco Catalyst software permits unauthorized access to the enable mode in the 5.4(1) release. Once initial access is granted, access can be obtained for the higher level "enable" mode without a password. This problem is resolved in version 5.4(2). Customers with vulnerable releases are urged to upgrade as soon as possible.

Anyone who can obtain ordinary console access to an affected switch can bypass password authentication to obtain "enable" mode access without knowledge of the "enable" password. This vulnerability can be exploited through the network using telnet or via the physical console.

This problem was introduced in software version 5.4(1), and is corrected in version 5.4(2). Due to this defect, software version 5.4(1) is deferred. Customers are urged to upgrade to version 5.4(2).

Applicable Platforms
Cisco CATOS Devices

Impact
This vulnerability permits unauthorized access to the configuration mode and unauthorized configuration changes on a Catalyst switch.

Suggested Fix
There are no known workarounds for this vulnerability. Strictly limiting telnet access to the device will prevent the initial connection required to exploit this vulnerability. Telnet access can be controlled with the following command set:

```
set ip permit <address> <mask> telnet
set ip permit enable
```

This command set will deny all traffic not specified in the permit statement.

CatOS Memory Leak Vulnerability - 13618 [CatOS]

Description
A series of failed telnet authentication attempts to the switch can cause the Catalyst Switch to fail to pass traffic or accept management connections until the system is rebooted or a power cycle is performed. All types of telnet authentication are affected, including Kerberized telnet, and AAA authentication.

This vulnerability has been assigned Cisco bug ID CSCds66191.

Applicable Platforms
Cisco CATOS Devices
References
CISCO PSIRT Advisories and Notices(13618 of 1.3)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
CATOS PSIRT-13618: Verify Memory Leak Vulnerability [IOS]

Description
The telnet process fails to release resources upon a failed authentication, or a successful login of extremely short duration such as a telnet from within an automated script. This memory leak eventually results in the failure of the switch to perform any other processes, such as forwarding traffic or management; a power cycle or reboot is required for recovery.

Applicable Platforms
Cisco CATOS Devices

Impact
This vulnerability enables a Denial of Service attack on the Catalyst switch.

Suggested Fix
There is no configuration workaround to eliminate the problem. However, if you are unable to upgrade to an unaffected version, you may use other devices to strictly control or prohibit telnet access to the switch, permitting only connections from your local network.

Access control lists on the switch can limit the remote exploitation of the vulnerability. To limit access to known hosts use the following commands:

set ip permit enable telnet
set ip permit <addr> [mask]

Remote management of the switch can also be disabled.

The above workarounds are provided as an option; however, the recommendation is to upgrade to fixed code as soon as possible.

CatOS Multiple SSH Vulnerabilities - 8118 [CatOS]

Description
Four different Cisco product lines are susceptible to multiple vulnerabilities discovered in the Secure Shell (SSH) protocol version 1.5. These issues have been addressed, and fixes have been integrated into the Cisco products that support this protocol.
By exploiting the weakness in the SSH protocol, it is possible to insert arbitrary commands into an established SSH session, collect information that may help in brute force key recovery, or brute force a session key.

**Applicable Platforms**
Cisco CATOS Devices

**References**
CISCO PSIRT Advisories and Notices (8118 of 1.6)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
CATOS PSIRT-8118: Verify Multiple SSH Vulnerability [IOS]

**Description**
An implementation of SSH in multiple Cisco products are vulnerable to three different vulnerabilities. These vulnerabilities are:

- **CRC-32 integrity check vulnerability** -- This vulnerability has been described in a CORE SDI S.A. paper entitled "An attack on CRC-32 integrity checks of encrypted channels using CBC and CFB modes".

  In order for this attack to succeed, an attacker must possess one or two known ciphertext/plaintext pairs. This should not be difficult since every session starts with a greeting screen which is fixed and which can be determined. This also implies that an attacker must be somewhere along the session path in order to be able to sniff the session and collect corresponding ciphertext.

  While fixing this vulnerability, we have not made the implementation mistake described by VU#945216 (see http://www.kb.cert.org/vuls/id/945216) which is being actively exploited.

- **Traffic analysis** -- This issue has been described in an analysis jointly made by Dug Song and Solar Designer. It can be found at:

  http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt, and is entitled "Passive Analysis of SSH (Secure Shell) Traffic". To exploit this vulnerability, an attacker must be able to capture packets. When sending a packet using the SSH protocol, it is padded to the next 8-byte boundary, but the exact length of the data (without the padding) is sent unencrypted. The timing between packets may yield additional information, such as the relative position of a letter on the keyboard, but that depends on overall jitter in the network and the typing habits of the person. For additional information, please see http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt.

- **Key recovery in SSH protocol 1.5** -- This has been discovered by CORE SDI S.A. and the paper describing it can be viewed at http://www.securityfocus.com/archive/1/161150. The subject line is "SSH protocol 1.5 session key recovery vulnerability". In order to exploit this vulnerability, an attacker must be able to sniff the SSH session and be able to establish a connection to the SSH server. In order to recover the server key, an attacker must perform an additional $2^{20}+2^{19}=1572864$ connections. Since the key has a lifespan of about an hour, this means that an attacker must perform around 400 connections per second. For further details, please see http://www.securityfocus.com/archive/1/161150.

**Applicable Platforms**
Cisco CATOS Devices
Impact

- **CRC-32 integrity check vulnerability** -- By exploiting this protocol weakness, the attacker can insert arbitrary commands in the session after the session has been established.

- **Traffic analysis** -- This vulnerability exposes the exact lengths of the passwords used for login authentication. This is only applicable to an interactive session that is being established over the tunnel protected by SSH. This can significantly help an attacker in guessing the password using the brute force attack.

- **Key recovery in SSH protocol 1.5** -- This vulnerability may lead to the compromise of the session key. Once the session key is determined, the attacker can proceed to decrypt the stored session using any implementation of the crypto algorithm used. This will reveal all information in an unencrypted form.

Suggested Fix

There are no workarounds for these vulnerabilities.

CatOS NAM (Network Analysis Module) Vulnerability - 81863 [CatOS]

**Description**
Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Internetwork Operating System (IOS) or Catalyst Operating System (CatOS).

Cisco has made free software available to address this vulnerability for affected customers.

**Applicable Platforms**
Cisco CATOS Devices

**References**
CISCO PSIRT Advisories and Notices(81863 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
CATOS PSIRT-81863: NAM Vulnerability [IOS]

**Description**
NAMs are deployed in Catalyst 6000, 6500 series and Cisco 7600 series to monitor and analyze network traffic by using Remote Monitoring (RMON), RMON2, and other MIBs.

NAMs communicate with the Catalyst system by using the Simple Network Management Protocol (SNMP). By spoofing the SNMP communication between the Catalyst system and the NAM an attacker may obtain complete control of the Catalyst system.

Devices running both Cisco IOS and Cisco CatOS are affected by this vulnerability. This vulnerability is introduced in CatOS at 7.6(15) and 8.5(1). Older CatOS images are not vulnerable.

**Applicable Platforms**
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Cisco CATOS Devices

Impact
By successfully exploiting this vulnerability, an attacker may gain complete control of the device.

Suggested Fix
No workarounds exist for this vulnerability.
This vulnerability requires an attacker to spoof SNMP packets from the IP address of the NAM. Filtering SNMP traffic to an affected device can be used as a mitigation. Filtering SNMP traffic needs to be done on systems that are deployed in front of an affected device, since it is ineffective to filter against such spoofed packets on the device itself.
Anti-spoofing measures and infrastructure access-lists can also be deployed at your network edge as a potential mitigation technique.
Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document.

CatOS OpenSSH Server Vulnerabilities - 45322 [CatOS]

Description
New vulnerabilities in the OpenSSH implementation for SSH servers have been announced.
An affected network device, running an SSH server based on the OpenSSH implementation, may be vulnerable to a Denial of Service (DoS) attack when an exploit script is repeatedly executed against the same device. There are workarounds available to mitigate the effects of these vulnerabilities.

Applicable Platforms
Cisco CATOS Devices
Chapter 4 Using Compliance and Audit Manager Feature

References
CISCO PSIRT Advisories and Notices (45322 of 1.6 INTERIM)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
CATOS PSIRT-45322: Verify OpenSSH Server Vulnerability [IOS]

Description
The buffer size or the number of channels in the fixed code is now correctly incremented only after a successful allocation where as initially they were being set before an allocation. Upon an allocation failure, which could be externally triggered, memory contents would be incorrectly erased by the cleanup process. This would result in a corruption of the memory which would eventually lead to a crash for the process using that memory.

If SSH is disabled the Catalyst switch will not be vulnerable to these vulnerabilities. CatOS K9 (crypto) release 6.1 was the first CatOS release which incorporated the SSH feature. To verify if SSH has been configured on the switch type show crypto key. If this shows you the RSA key then SSH has been configured and enabled on the switch. To remove the crypto key type clear crypto key RSA and this will disable the SSH server on the switch.

Applicable Platforms
Cisco CATOS Devices

Impact
An affected device, running an SSH server based on the OpenSSH implementation, may be vulnerable to a DoS attack when an exploit script is repeatedly executed against the same device.

Suggested Fix
The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code as soon as it is available.

- The following workarounds can be implemented for CatOS based switches.
  - Apply IP Permit List for SSH to enable access to the switch's management interface only from the network management workstations.
  - On the Catalyst 6000 series switches, if the VLAN Access Control List (ACL) (VACL) feature is available in the code base, you can use VACLs instead of the IP Permit List workaround above.
  - Implement the best practice to assign all of the management interfaces of all the switches in the network to a different VLAN, and apply appropriate ACLs on the router switching between the VLANs.
  - Apply ACLs on routers / switches / firewalls in front of the vulnerable switches such that traffic destined for the SSH TCP port 22 on the vulnerable switches is only allowed from the network management workstations.
• To turn off SSH access on the Cisco Network Analysis Modules (NAM), type the exsession off ssh command.
• Wherever possible, restrict access to the SSH server on the network device. Allow access to the network device only from trusted workstations by using ACLs / MAC filters that are available on the affected platforms.

**CatOS Password Bypass Vulnerability - 42340 [CatOS]**

**Description**
Cisco Catalyst software permits unauthorized access to the enable mode in the 7.5(1) release. Once initial access is granted, access can be obtained for the higher level "enable" mode without a password. This problem is resolved in version 7.6(1). Customers with vulnerable releases are urged to upgrade as soon as possible.

**Applicable Platforms**
Cisco CATOS Devices

**References**
CISCO PSIRT Advisories and Notices(42340 of 1.4)

**Rule 1**

**Rule**
CATOS PSIRT- 42340: Verify Cisco Catalyst Enable Password Bypass Vulnerability [IOS]

**Description**
Anyone who can obtain command line access to an affected switch can bypass password authentication to obtain "enable" mode access without knowledge of the "enable" password. If local user authentication is enabled, any username can be used to gain access to the switch without a valid password. This same local user could then enter enable without a valid password. Command line access is provided through the console, telnet access, or ssh access methods; http access mode is not affected. This problem was introduced with the local user authentication feature in software version 7.5(1), and is corrected in version 7.6(1).

**Applicable Platforms**
Cisco CATOS Devices

**Impact**
This vulnerability permits unauthorized access to the configuration mode and unauthorized configuration changes on a Catalyst switch.

**Suggested Fix**
Strictly limiting telnet and/or ssh access to the device will prevent the initial connection required to exploit this vulnerability. Telnet and/or ssh access can be controlled with the following command set:

```
set ip permit <address> <mask> telnet
set ip permit <address> <mask> ssh
set ip permit enable
```

This command set will deny all traffic not specified in the permit statements for each protocol. Additionally, out-of-band management solutions and isolated management VLAN configurations can help mitigate this vulnerability by limiting the initial access necessary for exploitation.

**CatOS SNMP Malformed Message Handling - 19296 [CatOS]**

**Description**

Multiple Cisco products contain vulnerabilities in the processing of Simple Network Management Protocol (SNMP) messages. These vulnerabilities can be repeatedly exploited to produce a denial of service. In most cases, workarounds are available that may mitigate the impact. Some of these vulnerabilities are identified by various groups as VU#617947, VU#107186, OUSPG #0100, CAN-2002-0012, and CAN-2002-0013.


**Applicable Platforms**

Cisco CATOS Devices

**References**

CISCO PSIRT Advisories and Notices(19296 of 2.6)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

CATOS PSIRT-19296: Verify Malformed SNMP Message-Handling Vulnerability [IOS]

**Description**

Multiple Cisco products contain vulnerabilities in the processing of Simple Network Management Protocol (SNMP) messages. These vulnerabilities can be repeatedly exploited to produce a denial of service.

SNMP defines a standard mechanism for remote management and monitoring of devices in an Internet Protocol (IP) network.

There are three general types of SNMP operations: "get" requests to request information, "set" requests which modify the configuration of the remote device, and "trap" messages which provide a monitoring function. SNMP requests and traps are transported over User Datagram Protocol (UDP) and are received at the assigned destination port numbers 161 and 162, respectively.
The largest group of vulnerabilities described in this advisory result from insufficient checking of SNMP messages as they are received and processed by an affected system. Malformed SNMP messages received by affected systems can cause various parsing and processing functions to fail, which may result in a system crash and reload (or reboot) in most circumstances. Some Cisco products may not reload but will become unresponsive instead. Some of the affected products are not directly vulnerable to malformed SNMP messages, but fail under extended testing or large volumes of SNMP messages due to memory leaks or other unrelated problems.

These vulnerabilities can be easily and repeatedly demonstrated with the use of the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for SNMPv1. The test suite is generally used to analyze a protocol and produce messages that probe various design limits within an implementation of a protocol. Test packets containing overly-long or malformed object identifiers and other combinations of exceptional values in various fields can be programmatically generated and then transmitted to a network device under test. The PROTOS test suite for SNMPv1, as distributed, contains approximately 53,000 individual test cases.

Although the test suite itself applies only to SNMPv1, similar vulnerabilities likely exist in SNMPv2c and SNMPv3. Cisco has attempted to resolve those additional potential vulnerabilities simultaneously.

Independent security advisories have implicated TCP or UDP port 1993 in this vulnerability. Port 1993 is assigned to Cisco for SNMP over TCP, but it appears only in Cisco IOS Software releases prior to 11.x. It is not currently supported nor employed in any current Cisco products.

### Applicable Platforms

Cisco CATOS Devices

### Impact

The vulnerabilities can be exploited to produce a Denial of Service (DoS) attack. When the vulnerabilities are exploited, they can cause an affected Cisco product to crash and reload.

SNMP messages are transported using User Datagram Protocol (UDP) and are subject to IP source address spoofing which could be used to circumvent the access control mechanisms.

If an attacker is able to guess or otherwise obtain a read-only community string for an affected device, then he or she could bypass SNMP access control relying on the community string.

### Suggested Fix

Apply IP Permit List for SNMP to enable access to the switch's management interface only from the network management workstations.

Please note that this will not prevent spoofed IP packets with the source IP address set to that of the network management station from reaching the switch's management interface.

### CatOS SNMP Multiple Community String Vulnerabilities - 13629  [CatOS]

#### Description

Multiple Cisco IOS Software and CatOS software releases contain several independent but related vulnerabilities involving the unexpected creation and exposure of SNMP community strings. These vulnerabilities can be exploited to permit the unauthorized viewing or modification of affected devices.

See "Cisco IOS Software Multiple SNMP Community String Vulnerabilities." at Cisco Security Advisories website.

### Applicable Platforms

Cisco CATOS Devices
Rule 1

CATOS PSIRT-13629: Verify Multiple SNMP Community String Vulnerability [IOS]

Description
Multiple Cisco IOS Software and CatOS software releases contain several independent but related vulnerabilities involving the unexpected creation and exposure of SNMP community strings. These vulnerabilities can be exploited to permit the unauthorized viewing or modification of affected devices.

See "Cisco IOS Software Multiple SNMP Community String Vulnerabilities." at Cisco Security Advisories website

Applicable Platforms
Cisco CATOS Devices

Impact
These vulnerabilities could be exploited separately or in combination to gain access to or modify the configuration and operation of any affected devices without authorization.

Suggested Fix
Disable SNMP access to the device.

CatOS SNMP Version 3 Authentication Vulnerability - 107408 [CatOS]

Description
Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default in Cisco products. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has also been assigned to these vulnerabilities.

Applicable Platforms
Cisco CATOS Devices

References
CISCO PSIRT Advisories and Notices(107408 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
CATOS PSIRT-107408: Verify SNMP Version 3 Authentication Vulnerability [IOS]

**Description**
SNMP defines a standard mechanism for remote management and monitoring of devices in an Internet Protocol (IP) network.

There are three general types of SNMP operations: "get" requests to request information, "set" requests that modify the configuration of a remote device, and "trap" messages that provide a monitoring function. SNMP requests and traps are transported over User Datagram Protocol (UDP) and are received at the assigned destination port numbers 161 and 162, respectively.

SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network. RFC2574 defines the use of HMAC-MD5-96 and HMAC-SHA-96 as the possible authentication protocols for SNMPv3.

Vulnerabilities have been identified in the authentication code of multiple SNMPv3 implementations. This advisory identifies two vulnerabilities that are almost identical. Both are specifically related to malformed SNMPv3 packets that manipulate the Hash Message Authentication Code (HMAC). The two vulnerabilities may impact both Secure Hashing Algorithm-1 (SHA-1) and Message-Digest Algorithm 5 (MD5). The vulnerabilities described in this document can be successfully exploited using spoofed SNMPv3 packets.

**Applicable Platforms**
Cisco CATOS Devices

**Impact**
Successful exploitation of these vulnerabilities could result in the disclosure of sensitive information on a device or allow an attacker to make configuration changes to a vulnerable device that is based on the SNMP configuration.

**Suggested Fix**
There are no workarounds for this vulnerability.

**CatOS SSH Can Cause a Crash - 24862 [CatOS]**

**Description**
While fixing vulnerabilities mentioned in the Cisco Security Advisory: Multiple SSH Vulnerabilities we inadvertently introduced an instability in some products. When an attacker tries to exploit the vulnerability VU#945216 (described in the CERT/CC Vulnerability Note at http://www.kb.cert.org/vuls/id/945216) the SSH module will consume too much of the processor's time, effectively causing a DoS. In some cases the device will reboot. In order to be exposed SSH must be enabled on the device.. See "Scanning for SSH Can Cause a Crash." at Cisco Security Advisories website.
Applicable Platforms
Cisco CATOS Devices

References
CISCO PSIRT Advisories and Notices (24862 of 1.0)
Security Advisories: For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices: For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
CATOS PSIRT-24862: Verify Scanning for SSH Can Cause a Crash Vulnerability [IOS]

Description
While fixing the vulnerabilities (Cisco Security Advisory: Multiple SSH Vulnerabilities) an instability is introduced in some products. When exposed to an overly large packet, the SSH process will consume a large portion of the processor's instruction cycles, effectively causing a DoS. The capability to create such a packet is available in publicly available exploit code. In some cases this availability attack may result in a reboot of the device. In order to be exposed SSH must be enabled on the device.

The vulnerability in question is named CRC-32. It is also marked as VU#945216 and described in the CERT/CC Vulnerability Note at http://www.kb.cert.org/vuls/id/945216.

Applicable Platforms
Cisco CATOS Devices

Impact
By repeatedly exploiting this vulnerability an attacker can cause a denial of service, though Cisco products remain unaffected to the exploits that are trying to exploit vulnerabilities.

Suggested Fix
It is possible to mitigate this vulnerability in two ways:

- Block all SSH connections on the border on your network, or
- On each individual device allow SSH connections only from the required IP addresses and block all others.

Blocking all SSH connections, and all other protocols that are not supposed to come from the outside, on the network edge should be an integral part of the network security best practice.

CatOS SSH Protocol Mismatch Vulnerability - 10932 [CatOS]

Description
Non-Secure Shell (SSH) connection attempts to an enabled SSH service on a Cisco Catalyst 6000, 5000, or 4000 switch might cause a "protocol mismatch" error, resulting in a supervisor engine failure. The supervisor engine failure causes the switch to fail to pass traffic and reboots the switch. This problem is resolved in release 6.1(1c). Due to a very limited number of customer downloads, Cisco has chosen to notify affected customers directly.

This vulnerability has been assigned Cisco bug ID CSCds85763.
Applicable Platforms
Cisco CATOS Devices

References
CISCO PSIRT Advisories and Notices(10932 of 1.2)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
CATOS PSIRT-10932: Verify SSH Protocol Mismatch Vulnerability [IOS]

Description
Non SSH protocol connection attempts to the SSH service cause a "protocol mismatch" error, which causes a switch to reload. SSH is not enabled by default, and must be configured by the administrator.

Applicable Platforms
Cisco CATOS Devices

Impact
This vulnerability enables a Denial of Service attack on the Catalyst switch.

Suggested Fix
The workaround for this vulnerability is to disable SSH service. For most customers using this image, SSH support is necessary, so the recommended action is to upgrade to a fixed version.

CatOS TCP Conn Reset - 50961 [CatOS]

Description
A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer), and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, the attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain a TCP stack are susceptible to this vulnerability.

Applicable Platforms
Cisco CATOS Devices

References
CISCO PSIRT Advisories and Notices(50961 of 2.7)
Understanding Compliance and Audit Manager (CAAM) Policies

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
CATOS PSIRT-50961: Verify TCP Connection Reset Vulnerability [IOS]

Description
TCP is the transport layer protocol designed to provide connection-oriented reliable delivery of a data stream. To accomplish this, TCP uses a mixture of flags to indicate state and sequence numbers to identify the order in which the packets are to be reassembled. TCP also provides a number, called an acknowledgement number, that is used to indicate the sequence number of the next packet expected. The packets are reassembled by the receiving TCP implementation only if their sequence numbers fall within a range of the acknowledgement number (called a "window"). The acknowledgement number is not used in a packet with the reset (RST) flag set because a reset does not expect a packet in return.

Applicable Platforms
Cisco CATOS Devices

Impact
The impact is different for each specific protocol. While, in the majority of cases, a TCP connection will be automatically re-established, in some specific protocols a second order of consequences may have a larger impact than tearing down the connection itself.

Suggested Fix
There are no workarounds available to mitigate the effects of this vulnerability. It is possible to mitigate the exposure on this vulnerability by applying anti-spoofing measures on the edge of the network.

CatOS TCP State Manipulation DoS Vulnerability - 109444 [CatOS]

Description
Multiple Cisco products are affected by denial of service (DoS) vulnerability that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

Applicable Platforms
Cisco CATOS Devices

References
CISCO PSIRT Advisories and Notices(109444 of 1.3)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Rule 1

Rule
CATOS PSIRT-109444: Verify TCP State Manipulation DoS Vulnerability [IOS]

Description
All Cisco CatOS Software versions are affected by these vulnerabilities. A device running Cisco CatOS Software that is under attack will have numerous hung TCP connections in the FIN_WAIT_1 state. The show netstat command can be used to display the hung TCP connections. The following is example output showing an attack in progress.

Console> (enable) show netstat

Active Internet connections (including servers)

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>(state)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>0</td>
<td>83</td>
<td>192.168.1.10.23</td>
<td>192.168.1.20.46056</td>
<td>FIN_WAIT_1</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>83</td>
<td>192.168.1.10.23</td>
<td>192.168.1.20.16305</td>
<td>FIN_WAIT_1</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>83</td>
<td>192.168.1.10.23</td>
<td>192.168.1.20.14628</td>
<td>FIN_WAIT_1</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>83</td>
<td>192.168.1.10.23</td>
<td>192.168.1.20.7275</td>
<td>FIN_WAIT_1</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>83</td>
<td>192.168.1.10.23</td>
<td>192.168.1.20.39559</td>
<td>FIN_WAIT_1</td>
</tr>
</tbody>
</table>

Applicable Platforms
Cisco CatOS Devices

Impact
Successful exploitation of the TCP state manipulation vulnerabilities may result in a DoS condition where new TCP connections are not accepted on an affected system. Repeated exploitation may result in a sustained DoS condition. A reboot may be required to recover affected systems.

Suggested Fix
Cisco CatOS software provides VLAN Access Control Lists (VACL) to mitigate against the TCP state manipulation vulnerabilities. For more information on configuring VACLs on CatOS 7.x software versions, please consult the following link:

For more information on configuring VACLs on CatOS 8.x software versions, please consult the following link:

CatOS Telnet Buffer Vulnerability - 20776 [CatOS]

Description
Some Cisco Catalyst switches, running certain CatOS based software releases, have a vulnerability wherein a buffer overflow in the Telnet option handling can cause the Telnet daemon to crash and result in a switch reload.
This vulnerability can be exploited to initiate a denial of service (DoS) attack. This vulnerability is documented as Cisco bug ID CSCdw19195. There are workarounds available to mitigate the vulnerability.

**Applicable Platforms**
Cisco CATOS Devices

**References**
CISCO PSIRT Advisories and Notices (20776 of 1.2)

Security Advisories: For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices: For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
CATOS PSIRT-20776: Verify Telnet Buffer Vulnerability [IOS]

**Description**
Some Cisco Catalyst switches, running certain CatOS-based software releases, have a vulnerability wherein a buffer overflow in the Telnet option handling can cause the Telnet daemon to crash and result in a switch reload. This vulnerability can be exploited to initiate a denial of service (DoS) attack. Once the switch has reloaded, it is still vulnerable and the attack can be repeated as long as the switch is IP reachable on port 23 and has not been upgraded to a fixed version of CatOS switch software.

**Applicable Platforms**
Cisco CATOS Devices

**Impact**
This vulnerability can be exploited to produce a denial of service (DoS) attack. When the vulnerability is exploited it can cause the Cisco Catalyst switch to crash and reload.

**Suggested Fix**
The following workarounds can be implemented.


- Apply IP Permit List for Telnet to enable access to the switch's management interface only from the network management workstations. Please note, this will not prevent spoofed IP packets with the source IP address set to that of the network management station from reaching the switch's management interface.

- On the Catalyst 6000 series switches, if the VLAN Access Control List (ACL) (VACL) feature is available in the code base, you can use VACLs instead of the IP Permit List workaround above. Please note, this will not prevent spoofed IP packets with the source IP address set to that of the network management station from reaching the switch's management interface.

- Implement the best practice to assign all of the management interfaces of all the switches in the network to a different VLAN, and apply appropriate ACLs on the router switching between the VLANs.
• Apply ACLs on routers / switches / firewalls in front of the vulnerable switches such that traffic destined for the Telnet port 23 on the vulnerable switches is only allowed from the network management workstations.

Cisco IOS Software IGMP Vulnerability - 112027 [IOS]

Description
A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS® Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(112027 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-112027: Verify Cisco IOS Software IGMP Vulnerability [IOS]

Description
To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the show version command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to “Cisco Internetwork Operating System Software” or “Cisco IOS Software.” The image name displays in parentheses, followed by “Version” and the Cisco IOS Software release name. Other Cisco devices do not have the show version command or may provide different output. The following example identifies a Cisco product that is running Cisco IOS Software Release 12.4(20)T with an installed image name of C1841-ADVENTERPRISEK9-M:

Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
Additional information about Cisco IOS Software release naming conventions is available in White Paper: Cisco IOS and NX-OS Software Reference Guide.

Applicable Platforms
Cisco IOS Devices
Impact
Successful exploitation of this vulnerability may cause the affected device vulnerable device to reload. Repeated exploitation may result in a sustained DoS condition.

Suggested Fix
Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.

IGMP version 2
Customers who do not require the Source Specific Multicast (SSM) functionality can use IGMP version 2 as a workaround.

```
interface GigabitEthernet0/0
  ip address 192.168.0.1 255.255.255.0
  ip pim sparse-mode
  ip igmp version 2
```

Control Plane Policing
A partial mitigation of the vulnerability described in this document is to block IGMP packets with an IP Time to Live (TTL) field value that is not equal to 1. RFC1054 , "Host Extensions for IP Multicasting" RFC2236 , "Internet Group Management Protocol Version 2", and RFC3376 , "Internet Group Management Protocol Version 3", indicate that every IGMP message is sent with an IP TTL of 1.

CoPP may be configured on a device to protect the management and control planes, and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to your network. Drop of IGMP packets with unicast IP destination addresses can also be implemented with CoPP if the network is using all multicast applications that utilize only multicast group destination addresses for IGMP packets.

```
!
!  -- The following access list is used
!  -- to determine what traffic needs to be dropped by a control plane
!  -- policy (the CoPP feature.) If the access list matches (permit),
!  -- then traffic will be dropped. If the access list does not
!  -- match (deny), then traffic will be processed by the router.
!  -- all IGMP packets with ttl different from 1 will be selected
!  -- by this acl and the "drop" action will be applied in the
!  -- corresponding CoPP policy
!

  ip access-list extended IGMP-ACL
    permit igmp any any ttl neq 1

!
```
class-map match-all drop-IGMP-class
   match access-group name IGMP-ACL

!- Create a policy map that will be applied to the
!- Control Plane of the device, and add the "drop-tcp-traffic"
!- class map.
!

policy-map CoPP-policy
   class drop-IGMP-class
      drop

!- Apply the policy map to the control plane of the
!- device.
!

control-plane
   service-policy input CoPP-policy

Additional information on the configuration and use of the CoPP feature is available in the Control Plane Policing Implementation Best Practices.

Crafted Encryption Packet DoS Vulnerability - 110393 [IOS]

Description
Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet.
Cisco has released free software updates that address this vulnerability.

**Applicable Platforms**
Cisco IOS Devices
References
CISCO PSIRT Advisories and Notices(110393 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-110393: Verify Crafted Encryption Packet DoS Vulnerability [IOS]

Description
A Cisco IOS device that is configured for SSLVPN or SSH may reload when it receives a specially crafted TCP packet on TCP port 443 (SSLVPN) or TCP port 22 (SSH). Completion of the three-way handshake to the associated TCP port number of these features is required for the vulnerability to be successfully exploited; however, authentication is not required. A Cisco IOS device that is configured for IKE encrypted nonces may reload when it receives a specially crafted UDP packet on port 500 or 4500 (if configured for NAT Traversal (NAT-T)).

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability described in this document may result in a reload of the device. The issue could be repeatedly exploited to cause an extended DoS condition.

Suggested Fix
There are no available workarounds other than disabling the affected features and protecting SSH access with the use of VTY access control lists.

Use the no webvpn enable command to disable SSL VPN use.

For Cisco IOS the SSH server can be disabled by applying the command crypto key zeroize rsa while in configuration mode. The SSH server is enabled automatically upon generating an RSA key pair. Zeroing the RSA keys is the only way to completely disable the SSH server.

Access to the SSH server on Cisco IOS Software may also be disabled by removing SSH as a valid transport protocol. This action can be done by reapplying the transport input command with 'ssh' removed from the list of permitted transports on vty lines while in configuration mode. For example:

```plaintext
line vty 0 4
    transport input telnet
end
```

If SSH server functionality is desired, access to the server can be restricted to specific source IP addresses or blocked entirely through the use of Access Control Lists (ACLs) on the vty lines as shown in the following URL:

More information on configuring ACLs can be found on Cisco's public website:
The following is an example of a vty access-list:

```plaintext
access-list 2 permit 10.1.1.0 0.0.0.255
access-list 2 deny any
line vty 0 4
  access-class 2 in
```

In the previous example, only the 10.1.1.0/24 network is allowed to SSH to the Cisco IOS device.

To disable IKE encrypted nonces use the `no authentication rsa-encr` command under an ISAKMP policy, as shown in the following example:

```plaintext
crypto isakmp policy
  no authentication rsa-encr
```

Crafted ICMP Messages DoS for IPSec Tunnels - 64520 [IOS]

**Description**

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" ([draft-gont-tcpm-icmp-attacks-03.txt](#)).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

- Attacks that use ICMP "hard" error messages
- Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
- Attacks that use ICMP "source quench" messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

See "Crafted ICMP Messages Can Cause Denial of Service" at Cisco Security Advisories website.

**Applicable Platforms**

Cisco IOS Devices

CISCO PSIRT Advisories and Notices (64520 of 1.3)

Security Advisories: For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices: For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PSIRT-64520: Verify Crafted ICMP Messages DoS for IPsec Tunnels Vulnerability [IOS]

**Description**

IP Security (IPSec): when an IOS device is configured to use IPSec, PMTUD is enabled by default, and therefore, the device may be affected by the PMTUD attack described in this document. An IOS device is configured for IPSec if either crypto map or tunnel protection is applied to an interface.
For example:

crypto ipsec profile IPSEC_PROFILE
    [...]  
!  
crypto map MYMAP 1 ipsec-isakmp
    [...]  
!  
interface Tunnel0  
    tunnel protection ipsec profile IPSEC_PROFILE
    [...]  
!  
interface Ethernet1  
    crypto map MYMAP
    [...]  

**Generic Routing Encapsulation (GRE) and IPinIP**: devices configured to use these tunneling protocols are vulnerable to crafted ICMP "fragmentation needed and DF bit set" messages if PMTUD is enabled. PMTUD is *disabled by default* for these two protocols. The device is vulnerable if the command `tunnel path-mtu-discovery` is present in the configuration.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
These attacks may result in Denial-of-Service conditions. No remote code execution or unauthorized access results from these types of attacks.

**Suggested Fix**
**IPSec**
For IPSec, the recommended workaround is to "disable" PMTUD. Please note that there is not a single command to disable PMTUD under IPSec, but this can be achieved through other mechanisms. In particular, the following two things must be done:

1. Filter out ICMP "fragmentation needed and DF bit set" messages (type 3, code 4) destined to the router itself using an Access Control List or the Control Plane Policing (CoPP) feature. The following example shows how to block ICMP "fragmentation needed and DF bit set" (type 3, code 4) messages that are addressed to any of the device's IP addresses using an interface ACL (note how the type 3, code 4 message is specified using the `packet-too-big` keyword):

```plaintext
access-list 111 deny icmp any host <fa0/0's IP address> packet-too-big  
access-list 111 deny icmp any host <fa0/1's IP address> packet-too-big  
access-list 111 deny icmp any host <fa0/2's IP address> packet-too-big  
access-list 111 permit ip any any  
!  
interface fastEthernet 0/0  
    ip access-group 111 in  
    !
```
interface fastEthernet 0/1
  ip access-group 111 in
!
interface fastEthernet 0/2
  ip access-group 111 in

Note
CoPP is available in IOS release trains 12.0S, 12.2S and 12.3T.

2. Allow IPSec to fragment the embedded packet even when the DF bit is set. This can be accomplished by using the command `crypto ipsec df-bit clear` (which is available in IOS 12.2(2)T and later) or by using Policy-Based Routing (PBR) (available in IOS 12.1(6) and later) to clear the DF bit. What follows is an example of how to use PBR to clear the DF bit:

```
route-map clear-df permit 10
match ip address 101

卓越 The following command is used to change the
卓越 Don't Fragment (DF) bit value in the IP header;
卓越 it must be used in route-map configuration mode.

set ip df 0

access-list 101 permit tcp 10.1.3.0 0.0.0.255 any

interface ethernet0
...
卓越 The following command is used to identify a
卓越 route map to use for policy routing on an
卓越 interface; if must be used in interface
卓越 configuration mode.

ip policy route-map clear-df
```

In this example the route-map is applied to the interface where the unencrypted traffic enters the router, and 10.1.3.0/24 is the address space that is sending traffic through the IPSec tunnel.

**Generic Routing Encapsulation and IPinIP**

The only workaround for this case is to disable PMTUD on the tunnel interface if it has been enabled. This is accomplished via the command `no tunnel path-mtu-discovery`, while in the specific tunnel interface configuration mode.
Without the `tunnel path-mtu-discovery` command configured, the DF bit will always be cleared in the GRE IP header. This allows the GRE IP packet to be fragmented, even though the encapsulated data IP header had the DF bit set, which normally wouldn't allow the packet to be fragmented.

Please note that if you are using GRE with IPSec you need to use the command `no tunnel path-mtu-discovery` instead of the command `crypto ipsec df-bit clear` to make sure that DF bit is cleared in transmitted packets; and you also need to filter out ICMP "fragmentation needed and DF bit set" messages (type 3, code 4) destined to the router itself using an Access Control List or the Control Plane Policing (CoPP) feature as described above.

If you have an image that is fixed for Cisco Bug IDSCSe44699 (registered customers only) you can set a low limit on the MTU that is learned via the PMTUD process by using the new command `tunnel path-mtu-discovery min-mtu <minimum MTU>` under the specific tunnel interface configuration mode.

**Crafted ICMP Messages DoS for L2TPv2 - 64520 [IOS]**

**Description**

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

- Attacks that use ICMP "hard" error messages
- Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
- Attacks that use ICMP "source quench" messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

See "Crafted ICMP Messages Can Cause Denial of Service" at Cisco Security Advisories website.

**Applicable Platforms**

Cisco IOS Devices

**References**

CISCO PSIRT Advisories and Notices(64520 of 1.3)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PSIRT-64520: Verify Crafted ICMP Messages DoS for L2TPv2 Vulnerability [IOS]
Description
Layer 2 Tunneling Protocol Version 2 (L2TP) and Layer 2 Tunneling Protocol Version 3 (L2TPv3): devices configured to use these tunneling protocols are vulnerable to crafted ICMP "fragmentation needed and DF bit set" messages if PMTUD is enabled. PMTUD is disabled by default for these protocols. A device running L2TP is vulnerable if the command `ip pmtu` appears in the device's configuration.

Note
L2TP (version 2) and L2TPv3 (version 3) are two different and independent protocols. Both are affected, but throughout the rest of this document we will refer to them as one since they are affected in the same manner.

Applicable Platforms
Cisco IOS Devices

Impact
These attacks may result in Denial-of-Service conditions. No remote code execution or unauthorized access results from these types of attacks.

Suggested Fix
The only workaround to protect Layer 2 Tunneling Protocol sessions (both versions 2 and 3) against PMTUD attacks is to disable PMTUD if it has been enabled. For L2TPv2, this is done via the `no ip pmtu` command in `vpdn-group` configuration mode as shown here:

```
router(config)#vpdn enable
router(config)#vpdn-group 1
router(config-vpdn)#no ip pmtu
```

For L2TPv3, this is done via the commands `no ip pmtu` and `no ip dfbit set` in `pseudowire-class` configuration mode as shown here:

```
pseudowire-class [pseudowire class name]
   encapsulation l2tpv3
   no ip pmtu
   no ip dfbit set
   {...}
```

For L2TPv2, if you have an image that is fixed for Cisco Bug ID CSCsa52807 (registered customers only) you can set low and high limits on the MTU that is learned via the PMTUD process by using the new commands `vpdn pmtu minimum <minimum MTU>` and `vpdn pmtu maximum <maximum MTU>` under `vpdn-group` configuration mode.
Crafted ICMP Messages DoS for TCP over IPv4 - 64520 [IOS]

Description
A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt)

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:
1. Attacks that use ICMP "hard" error messages
2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP "source quench" messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

See "Crafted ICMP Messages Can Cause Denial of Service" at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(64520 of 1.3)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-64520: Verify Crafted ICMP Messages DoS for TCP over IPv4 Vulnerability [IOS]

Transmission Control Protocol over Internet Protocol (IP) Version 4: if an IOS device establishes TCP sessions with other devices, for example, to speak Border Gateway Protocol (BGP) with other peers, it may be vulnerable to crafted ICMP "fragmentation needed and DF bit set" error messages if PMTUD is enabled. PMTUD is disabled by default for TCP in IOS. PMTUD is enabled if the command ip tcp path-mtu-discovery is present in the device configuration.

Applicable Platforms
Cisco IOS Devices

Impact
These attacks may result in Denial-of-Service conditions. No remote code execution or unauthorized access results from these types of attacks.
Suggested Fix

Transmission Control Protocol Over IP Version 4

If PMTUD has been explicitly enabled, a possible workaround to prevent PMTU D attacks is to disable it by using the global configuration command `no ip tcp path-mtu-discovery`. Once this command is executed, PMTUD will be disabled for all new TCP connections; configuring PMTD on the IOS device does not have any effect on existing TCP sessions already established from/to the router.

Please note that with PMTUD disabled, the MSS that will be used will be the value set with the `ip tcp mss` command, or the default of 536 bytes for remote destinations, or 1460 bytes for local destinations.

Crafted ICMP Messages DoS for TCP over IPv6 - 64520 [IOS]

Description

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt)

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP "hard" error messages
2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP "source quench" messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

See "Crafted ICMP Messages Can Cause Denial of Service" at Cisco Security Advisories website.

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices(64520 of 1.3)

Security Advisories: For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices: For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule

PSIRT-64520: Verify Crafted ICMP Messages DoS for TCP over IPv6 Vulnerability [IOS]

Description

Transmission Control Protocol over Internet Protocol Version 6 (IPv6): PMTUD is enabled by default for IPv6; therefore, devices configured for IPv6 are vulnerable to PMTUD attacks if they are running services that rely on TCP, like BGP. If the device is just forwarding IPv6 traffic, i.e., it does not establish TCP sessions with other hosts, then it is not affected.
Applicable Platforms
Cisco IOS Devices

Impact
These attacks may result in Denial-of-Service conditions. No remote code execution or unauthorized access results from these types of attacks.

Suggested Fix
Transmission Control Protocol Over IP Version 6
PMTUD is enabled by default when using TCP over IPv6, and it is not possible to disable it. For this reason a possible workaround is to use an ACL to block the ICMPv6 "packet too big" message.

Please note that filtering out ICMPv6 "packet too big" messages means that the layer 3 (IPv6) PMTUD is being shut down as well. Therefore, it is necessary to make sure that the MTU is set on the end host to the lowest possible IPv6 MTU - 1280 bytes. Otherwise, since the device is not seeing the "packet too big" message, the device will not know that an intermediate system has dropped a packet because it was too big.

ICMPv6 "packet too big" messages are the IPv6 equivalent to the ICMPv4 "fragmentation needed and DF bit set" message.

Crafted IP Option - 81734 [IOS]

Description
Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

Cisco has made free software available to address this vulnerability for affected customers.

There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability was discovered during internal testing.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(81734 of 1.4)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-81734 : Verify Crafted IP Option Can Cause DoS Vulnerability [IOS]
Description
This vulnerability may be exploited when an affected device processes a packet that meets all three of the following conditions:

1. The packet contains a specific crafted IP option.
   \[ \text{AND} \]
2. The packet is one of the following protocols:
   - ICMP - Echo (Type 8) - 'ping'
   - ICMP - Timestamp (Type 13)
   - ICMP - Information Request (Type 15)
   - ICMP - Address Mask Request (Type 17)
   - PIMv2 - IP protocol 103
   - PGM - IP protocol 113
   - URD - TCP Port 465
   \[ \text{AND} \]
3. The packet is sent to a physical or virtual IPv4 address configured on the affected device.

No other ICMP message types are affected by this issue.
No other IP protocols are affected by this issue.
No other TCP services are affected by this issue.
The packet can be sent from a local network or from a remote network.
The source IP address of the packet can be spoofed or non-spoofed.
Packets which transit the device (packets not sent to one of the device's IP addresses) do not trigger the vulnerability and the device is not affected.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability on Cisco IOS may result in a reload of the device or execution of arbitrary code. Repeated exploitation could result in a sustained DoS attack.

Suggested Fix
Configure \textit{ip option drop} configuration command to drop IP packets that has options.
Crafted TCP Packet Denial of Service Vulnerability - 111450  [IOS]

Description
Cisco IOS\(^2\) Software is affected by a denial of service vulnerability that may allow a remote unauthenticated attacker to cause an affected device to reload or hang. The vulnerability may be triggered by a TCP segment containing crafted TCP options that is received during the TCP session establishment phase. In addition to specific, crafted TCP options, the device must have a special configuration to be affected by this vulnerability.

Cisco has released free software updates that address this vulnerability.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(111450 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices for issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-111450: Verify Crafted TCP Packet DoS Vulnerability [IOS]

Description
Cisco IOS Software is affected by a denial of service vulnerability that may allow a remote unauthenticated attacker to cause a device reload or hang.

The vulnerability may only be triggered by a TCP segment received during the TCP session establishment phase. The received TCP segment must contain crafted, not malformed, TCP options. A TCP three-way handshake does not need to be completed to exploit the vulnerability.

To be affected by this vulnerability, a device must be configured for any of the following:
- A specific TCP receive window size
- PMTUD
- SNAT with TCP as the transport protocol

The vulnerability exists in the TCP options processing code of Cisco IOS Software. When the vulnerability is triggered, Cisco IOS Software enters an infinite loop that may cause the device to reload or hang. The following syslog messages may indicate that this vulnerability has been exploited:

%SYS-3-CPUHOG: Task is running for (128004)msecs, more than (2000)msecs (23/1),process = IP Input.

-Tracback= 0x41CA6AC4 0x41C83170 0x41A2724 0x41F249D4 0x41A24A34 0x41B24C58
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = IP Input.
BGP Considerations
This vulnerability could be exploited through the BGP port (TCP port 179) if all the following conditions are met:

- The device is configured for one or more of the features that make a device affected, as explained above. Note that in recent versions of Cisco IOS Software, configuring BGP automatically enables PMTUD for all BGP neighbor sessions.
- The source IP address of an attack packet is the IP address of a configured BGP peer.
- If the BGP TTL Security Hack (BTSH)/Generalized TTL Security Mechanism (GTSM) is configured, the TTL of the received attack packet is within the allowed TTL range.
- If the BGP peering session is protected by the TCP MD5 option, the attack packet has the correct MD5 hash.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability may cause the affected device to reload or hang. Repeated exploitation could result in a sustained denial of service condition. In the case of a hang, cycling power to the device may be required to put the device back in service.

Suggested Fix
There are no workarounds to mitigate this vulnerability other than disabling the specific features that make a device vulnerable, if feasible.

Additionally, allowing only legitimate devices to connect to affected devices will help limit exposure to this vulnerability. Since a TCP three-way handshake is not required, to increase effectiveness, the mitigation must be coupled with anti-spoofing measures on the network edge.

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco IOS Software Crafted TCP Packet Denial of Service Vulnerability".

Configurations Using a Specific TCP Window Size
Not setting a specific TCP receive window size can be accomplished by removing the ip tcp window-size command from the configuration.

Configurations Using Path MTU Discovery
PMTUD may be disabled in some of the Cisco IOS Software features that make use of PMTUD. The specific command to use to disable PMTUD varies depending on the specific feature:

- TCP over IPv4: removing the ip tcp path-mtu-discovery command from the configuration will disable PMTUD for TCP over IPv4 sessions that originate on the device.
- TCP over IPv6: PMTUD is enabled by default for IPv6 and cannot be disabled.
- BGP: if BGP is configured on a recent version of Cisco IOS Software that enables PMTUD for BGP sessions, PMTUD can be disabled for all BGP sessions with the no bgp transport path-mtu-discovery command in router configuration mode (Cisco IOS Release 12.2(33)SRA, 12.2(31)SB, 12.2(33)SXH, 12.4(20)T, and later releases).

Configurations Using Stateful NAT with TCP as the Transport Protocol
SNAT can be disabled by removing the ip nat Stateful id command from the configuration.

Control Plane Policing
For devices that need to offer TCP services, it is possible to use Control Plane Policing (CoPP) to block TCP traffic to the device from untrusted sources. Cisco IOS Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to specific network configurations:

```
!-- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.
!-- Everything else is not trusted. The following access list is used
!-- to determine what traffic needs to be dropped by a control plane
!-- policy (the CoPP feature.) If the access list matches (permit)
!-- then traffic will be dropped and if the access list does not
!-- match (deny) then traffic will be processed by the router.
!-- Note that TCP ports 22 and 23 are just examples; this configuration
!-- needs to be expanded to include all used TCP ports.
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 23
access-list 100 deny tcp host 172.16.1.1 any eq 22
access-list 100 deny tcp host 172.16.1.1 any eq 23
access-list 100 permit tcp any any

!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices.
!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature.
class-map match-all drop-tcp-class
    match access-group 100
```
Understanding Compliance and Audit Manager (CAAM) Policies

```
!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device, and add the "drop-tcp-traffic"
!-- class map.
policy-map control-plane-policy
class drop-tcp-class
drop

!-- Apply the Policy-Map to the Control-Plane of the
!-- device.
control-plane
  service-policy input control-plane-policy
```

**Warning** Because a TCP three-way handshake is not required to exploit this vulnerability, it is possible to easily spoof the IP address of the sender, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses.

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function.


**Configuring Infrastructure Access Lists (iACLs)**

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

**BGP Considerations**

BTSH/GTSM can help prevent exploitation of this vulnerability via the BGP port because packets coming from devices that do not pass the TTL check configured via BTSH are dropped before any TCP processing takes place. For information on BTSH refer to: http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_btsh.html

MD5 authentication for BGP peering sessions can also help prevent exploitation via the BGP port because the MD5 hash in an attack packet is checked before processing the crafted TCP option. For a detailed discussion on how to configure BGP, refer to the following document: http://www.cisco.com/en/US/docs/ios/redirect/eol.html
Crafted UDP Packet Vulnerability - 108558 [IOS]

Description
Several features within Cisco IOS Software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(108558 of 1.2)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-108558: Verify Crafted UDP Packet Vulnerability [IOS]

Description
Devices running affected versions of Cisco IOS Software and Cisco IOS XE Software are affected when running any of the following features:

- IP Service Level Agreements (SLA) Responder
- Session Initiation Protocol (SIP)
- H.323 Annex E Call Signaling Transport
- Media Gateway Control Protocol (MGCP)

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of this vulnerability may cause the inbound interface to be blocked and will silently drop any received traffic. A reload of the device is required to restore normal functionality.

Suggested Fix
The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.
Disable Affected Listening Ports

If an affected feature is not required it can be explicitly disabled. Once disabled confirm the listening UDP port has been closed by entering the CLI command "show udp" or "show ip socket". Some features may require a reload of the device after disabling the feature in order to close the listening UDP port.

For SIP it is possible to disable UDP listening if only TCP services are required. The following example shows how to disable SIP from listening on its associated UDP port.

Infrastructure Access Control Lists

Warning

Because the features in this vulnerability utilize UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure Access Control Lists (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability.

Control Plane Policing

Warning

Because the features in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations.

Exploit Detection

It is possible to detect blocked interface queues with an Cisco IOS Embedded Event Manager (EEM) policy. EEM provides event detection and reaction capabilities on a Cisco IOS device. EEM can alert administrators of blocked interfaces with email, a syslog message, or a Simple Network Management Protocol (SNMP) trap.

Crypto - 91890 [IOS]

Description

A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).
Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker to decrypt any previously encrypted information.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices (91890 of 1.3)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT-91890: Verify For Vulnerabilities In Crypto Library Vulnerability [IOS]

**Description**
A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker to decrypt any previously encrypted information.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
Successful exploitation of the vulnerability listed in this advisory may result in the crash of a vulnerable device. Repeated exploitation can result in a sustained DoS attack.

**Suggested Fix**
The only way to prevent a device being susceptible to the listed vulnerabilities is to disable the affected service(s). However, if regular maintenance and operation of the device relies on these services then there is no workaround.

It is possible to mitigate these vulnerabilities by preventing unauthorized hosts to access the affected devices. Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document.
DFS ACL Leakage - 13655 [IOS]

Description
Errors in certain Cisco IOS software versions for certain routers can cause IP datagrams to be output to network interfaces even though access lists have been applied to filter those datagrams. This applies to routers from the Cisco 7xxx family only, and only when those routers have been configured for distributed fast switching (DFS).

There are two independent vulnerabilities, which have been given Cisco bug IDs CSCdk35564 and CSCdk43862. Each vulnerability affects only a specialized subset of DFS configurations. Affected configurations are not believed to be extremely common, but neither are they extremely rare. More details of affected configurations are in the "Who is Affected" section of this document.

These vulnerabilities may permit users to send packets to parts of the customer's network for which they are not authorized. This may permit unauthorized access or other attacks on customer computer systems or data. Cisco does not know of any incidents in which these vulnerabilities have actually been exploited by attackers.

Neither vulnerability affects any Cisco product other than routers in the 70xx or 75xx series. Of 70xx routers, only routers with the optional route-switch processor (RSP) card are affected. Additional configuration conditions apply.

See "Cisco IOS DFS Access List Leakage." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(13655 of 1.3)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-13655 : Verify DFS Access List Leakage Vulnerability [IOS]

Description
Errors in certain Cisco IOS software versions for certain routers can cause IP datagrams to be output to network interfaces even though access lists have been applied to filter those datagrams. This applies to routers from the Cisco 7xxx family only, and only when those routers have been configured for distributed fast switching (DFS).

There are two independent vulnerabilities, which have been given Cisco bug IDs CSCdk35564 and CSCdk43862. Each vulnerability affects only a specialized subset of DFS configurations. Affected configurations are not believed to be extremely common, but neither are they extremely rare. More details of affected configurations are in the "Who is Affected" section of this document.

These vulnerabilities may permit users to send packets to parts of the customer's network for which they are not authorized. This may permit unauthorized access or other attacks on customer computer systems or data. Cisco does not know of any incidents in which these vulnerabilities have actually been exploited by attackers.
Neither vulnerability affects any Cisco product other than routers in the 70xx or 75xx series. Of 70xx routers, only routers with the optional route-switch processor (RSP) card are affected. Additional configuration conditions apply.

See "Cisco IOS DFS Access List Leakage." at Cisco Security Advisories website

**Applicable Platforms**
Cisco IOS Devices

**Impact**
Incorrect access-list filtering may be applied to output packets. Output access lists are frequently used to implement security filtering, and the failure of such access lists may permit users to send packets to parts of the network for which they are not authorized. This, in turn, may permit them to bypass security restrictions, and to gain access to data or resources from which they should be excluded.

Neither of the defects described in this notice "fails reliably". The same access lists, on the same interfaces, may work correctly at some times, and fail at other times. Because of this, administrators who test their access lists may be misled into believing that the access lists are providing effective protection, when in fact they are not.

CSCdk43862 may result in legitimate traffic being filtered out, as well as in undesired traffic being permitted to pass through the router. CSCdk35564 never filters legitimate traffic; it only permits undesired traffic.

An attacker who had detailed knowledge of these vulnerabilities might be able to create conditions favorable to unauthorized access being permitted. However, such activity would probably be unnecessary; even without deliberate intervention by an attacker, such conditions would be expected to occur frequently during the operation of most affected networks.

**Suggested Fix**
These vulnerabilities can be worked around by disabling DFS on network interfaces (with no ip route-cache distributed). Be aware that the purpose of DFS is to transfer computational load from the router's primary CPU to the CPUs on the VIP cards, and that disabling DFS may therefore cause overload of the primary CPU. Evaluate your traffic load and CPU usage before using this workaround.

If all interfaces in the router are DFS-capable, but DFS has for some reason been enabled only on some of the interfaces, it may be possible to work around CSCdk35564 by enabling DFS on all interfaces. This will not affect CSCdk43862.

CSCdk43862 can sometimes be worked around by reconfiguring to use the same output access list on all the subinterfaces of a physical interface.

Another possible workaround is to redesign the access lists structure on the router to avoid the need for output access lists on affected interfaces.

**DHCP - 63312 [IOS]**

**Description**
Cisco IOS devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices (63312 of 1.2)

Security Advisories: For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices: For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-63312: Verify DHCP Blocked Interface Denial-of-Service Vulnerability [IOS]

Description
Cisco IOS devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets.

See "Cisco IOS DHCP Blocked Interface Denial-of-Service." at Cisco Security Advisories website for more information.

Applicable Platforms
Cisco IOS Devices

Impact
A device receiving these specifically crafted DHCP packets will force the inbound interface to stop processing traffic. The device may stop processing packets destined to the router, including routing protocol packets and ARP packets. No alarms will be triggered, nor will the router reload to correct itself. This vulnerability may be exercised repeatedly resulting in loss of availability until a workaround has been applied or the device has been upgraded to a fixed version of code.

Suggested Fix
This vulnerability can be mitigated by utilizing the command, "no service dhcp". However, this workaround will disable all DHCP processing on the device, including the DHCP helper functionality that may be necessary in some network configurations.

DLSw Denial of Service Vulnerabilities - 99758 [IOS]

Description
Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

Applicable Platforms
Cisco IOS Devices
Rule 1

Rule
PSIRT-99758: Verify Multiple DLSw Denial of Service Vulnerabilities in Cisco [IOS]

Description
Data-link switching (DLSw) provides a means of transporting IBM Systems Network Architecture (SNA) and network basic input/output system (NetBIOS) traffic over an IP network. Cisco implementation of DLSw also uses UDP port 2067 and IP Protocol 91 for Fast Sequenced Transport (FST).

Multiple vulnerabilities exists in Cisco IOS when processing UDP and IP protocol 91 packets. These vulnerabilities do not affect TCP packet processing. A successful exploitation may result in a reload of the system or a memory leak on the device, leading to a denial of service (DoS) condition.

Cisco IOS devices configured for DLSw with `dlsw local-peer` automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the `dlsw local-peer peer-id <IP-address>` command listen for IP protocol 91 packets and UDP port 2067.

Cisco IOS devices listen to IP protocol 91 packets when DLSw is configured. However, it is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

```
dlsw remote-peer 0 fst <ip-address>
```

It is possible to disable UDP processing in DLSw with the `dlsw udp-disable` command. However, disabling UDP only prevents the sending of UDP packets, it does not prevent the device from receiving and processing incoming UDP packets.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of these vulnerabilities may result in the reload of the device or memory leaks, leading to a DoS condition.

Suggested Fix
The workaround consists of filtering UDP packets to port 2067 and IP protocol 91 packets. Filters can be applied at network boundaries to filter all IP protocol 91 packets and UDP packets to port 2067 or can be applied on individual affected devices to permit such traffic only from trusted peer IP addresses. However, since both of the protocols are connectionless, it is possible for an attacker to spoof malformed packets from legitimate peer IP addresses.

As soon as DLSw is configured, the Cisco IOS device begins listening on IP protocol 91. However, this protocol is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

dls w remote-peer 0 fst <ip-address>

If FST is used, filtering IP protocol 91 will break the operation, so filters need to permit protocol 91 traffic from legitimate peer IP addresses.

It is possible to disable UDP processing in DLSw with the dlsw udp-disable command. However, disabling UDP only prevents the sending of UDP packets, it does not prevent the receiving and processing of incoming UDP packets. To protect a vulnerable device from malicious packets via UDP port 2067, both of the following actions must be taken:

1. Disable UDP outgoing packets with the "dlsw udp-disable" command, AND
2. Filter UDP 2067 in the vulnerable device using infrastructure ACL.

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.

DLSw Vulnerability - 77859 [IOS]

Description
A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device. Applicable Platforms

Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(77859 of 1.2)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-77859: Check for DLSw Vulnerability [IOS]

Description
Data-link switching (DLSw) provides a means of transporting IBM Systems Network Architecture (SNA) and network basic input/output system (NetBIOS) traffic over an IP network. Establishing DLSw communications involves several operational stages.

In phase one, DLSw peers establish two TCP connections with each other via TCP ports 2065 or 2067. Those TCP connections provide the foundation for the DLSw communication.

After a connection is established, the DLSw partners exchange a list of supported capabilities in phase two. This helps to ensure that the peers use the same options. This is particularly vital when the DLSw partners are manufactured by different vendors.

Next, the DLSw partners establish circuits between SNA or NetBIOS end systems, and information frames can flow over the circuit.

A vulnerability exists in certain Cisco IOS software releases when configured for DLSw. After the connection is established, it is possible for a reload to occur should the device receive an invalid option during the capabilities exchange.
Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability may result in a reload of the device.

Suggested Fix
If DLSw is configured with no remote peers defined, then it must be operating in promiscuous mode on one end of the connection. Promiscuous mode could allow for any device to attempt to establish a DLSw peer with the router. To prevent malicious connections, DLSw peers may be explicitly defined with the dlsw remote-peer command removing the need for promiscuous mode.

FTP Server - 90782 [IOS]

Description
The Cisco IOS FTP Server feature contains multiple vulnerabilities that can result in a denial of service (DoS) condition, improper verification of user credentials, and the ability to retrieve or write any file from the device filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

This vulnerability does not apply to the IOS FTP Client feature.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(90782 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-90782: Check for Multiple Vulnerabilities in the IOS FTP Server [IOS]
Description

Multiple vulnerabilities exist in the IOS FTP Server feature. These vulnerabilities are documented with the following Cisco bug IDs:

- CSCek55259 - Improper authorization checking in IOS FTP server
- CSCse29244 - IOS reload when transferring files via FTP

Due to these issues with the IOS FTP server, the feature is being removed. Cisco is considering adding fully featured and secure FTP server functionality at a later date.

The IOS FTP Server feature removal is addressed with Cisco bug ID CSCsg16908.

Applicable Platforms

Cisco IOS Devices

Impact

Successful exploitation of these vulnerabilities may allow unauthorized, remote users to access the filesystem on the IOS device, cause the affected device to reload, or execute arbitrary code.

Unauthorized users could retrieve the device's startup-config file from the filesystem. This file may contain information that could allow the attacker to gain escalated privileges.

Repeated exploitation of the vulnerabilities could lead to an extended Denial of Service (DoS).

Suggested Fix

Customers can disable the use of the IOS FTP Server feature by executing the following command in configuration mode:

`no ftp-server enable`

Firewall Application Inspection Control Vulnerability - 107716 [IOS]

Description

Cisco IOS software configured for IOS firewall Application Inspection Control (AIC) with a HTTP configured application-specific policy are vulnerable to a Denial of Service when processing a specific malformed HTTP transit packet. Successful exploitation of the vulnerability may result in a reload of the affected device.

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices(107716 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule

PSIRT-107716: Verify Firewall Application Inspection Control Vulnerability [IOS]
Description
Firewalls are networking devices that control access to an organization's network assets. Firewalls are often positioned at the entrance points into networks. Cisco IOS software provides a set of security features that enable you to configure a simple or elaborate firewall policy, according to your particular requirements.

HTTP uses port 80 by default to transport Internet web services, which are commonly used on the network and rarely challenged with regard to their legitimacy and conformance to standards. Because port 80 traffic is typically allowed through the network without being challenged, many application developers are leveraging HTTP traffic as an alternative transport protocol that will allow their application's traffic to travel through or even bypass the firewall. When the Cisco IOS Firewall is configured with HTTP AIC, it performs packet inspection to detect HTTP connections that are not authorized in the scope of the security policy configuration. It also detects users who are tunneling applications through port 80. If the packet is not in compliance with the HTTP protocol, it will be dropped, the connection will be reset, and a syslog message will be generated, as appropriate.

Cisco IOS Software that is configured for IOS firewall AIC with an HTTP application-specific policy is vulnerable to a denial of service condition when it processes a specific malformed HTTP transit packet. Successful exploitation of the vulnerability may result in a reload of the affected device.

HTTP runs over TCP. For this vulnerability to be exploited, a full three-way handshake between client and server is required before any malicious traffic would be processed to result in a device reload.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability may result in a reload of the affected device. Repeated exploitation attempts may result in a sustained denial of service attack.

Suggested Fix
There are no known workarounds for this vulnerability. The only known action to help counter this vulnerability is to disable AIC HTTP deep packet inspection in the affected device's configuration. Disabling deep packet HTTP inspection will allow the rest of the firewall features to continue to function until a software upgrade can be implemented. All other firewall features will continue to perform normally.

Disabling AIC HTTP Deep Packet Inspection
To disable AIC HTTP Deep Packet Inspection, remove the linkage between policy-map type inspect layer4-policymap and policy-map type inspect http layer7-policymap. This example shows an existing configuration, followed by how to remove AIC HTTP Deep Packet Inspection:

```plaintext
!--- Existing Configuration
!

parameter-map type inspect global
!

class-map type inspect http match-any layer7-classmap
class-map type inspect match-any layer4-classmap
match protocol http
```
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

! policy-map type inspect http layer7-policymap
class type inspect http layer7-classmap
  allow
class class-default
policy-map type inspect layer4-policymap
class type inspect layer4-classmap
  inspect global
  service-policy http layer7-policymap
class class-default
!

zone security inside
description ** Inside Network **
zone security outside
description ** Outside Network **
zone-pair security in2out source inside destination outside
description ** Zone Pair - inside to outside **
service-policy type inspect layer4-policymap

Remove the service-policy from the zone-pair in question:
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#zone-pair security in2out source inside destination outside
Router(config-sec-zone-pair)#no service-policy type inspect layer4-policymap
Router(config-sec-zone-pair)#exit

Remove the linkage between policy-map type inspect layer4-policymap and policy-map type inspect http layer7-policymap:
Router(config)#policy-map type inspect layer4-policymap
Router(config-pmap)#class type inspect layer4-classmap
Router(config-pmap-c)#no service-policy http layer7-policymap
Router(config-pmap-c)#exit
Router(config-pmap)#exit

Reapply the service-policy to the zone-pair in question:
Router(config)#zone-pair security in2out source inside destination outside
Router(config-sec-zone-pair)#service-policy type inspect layer4-policymap
Router(config-sec-zone-pair)#exit

Although not required, for completeness of the configuration the policy-map type inspect http layer7-policymap and class-map type inspect http match-any layer7-classmap are recommended to be removed.

Router(config)#no policy-map type inspect http layer7-policymap
Router(config)#no class-map type inspect http match-any layer7-classmap
Router(config)#exit
Router#

H.323 Denial of Service Vulnerability - 111265 [IOS]

Description
The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (111265 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-111265: Verify H.323 Denial of Service Vulnerability [IOS]

Description
H.323 is the ITU standard for real-time multimedia communications and conferencing over packet-based (IP) networks. A subset of the H.323 standard is H.225.0, a standard used for call signaling protocols and media stream packetization over IP networks.

The H.323 implementation in Cisco IOS Software contains two DoS vulnerabilities. An attacker can exploit these vulnerabilities remotely by sending crafted H.323 packets to the affected device that is running Cisco IOS Software. A TCP three-way handshake is needed to exploit these vulnerabilities.

When exploited, the first vulnerability may lead to an interface queue wedge. The second vulnerability may cause a memory leak and, in most cases, the device to reload.

An interface queue wedge is a class of vulnerability in which certain packets are received and queued by a Cisco IOS router or switch, but due to a processing error, are never removed from the queue.
Received packets are counted against the interface input "queue," which is of a limited and relatively small size. For example, on most interface types on most platforms the default interface input queue is 75 packets, a value that can be configured via the hold-queue value in interface configuration command. Once the input queue contains nothing but packets that, due to a bug, will never be dequeued, the queue is said to be wedged. More recently this condition has been termed a "blocked interface".

This can be seen on a Cisco IOS device when the input queue size is equal to or greater than (depending on the Cisco IOS Software Release) the input queue max value, as shown below. In this example, the current "size" of the input queue is 75, which is equal to the "max" size of the input queue, which is also 75.

Router#show interface Ethernet 0/0

Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is 0001.0001.0001
  Internet address is 10.1.1.100/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, 
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:20, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 75/75/44/0 (size/max/drops/flushes);
  Total output drops: 0
  Queueing strategy:fifo

  Output queue: 0/40 (size/max)
  5 minute input rate 4000 bits/sec, 9 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    2937 packets input, 182298 bytes, 0 no buffer
    Received 7 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    58 packets output, 6540 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out

To display detected memory leaks, use the show memory debug leaks command in privileged EXEC mode.

Router#show memory debug leaks
Adding blocks for GD...

I/O memory

<table>
<thead>
<tr>
<th>Address</th>
<th>Size</th>
<th>Alloc_pc</th>
<th>PID</th>
<th>Alloc-Proc</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>640854D4</td>
<td>1940</td>
<td>622265A4</td>
<td>196</td>
<td>CCH323_CT</td>
<td>CCH323_CT</td>
</tr>
<tr>
<td>1940</td>
<td>622265A4</td>
<td>196</td>
<td>CCH323_CT</td>
<td>CCH323_CT</td>
<td></td>
</tr>
<tr>
<td>1940</td>
<td>622265A4</td>
<td>196</td>
<td>CCH323_CT</td>
<td>CCH323_CT</td>
<td></td>
</tr>
</tbody>
</table>

The previous example shows a memory leak in the process CCH323_CT. The show memory debug leaks command was introduced in Cisco IOS Software versions 12.3(8)T1 and 12.2(25)S, respectively.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
Successful exploitation of the vulnerabilities described in this advisory may cause the affected device to experience an interface queue wedge or to reload. These vulnerabilities could be exploited repeatedly to cause an extended DoS condition.

**Suggested Fix**
There are no workarounds to mitigate these vulnerabilities apart from disabling H.323 if the Cisco IOS device does not need it. Applying access lists on interfaces that should not accept H.323 traffic and putting firewalls in strategic locations may greatly reduce exposure until an upgrade can be performed.

Cisco provides Solution Reference Network Design (SRND) guides to help design and deploy networking solutions, which can be found at [http://www.cisco.com/go/srnd](http://www.cisco.com/go/srnd) Voice Security best practices are covered in the Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x.
You can use the call service stop forced command under the voice service voip mode, as shown in the following example:

```
voice service voip
h323
call service stop forced
```

**Note**  The call service stop forced command disables all H.323 call processing.

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Denial of Service Vulnerabilities in Cisco Unified Communications Manager and Cisco IOS Software", which is available at the following location:


### H.323 Protocol DoS Vulnerability - 110396 [IOS]

**Description**

The H.323 implementation in Cisco IOS Software contains a vulnerability that can be exploited remotely to cause a device that is running Cisco IOS Software to reload.

Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services.

**Applicable Platforms**

Cisco IOS Devices

**References**

CISCO PSIRT Advisories and Notices(110396 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

#### Rule 1

**Rule**


**Description**

H.323 is the ITU standard for real-time multimedia communications and conferencing over packet-based (IP) networks. A subset of the H.323 standard is H.225.0, a standard used for call signalling protocols and media stream packetization over IP networks.

The H.323 implementation in Cisco IOS Software contains a vulnerability. An attacker can exploit this vulnerability remotely by sending an H.323 crafted packet to the affected device that is running Cisco IOS Software. A TCP three-way handshake is needed to exploit this vulnerability.

**Applicable Platforms**

Cisco IOS Devices
Impact
Successful exploitation of the vulnerability described in this document may cause the affected device to reload. The issue could be exploited repeatedly to cause an extended DoS condition.

Suggested Fix
There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the Cisco IOS device does not need to run H.323 for VoIP services. Affected devices that must run H.323 are vulnerable, and there are not any specific configurations that can be used to protect them. Applying access lists on interfaces that should not accept H.323 traffic and putting firewalls in strategic locations may greatly reduce exposure until an upgrade can be performed.

Cisco provides Solution Reference Network Design (SRND) guides to help design and deploy networking solutions, which can be found at [http://www.cisco.com/go/srnd](http://www.cisco.com/go/srnd) Voice Security best practices are covered in the Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x.

Below is an example of an access list to block H.323 management traffic from anywhere but a permitted network. In this example, the permitted network is 172.16.0.0/16.

```plaintext
!--- Permit access from any IP address in the 172.16.0.0/16
!--- network to anywhere on port 1720.

access-list 101 permit tcp 172.16.0.0 0.0.255.255 any eq 1720

!--- Permit access from anywhere to a host in the
!--- 172.16.0.0/26 network on port 1720.

access-list 101 permit tcp any 172.16.0.0 0.0.255.255 eq 1720

!--- Deny all traffic from port 1720.

access-list 101 deny tcp any eq 1720 any

!--- Deny all traffic to port 1720.

access-list 101 deny tcp any any eq 1720

!--- Permit all other traffic.
```
access-list 101 permit ip any any

Alternatively, you can use the call service stop forced command under the voice service voip mode, as shown in the following example:

```sh
voice service voip
h323
call service stop forced
```

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Denial of Service Vulnerabilities in Cisco Unified Communications Manager and Cisco IOS Software".

**H323 DoS Vulnerability - 112021 [IOS]**

**Description**
The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices(112021 of 1.1)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT-112021: Verify Cisco IOS Software H323 DoS Vulnerability [IOS]

**Description**
Cisco devices that are running affected Cisco IOS Software versions that are configured to process H.323 messages are affected by these vulnerabilities. H.323 is not enabled by default.
To determine if the Cisco IOS Software device is running H.323 services, issue the show process cpu | include H323 command, as shown in this example:

Router# show process cpu | include H323
249       16000           3       5333  0.00%  0.00%  0.00%   0 CCH323_CT
250           0           1          0  0.00%  0.00%  0.00%   0 CCH323_DNS
Router#

In the previous example the processes CCH323_CT and CCH323_DNS are running on the device; therefore, the device is listening to H.323 messages. The device is vulnerable if any of these processes (or similar) are active.

Note
Creating a dial peer by issuing the **dial-peer voice** command will start the H.323 processes, which causes the Cisco IOS device to process H.323 messages.

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the **show version** command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

!--- output truncated

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.4(20)T with an installed image name of C1841-ADVENTERPRISEK9-M:

Router# show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T,
 RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide".

**Applicable Platforms**
Cisco IOS Devices

**Impact**
Successful exploitation of the vulnerability described in this document may cause the affected device to reload. The issue could be exploited repeatedly to cause an extended DoS condition.

**Suggested Fix**
There are no workarounds to mitigate these vulnerabilities apart from disabling H.323 if the Cisco IOS device does not require it. Applying access lists on interfaces that should not accept H.323 traffic and placing firewalls in strategic locations may greatly reduce exposure until an upgrade can be performed.

Cisco provides Solution Reference Network Design (SRND) guides to help design and deploy networking solutions. Voice Security best practices are covered in the Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x.

To disable all H.323 call processing, administrators can issue the `call service stop forced` command under the `voice service voip` mode, as shown in this example:

```
voice service voip
  h323
  call service stop forced
```

**Note**
The `call service stop forced` command disables all H.323 call processing.

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco Voice Products".

**HTTP - 13627 [IOS]**

**Description**
A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled and browsing to "http:///%%" is attempted. This defect can be exploited to produce a denial of service (DoS) attack. See "Cisco IOS HTTP Server Vulnerability." at Cisco Security Advisories website.

**Applicable Platforms**
Cisco IOS Devices
Chapter 4 Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

References
CISCO PSIRT Advisories and Notices(13627 of 1.1)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-13627: Verify HTTP Server Vulnerability [IOS]

Description
The HTTP server was introduced in IOS release 11.0 to extend router management to the worldwide web. The defect appears in a function added in IOS releases 11.1 and 11.2 that parses special characters in a URI of the format "%nn" where each "n" represents a hexadecimal digit. The vulnerability is exposed when an attempt is made to browse to "http:// / %%". Due to the defect, the function incorrectly parses "%%" and it enters an infinite loop. A watchdog timer expires two minutes later and forces the router to crash and reload. Once it has resumed normal operation, the router is again vulnerable to the same defect until the HTTP server is disabled, access from untrusted hosts is prohibited, or the router is upgraded to a release of Cisco IOS software that is not vulnerable to this defect. In rare cases, the affected device fails to reload, forcing the administrator to cycle the power to resume operation. Some devices have reloaded without providing stack traces and may indicate wrongly that they were "restarted by power-on" when that did not occur.

Applicable Platforms
Cisco IOS Devices

Impact
Any affected Cisco IOS device that is operating with the HTTP server enabled and is not protected against unauthorized connections can be forced to halt for a period of up to two minutes and then reload. The vulnerability can be exercised repeatedly, possibly creating a denial of service (DoS) attack, until such time as the HTTP server is disabled, the router is protected against the attack, or the software on the router is upgraded to an unaffected release of IOS.

Suggested Fix
Completely disable the HTTP server using the command no ip http server while in global configuration mode.

HTTP Auth - 13626 [IOS]

Description
When the HTTP server is enabled and local authorization is used, it is possible, under some circumstances, to bypass the authentication and execute any command on the device. In that case, the user will be able to exercise complete control over the device. All commands will be executed with the highest privilege (level 15).

See "IOS HTTP Authorization Vulnerability." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices
References

CISCO PSIRT Advisories and Notices (13626 of 1.8)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule

PSIRT-13626: Verify HTTP Authorization Vulnerability [IOS]

Description

When the HTTP server is enabled and local authorization is used, it is possible, under some circumstances, to bypass the authentication and execute any command on the device. In that case, the user will be able to exercise complete control over the device. All commands will be executed with the highest privilege (level 15).

See "IOS HTTP Authorization Vulnerability." at Cisco Security Advisories website

Applicable Platforms

Cisco IOS Devices

Impact

An attacker can exercise complete control over the device. By exploiting this vulnerability, the attacker can see and change the configuration of the device.

Suggested Fix

The workaround for this vulnerability is to disable HTTP server on the router or to use TACACS+ or Radius for authentication.

HTTP Command Injection - 68322 [IOS]

Description

A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

See "IOS HTTP Server Command Injection Vulnerability." at Cisco Security Advisories website

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices (68322 of 1.1)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Rule 1

Rule
PSIRT- 68322: Verify HTTP Server Command Injection Vulnerability [IOS]

Description
A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks.

See "IOS HTTP Server Command Injection Vulnerability." at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability may result in an attacker executing commands on the device, including the possibility of gaining full administrative privileges on the device which is dependent on the privilege level of the authenticated user.

Suggested Fix
If the HTTP server is not used for any legitimate purposes on the device, it is a best practice to disable it by issuing the following commands in configure mode:

```shell
no ip http server no ip http secure-server
```

HTTP GET Vulnerability - 44162 [IOS]

Description
A vulnerability has been reported by an external researcher in Cisco IOS® release for Cisco Aironet AP1x00 Series Wireless devices. The vulnerability affects only IOS-based Cisco Aironet Wireless products. The VxWorks based Cisco Aironet Wireless Devices are not affected. This vulnerability can cause the AP1x00 to reload.

See "HTTP GET Vulnerability in AP1x00." at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(44162 of 1.1)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT- 44162: Verify HTTP GET Vulnerability in AP1x00 Vulnerability[IOS]
Understanding Compliance and Audit Manager (CAAM) Policies

**Description**

Sending a malformed URL to the Cisco Aironet AP1x00 can cause the device to reload.

**Applicable Platforms**

Cisco IOS Devices

**Impact**

This causes device reload. Repeated exploitation of this vulnerability can lead to a prolonged Denial-of-Service (DoS) of the AP1x00.

**Suggested Fix**

There are two workarounds for this vulnerability. One is to use `access-class` or `access-list` commands to limit the access to legitimate hosts only, and another workaround is to disable HTTP and use SSH to administer the Cisco Aironet Access Point.

**HTTP Server Query - 13628 [IOS]**

**Description**

A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled, browsing to "http://router-ip/anytext?/" is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

This vulnerability can only be exploited if the enable password is known or not set. See "Cisco IOS HTTP Server Query Vulnerability." at Cisco Security Advisories website.

**Applicable Platforms**

Cisco IOS Devices

**References**

CISCO PSIRT Advisories and Notices(13628 of 1.6)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PSIRT- 13628: Verify HTTP Server Query Vulnerability [IOS]

**Description**

The HTTP server was introduced in IOS release 11.0 to extend router management to the worldwide Web. The "?" (question mark) character is defined in the HTML specifications as a delimiter for CGI arguments. It is also interpreted by the IOS command-line interface as a request for help.

As of Cisco IOS Software Release 12.0T, the meaning of a question mark when it appears adjacent to a "/" (slash) character cannot be determined properly by the URI parser in affected versions of Cisco IOS software. When a URI containing "!/" is presented to the HTTP service on the router and a valid enable password is supplied, the router enters an infinite loop. A watchdog timer expires two minutes later and forces the router to crash and reload. The router continues to be vulnerable to this defect as long as it is running an affected IOS software release and the enable password is known.
This vulnerability may only be exploited if the enable password is not set, it is well known, or it can be guessed.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
An affected Cisco IOS device that is operating with the HTTP service enabled and is not protected by having the enable password configured can be forced to halt for up to two minutes and then reload. The vulnerability can be exercised repeatedly, possibly creating a denial of service (DOS) attack, unless the service is disabled, the enable password is set, or the router is upgraded to a fixed release.

In instances in which a router at a remote location fails to reload, an administrator must visit the site to enable the device to recover from the defect.

**Suggested Fix**
In lieu of an upgrade, the threat may be eliminated or reduced by taking any of the following measures:

- Select and configure strong enable passwords on networking devices.
- Disable the HTTP server using the command `no ip http server` while in global configuration mode.
- If the HTTP server must remain enabled while unrepaired, network access to it can be controlled by applying a standard access list to the HTTP service itself.

---

**Hard-Coded SNMP Community Names in Cisco Industrial Ethernet 3000 Series Switches Vulnerability- 111895 [IOS]**

**Description**
Cisco Industrial Ethernet 3000 (IE 3000) Series switches running Cisco IOSi;½ Software releases 12.2(52)SE or 12.2(52)SE1, contain a vulnerability where well known SNMP community names are hard-coded for both read and write access. The hard-coded community names are “public” and “private.”

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices(111895 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT- 111895: Hard-Coded SNMP Community Names in Cisco Industrial Ethernet 3000 Series Switches Vulnerability [IOS]
Description
Cisco Industrial Ethernet 3000 Series switches that are running affected versions of Cisco IOS Software contain hard-coded SNMP read-write community names.

The Cisco Industrial Ethernet 3000 Series is a family of switches that provide a rugged, easy-to-use, secure infrastructure for harsh environments.

SNMP is used for managing and monitoring the device and community names are the equivalent to a password.

The hard-coded SNMP community names are:

- `snmp-server community public RO`
- `snmp-server community private RW`

The SNMP community names can be removed; however, the hard-coded community names are reapplied to the running configuration when the device reloads. Cisco has provided a workaround that ensures the community names are removed when the device reloads.

Note
Configuring an access list or a restricted mib view:

```
snmp-server community public RO 99
snmp-server community private RW 99
snmp-server community public view <mib> RO 99
snmp-server community private view <mib> RO 99
access-list 99 deny any
```

The proceeding works as a workaround until the device is reloaded. Once the device is reloaded the original configuration is inserted without the access lists or mib views assigned to the community names. Consult the workarounds section of this advisory.

This vulnerability was introduced as part of a new feature integrated into the affected releases called PROFINET. At the time of the publication of this advisory, PROFINET was only supported on Cisco Industrial Ethernet 3000 Series switches.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability could result in an attacker obtaining full control of the device

Suggested Fix
Manually Remove SNMP Community Names

Note
The following workaround is only effective until the device is reloaded. Upon each reload of the device this workaround must be re-applied. Cisco encourages performing a Cisco IOS Software upgrade as a permanent fix for this vulnerability.
Log in to the device, and enter configuration mode. Enter the following configuration commands:

```plaintext
no snmp-server community public RO
no snmp-server community private RW
```

Saving the configuration will update the start-up configuration files; however the hard-coded community names will be reinserted to the running configuration when the device reloads. This workaround must be applied each time the device is reloaded.

### Automatically Remove SNMP Community Names

By creating an Embedded Event Manager (EEM) policy, it is possible to automatically remove the hard-coded SNMP community names each time the device is reloaded. The following example shows an EEM policy that runs each time the device is reloaded and removes the hard-coded SNMP community names.

```plaintext
event manager applet cisco-sa-20100707-snmp
event timer countdown time 30
action 10 cli command "enable"
action 20 cli command "configure terminal"
action 30 cli command "no snmp-server community public RO"
action 40 cli command "no snmp-server community private RW"
action 50 cli command "end"
action 60 cli command "disable"
action 70 syslog msg "Hard-coded SNMP community names as per Cisco Security Advisory cisco-sa-20100707-snmp removed"
```

For more information on EEM policies consult the Cisco IOS Network Management Configuration Guide - Embedded Event Manager Overview at the following link:


### Infrastructure Access Control Lists

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the device interface or the border of networks.

If SNMP management is not required on the IE3000, then dropping all SNMP traffic to the device is a sufficient workaround. The iACL below shows an example of an IE3000 with two interfaces configured with layer 3 access, dropping all SNMP queries destined to the IE3000:

```plaintext
!---
!--- Deny SNMP traffic from all other sources destined to
!--- configured IP addresses on the IE3000.
!---
access-list 150 deny udp any host 192.168.0.1 eq snmp
access-list 150 deny udp any host 192.168.1.1 eq snmp
```
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

!---
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and configurations
!--- Permit all other traffic to transit the device.
!---

access-list 150 permit ip any any

!---
!--- Apply access-list to all Layer 3 interfaces
!--- (only two examples shown)
!---

interface Vlan1
ip address 192.168.0.1 255.255.255.0
ip access-group 150 in

interface GigabitEthernet1/1
ip address 192.168.1.1 255.255.255.0
ip access-group 150 in

The white paper "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

IKE Resource Exhaustion Vulnerability - 110559  [IOS]

Description
Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions.

Cisco has released free software updates that address this vulnerability.

Applicable Platforms
Cisco IOS Devices
Rule 1

Rule
PSIRT- 110559: Verify IKE Resource Exhaustion Vulnerability [IOS]

Description
A vulnerability exists in the IKE implementation of Cisco IOS Software, if the certificate based authentication method is used. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 SAs, which may prevent new IPSec sessions from being established.

Administrators can view Phase 1 SAs that are allocated as a result of exploitation by issuing the show crypto isakmp sa command. The following example displays sample output for this command:

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA

dst                     src                   state                               conn-id slot status
10.48.66.77     10.48.66.6      MM_KEY_EXCH       1004 ACTIVE
10.48.66.77     10.48.66.6      MM_KEY_EXCH       1003 ACTIVE
10.48.66.77     10.48.66.6      MM_KEY_EXCH       1002 ACTIVE
....
```

Any allocated SA can be de-allocated up manually by using the clear crypto isakmp <conn-ID> command.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 SAs, which may prevent new IPSec sessions from being established.

Suggested Fix
If RSA keys are not needed on the system, the crypto key zeroize rsa command can be used to delete all RSA keys from your system. Note that this will break all features that are using RSA keys, including the Secure Shell (SSH).

Additional mitigations that can be deployed on Cisco devices in the network are available in the Cisco Applied Mitigation Bulletin companion document.
IKE Xauth - 64424 [IOS]

Description
Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

See "Vulnerabilities in the Internet Key Exchange Xauth Implementation" at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(64424 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT- 64424: Verify Vulnerabilities in the IKE Xauth Implementation [IOS]

Description
Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

See "Vulnerabilities in the Internet Key Exchange Xauth Implementation" at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation may result in the affected device allowing an unauthorized user to complete authentication and access network resources.

Suggested Fix
Because the preshared group password (also referred to as the group key) must be known by an attacker, the use of a best practice to deploy strong preshared group keys may mitigate a brute-force attack against this group key.
IPS ATOMIC.TCP Signature Vulnerability - 81545 [IOS]

Description
The Intrusion Prevention System (IPS) feature set of Cisco IOS contains several vulnerabilities. These include:

- Fragmented IP packets may be used to evade signature inspection.
- IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(81545 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT- 81545: Verify IPS ATOMIC.TCP Signature Vulnerability [IOS]

Description
Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based feature that enables Cisco IOS software to mitigate network attacks. Cisco IOS IPS enables the network to defend itself with the intelligence to identify, classify, and stop or block certain malicious or damaging traffic in real time. The IOS IPS feature set contains multiple vulnerabilities. Only IOS images containing the IPS feature set are affected by these vulnerabilities.

ATOMIC.TCP Regular Expression Denial of Service Vulnerability
Certain network traffic can trigger IPS signatures which use the regular expression feature of the ATOMIC.TCP signature engine which may cause the IOS IPS device to crash. This may cause a denial of service resulting in disruption network traffic. Signature 3123.0 (Netbus Pro Traffic) has been demonstrated to trigger this vulnerability. There is a workaround for this vulnerability.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the ATOMIC.TCP regular expression denial of service vulnerability may cause an IOS IPS device to crash.

Suggested Fix
There is a workaround for the ATOMIC.TCP regular expression denial of service vulnerability by deleting IPS signature 3123.0 from the IOS IPS Signature Definition File (SDF). Disabling signature 3123.0 is alone not sufficient for the workaround to be effective. The following commands will delete signature 3123.0 from an IOS IPS device.
router#configure terminal
router(config)#ip ips signature 3123 delete

%IPS Signature 3123:0 is marked for deletion
%IPS The signature will be deleted when signatures are reloaded or saved
router(config)#interface FastEthernet0/0
router(config)#no ip ips test in
router(config)#ip ips test in
router(config)#exit

In the above example, signature 3123.0 is first deleted from the Signature Definition File, then the IPS instance running on interface FastEthernet0/0 is stopped and started to reinitialize the IPS state to reflect the signature deletion. If the IPS feature set is configured on multiple interfaces, then these steps must be completed for each affected interface.

To determine if signature 3123 is active, use the `show ip ips signature` command.

```
router#show ip ips signatures | include 3123
3123:0 N A MED 0 0 0 100 30 FA N S46
```

In the command output above, the N after 3123.0 indicates that the signature is present in the configuration but not enabled. Once the signature has been deleted, rerunning the `show ip ips signature` command shows:

```
router#show ip ips signatures | include 3123
3123:0 N* A MED 0 0 0 100 30 FA N S46
```

In the command output above, the N* after 3123.0 indicates that the signature has been deleted from the configuration. The IPS feature set must be restarted on each interface configured for IPS to complete the workaround. Once completed, the output of the `show ip ips signature` command will show:

```
router#show ip ips signatures | include 3123
```

```
router#
```

This vulnerability may affect any IPS signature using the regular expression functionality of the ATOMIC.TCP engine. Currently, Cisco only ships one signature configured this way (3123.0). If custom signatures have been added to an IOS IPS device configured use the ATOMIC.TCP engine with a regular expression, these signatures must also be deleted from the IPS configuration to ensure the effectiveness of the workaround.

### IPS DoS Vulnerability - 107583 [IOS]

**Description**

The Cisco IOS Intrusion Prevention System (IPS) feature contains a vulnerability in the processing of certain IPS signatures that use the SERVICE.DNS engine. This vulnerability may cause a router to crash or hang, resulting in a denial of service condition.

Cisco has released free software updates that address this vulnerability. There is a workaround for this vulnerability.
Note
This vulnerability is not related in any way to CVE-2008-1447 - Cache poisoning attacks.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(107583 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT- 107583: Verify IPS DoS Vulnerability [IOS]

Description
Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection feature that effectively mitigates a wide range of network attacks. A component of the Cisco IOS Integrated Threat Control framework and complemented by Cisco IOS Flexible Packet Matching feature, Cisco IOS IPS provides your network with the intelligence to accurately identify, classify, and stop or block malicious traffic in real time. Additional information on the Cisco IOS IPS feature can be found at http://www.cisco.com/en/US/docs/ios/redirect/eol.html

Previous to the introduction of the Cisco IOS IPS feature, Cisco IOS provided a similar feature, the Cisco IOS Intrusion Detection System (IDS). The Cisco IOS IDS feature is not affected by this vulnerability. Additional information on the Cisco IOS IDS feature can be found at http://www.cisco.com/en/US/docs/ios/redirect/eol.html

Certain network traffic can trigger IPS signatures on the SERVICE.DNS signature engine which may cause the Cisco IOS device to crash or hang. This may cause a denial of service that results in disruption of network traffic.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of this vulnerability may cause a Cisco IOS device configured with the Cisco IOS IPS feature to crash or hang, resulting in a denial of service condition.

Suggested Fix
The workaround consists of adding an Access Control List (ACL) to every Cisco IOS IPS policy configured on the device so that traffic destined to ports 53/udp or 53/tcp is not inspected by the Cisco IOS IPS feature. The following ACL would need to be added to the device configuration:

! deny inspection of traffic with a destination port of 53/udp
access-list 177 deny  udp any any eq 53

! deny inspection of traffic with a destination port of 53/tcp
access-list 177 deny  tcp any any eq 53
! allow all other traffic to be inspected
access-list 177 permit ip any any

Every instance of a Cisco IOS IPS policy on the device would then need to be modified in order to reference the previous ACL. In order to determine which Cisco IOS IPS policies are configured on the device, execute the command show running-config | include ip ips name as in the following example:

Router#show running-config | include ip ips name
ip ips name ios-ips-incoming
ip ips name ios-ips-outgoing
Router#

In the previous example, two Cisco IOS IPS policies are configured on the device. The following example shows the addition of an ACL to each one of the Cisco IOS IPS policies previously identified:

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip ips name ios-ips-incoming list 177
Router(config)#ip ips name ios-ips-outgoing list 177
Router(config)#end
Router#

As a verification step, the command show ip ips interfaces can be executed again to verify the ACL has been properly attached to each one of the Cisco IOS IPS policies:

Router#show ip ips interfaces
  Interface Configuration
    Interface FastEthernet0/0
      Inbound IPS rule is ios-ips-incoming
      acl list 177
      Outgoing IPS rule is not set
**Understanding Compliance and Audit Manager (CAAM) Policies**

**Interface FastEthernet0/1**

*Inbound IPS rule is not set*

*Outgoing IPS rule is ios-ips-outgoing*

`acl list 177`

`Router#`

---

**Note**

Disabling or deleting individual or all signatures using the SERVICE.DNS engine of the Cisco IOS IPS feature is not a recommended workaround. The previous workaround is the only Cisco-recommended workaround for this vulnerability.

---

**IPS Fragmented Packet Vulnerability - 81545 [IOS]**

**Description**

The Intrusion Prevention System (IPS) feature set of Cisco IOS contains several vulnerabilities. These include:

- Fragmented IP packets may be used to evade signature inspection.
- IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

**Applicable Platforms**

Cisco IOS Devices

**References**

CISCO PSIRT Advisories and Notices (81545 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PSIRT- 81545: Verify IPS Fragmented Packet Vulnerability [IOS]

**Description**

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based feature that enables Cisco IOS software to mitigate network attacks. Cisco IOS IPS enables the network to defend itself with the intelligence to identify, classify, and stop or block certain malicious or damaging traffic in real time. The IOS IPS feature set contains multiple vulnerabilities. Only IOS images containing the IPS feature set are affected by these vulnerabilities.
Fragmented Packet Evasion Vulnerability

Some of the IPS signatures utilize regular expressions. Due to a vulnerability, an attacker can evade those IPS signatures by sending malicious network traffic as IP fragments. This may result in potential malicious traffic bypassing signature inspection and possibly allow the exploitation of protected systems. IPS signatures which do not utilize regular expressions are not affected by this vulnerability. All IP protocols (e.g. TCP, UDP, ICMP) are affected by this vulnerability. There is a mitigation for this vulnerability.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the fragmented packet evasion vulnerability may result in an attacker being able to evade detection by an IOS IPS device. This could allow protected systems to be covertly attacked.

Suggested Fix
There is a mitigation for the fragmented packet evasion vulnerability. The fragments keyword of IOS transit Access Control Lists (ACL) can be used to prohibit fragmented IP packets from transiting an IOS device. More information about filtering IP fragments can be found here:


Blocking IP fragments may have adverse affects on some protocols (like HTTP, FTP and Kerberos/Active Directory), so this workaround should be used with caution.

```
access-list 100 deny tcp any 10.1.1.0 0.0.0.255 fragments
access-list 100 deny udp any 10.1.1.0 0.0.0.255 fragments
```

IPSec IKE Malformed Packet - 50430 [IOS]

Description
A malformed Internet Key Exchange (IKE) packet may cause the Cisco Catalyst 6500 Series Switch or the Cisco 7600 Series Internet Router to reload. Only devices running Cisco IOS software with Crypto support are affected.

See "Cisco IPSec Malformed IKE Packet Vulnerability" at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(50430 of 2.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT- 50430: Verify IPSec Malformed IKE Packet Vulnerability [IOS]
Description
A malformed Internet Key Exchange (IKE) packet may cause the Cisco Catalyst 6500 Series Switch or the Cisco 7600 Series Internet Router to reload. Only devices running Cisco IOS software with Crypto support are affected.
See "Cisco IPSec Malformed IKE Packet Vulnerability" at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of this vulnerability could result in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

Suggested Fix
Customers that do not require IPSec functionality on their devices can use the command 'no crypto isakmp enable' in configuration mode to disable processing of IPSec and eliminate their exposure. As a possible mitigation, access-lists could be applied on the affected IOS platforms to limit the source IP addresses permitted to establish IPSec sessions to the device.

IPsec Vulnerability- 111266  [IOS]

Description
A malformed Internet Key Exchange (IKE) packet may cause a device running Cisco IOS Software to reload. Only Cisco 7200 Series and Cisco 7301 routers running Cisco IOS software with a VPN Acceleration Module 2+ (VAM2+) installed are affected. Cisco has released free software updates that address this vulnerability.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(111266 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT- 111266: Verify IOS Software IPsec Vulnerability [IOS]

Description
IPsec is an IP security feature that provides robust authentication and encryption of IP packets. IKE is a key management protocol standard that is used with the IPsec standard. IKE is a hybrid protocol that implements the Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and SKEME are security protocols that are implemented by IKE.). More information on IKE is available at the following link:
A vulnerability exists in the Cisco IOS Software implementation of IKE where a malformed packet may cause a device running Cisco IOS Software to reload. Only Cisco 7200 Series and Cisco 7301 routers running Cisco IOS software with a VPN Acceleration Module 2+ (VAM2+) installed are affected.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
Successful exploitation of this vulnerability may cause the affected device to reload. Repeated exploitation will result in a denial of service (DoS) condition.

**Suggested Fix**
There are no workarounds available

---

**IPv4 - 44020 [IOS]**

**Description**
Cisco routers and switches running Cisco IOS® software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. Multiple IPv4 packets with specific protocol fields sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. Traffic passing through the device cannot block the input queue. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. Multiple valid workarounds are available in the form of best practices for situations where software upgrades are not currently feasible. See "Cisco IOS Interface Blocked by IPv4 Packets."at Cisco Security Advisories website for more information.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices(44020 of 1.15)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT- 44020: Verify Cisco IOS Interface Blocked by IPv4 Packets [IOS]

**Description**
Cisco routers and switches running Cisco IOS® software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. Multiple IPv4 packets with specific protocol fields sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. Traffic passing through the device cannot block the input queue. No
authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by
default. Devices running only IP version 6 (IPv6) are not affected. Multiple valid workarounds are
available in the form of best practices for situations where software upgrades are not currently feasible.
See "Cisco IOS Interface Blocked by IPv4 Packets." at Cisco Security Advisories website for more
information.

Applicable Platforms
Cisco IOS Devices

Impact
A device receiving these specifically crafted IPv4 packets will force the inbound interface to stop
processing traffic. The device may stop processing packets destined to the router, including routing
protocol packets and ARP packets. No alarms will be triggered, nor will the router reload to correct
itself. This issue can affect all Cisco devices running Cisco IOS software. This vulnerability may be
exercised repeatedly resulting in loss of availability until a workaround has been applied or the device
has been upgraded to a fixed version of code.

Suggested Fix
Cisco recommends that all IOS devices which process IPv4 packets be configured to block unwanted
traffic, or any traffic directed to the router from an unauthorized source with the use of Access Control
Lists (ACLs).

For devices with interfaces that are currently blocked due to exploitation of this vulnerability, ACL
workarounds may be applied. AFTER APPLYING THE WORKAROUND, the input queue depth may
be raised with the hold-queue in interface command to something larger than the default size of 75.
This will allow traffic flow on the interface. The device may then be reloaded at a convenient time to
release the blocked packets.

For interfaces blocked with PIM packets only, the PIM process may be enabled on the router after
applying a workaround which will clear protocol type 103 packets from the blocked input queue. This
does not clear packets with protocol type 53, 55, or 77 from the input queue.

IPv6 Crafted Packet - 65783 [IOS]

Description
Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) and
potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must
be sent from a local network segment. Only devices that have been explicitly configured to process IPv6
traffic are affected. Upon successful exploitation, the device may reload or be open to further
exploitation.

See "IPv6 Crafted Packet Vulnerability." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices
References
CISCO PSIRT Advisories and Notices(65783 of 1.8)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT- 65783: Verify IPv6 Crafted Packet Vulnerability [IOS]

Description
IPv6 is the "Internet Protocol Version 6", designed by the Internet Engineering Task Force (IETF) to replace the current version Internet Protocol, IP Version 4 (IPv4).

A vulnerability exists in the processing of IPv6 packets. Crafted packets from the local segment received on logical interfaces (that is, tunnels including 6to4 tunnels) as well as physical interfaces can trigger this vulnerability. Crafted packets can not traverse a 6to4 tunnel and attack a box across the tunnel.
The crafted packet must be sent from a local network segment to trigger the attack. This vulnerability can not be exploited one or more hops from the IOS device. See "IPv6 Crafted Packet Vulnerability." at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability on Cisco IOS may result in a reload of the device or execution of arbitrary code. Repeated exploitation could result in a sustained DoS attack or execution of arbitrary code on Cisco IOS devices.
Successful exploitation of the vulnerability on Cisco IOS-XR may result in a restart of the IPv6 neighbor discovery process. A restart of this process will only affect IPv6 traffic passing through the system. All other processes and traffic will be unaffected. Repeated exploitation could result in a sustained DoS attack on IPv6 traffic.

Suggested Fix
In networks where IPv6 is not needed but enabled, disabling IPv6 processing on an IOS device will eliminate exposure to this vulnerability. On a router which is configured for IPv6, this must be done by issuing the command no ipv6 enable and no ipv6 address on each interface.

IPv6 Routing Header - 72372 [IOS]

Description
Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.
Cisco has made free software available to address this vulnerability for affected customers.
There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.
This vulnerability was initially reported by a customer and further trigger vector was discovered during developing the fix for this vulnerability.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices (72372 of 1.2)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT- 72372: Verify IPv6 Routing Header Vulnerability [IOS]

**Description**
This vulnerability can be triggered only when Cisco IOS processes specifically crafted IPv6 Type 0 Routing headers, which are used for source routing. Source routing is when an originator node explicitly specifies the exact path that a packet must take to reach the destination. Source routing is enabled by default on Cisco IOS if IPv6 is configured on the device. In order to trigger this vulnerability the packet must be destined to any of the IPv6 addresses defined on the device. The exact packet type is not relevant (e.g., TCP, ICMP, UDP) as the vulnerability is on the IP layer. For this reason care must be taken when implementing a workaround as this vulnerability can be triggered by a spoofed packet.

IPv6 multicast packets can not be used to trigger this vulnerability.

In addition to Type 0 Routing headers, IPv6 also supports Type 2 Routing that is used in Mobile IPv6 implementation. Type 2 Routing headers can not be used to trigger the vulnerability described in this Advisory.

A router running vulnerable Cisco IOS software will process Type 0 Routing headers only if the destination address in the IPv6 packet is one of the IPv6 addresses defined on any of the interfaces. The address may be either a global (i.e., routable), loopback or link local address. Link local addresses are not supposed to be routable and they are valid only among directly connected devices.

A device may also be susceptible in scenarios where IPv6 packets are tunneled over IPv4 networks provided that the IPv6 destination address (after de-encapsulation) is one of the IPv6 addresses defined on the device. This is independent of the exact encapsulation method used (e.g., MPLS, GRE or IPv6-in-IPv4).

**Applicable Platforms**
Cisco IOS Devices

**Impact**
Successful exploitation of the vulnerability listed in this Advisory can corrupt some memory structures. In most cases this will cause the affected device to crash and repeated exploitation could result in a sustained DoS attack. However, due to memory corruption, there is a potential to execute an arbitrary code. In the event of a successful remote code execution, device integrity will have been completely compromised.
Suggested Fix
The workaround consists of filtering packets that contain Type 0 Routing header(s). Special attention must be paid not to filter packets with Type 2 Routing headers as that would break Mobile IPv6 deployment.

Information Leakage Using IPv6 Routing Header - 97848 [IOS]

Description
Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected IOS and IOS XR devices, and may also result in a crash of the affected IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(97848 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT- 97848: Verify Information Leakage Using IPv6 Routing Header [IOS]

Description
Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected IOS and IOS XR devices, and may also result in a crash of the affected IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability affects devices that are configured to use the IPv6 protocol and are running affected versions.

Successful exploitation of the vulnerability described in this document may result in swapping memory between the destination IPv6 address in the IPv6 packet header and 16 bytes from the packet buffer memory. Memory that can be accessed through this vulnerability can not be further than 1500 bytes from the packet header start.

Applicable Platforms
Cisco IOS Devices
Impact
Successful exploitation of this vulnerability may result in the swapping of memory between the destination IPv6 address field and packet buffer memory. This can lead to the leakage of data from the buffer memory in the form of an IPv6 destination address and, in a worst case scenario for devices running Cisco IOS, a complete crash of the IOS device.

Note
Given that the destination IPv6 address will contain the contents of a buffer memory, the packet may not get routed outside of the local network. Depending on the exact destination address the packet may get dropped by the next router or on the targeted router itself if it does not have route to the newly formed IPv6 address.

In the case of Cisco IOS XR, successful exploitation will not crash the whole device but only lead to a restart of the IPv6 subsystem. Successful repeated exploitation of this vulnerability may lead to a sustained denial of service (DoS) of all upper layer services that use IPv6 as the transport protocol but not the whole device.

Suggested Fix
The workaround consists of filtering packets that contain Type 0 Routing header(s). Special attention must be paid not to filter packets with Type 2 Routing headers as that would break a Mobile IPv6 deployment. Depending on which Cisco IOS software release is used, and if Mobile IPv6 is deployed, there are several potential workarounds. Because any packet type (TCP, UDP, ICMP) can be used to trigger this vulnerability, care must be taken when implementing a workaround to account for a spoofed IPv6 packet.

Inter Process Communication (IPC) Vulnerability - 107661 [IOS]

Description
Cisco 10000, uBR10012 and uBR7200 series devices use a User Datagram Protocol (UDP) based Inter-Process Communication (IPC) channel that is externally reachable. An attacker could exploit this vulnerability to cause a denial of service (DoS) condition on affected devices. No other platforms are affected.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (107661 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT- 107661: Verify Inter Process Communication (IPC) Vulnerability [IOS]
Description
Cisco 10000, uBR10012 and uBR7200 series devices use a UDP-based IPC channel. This channel uses addresses from the 127.0.0.0/8 range and UDP port 1975. Cisco 10000, uBR10012 and uBR7200 series devices that are running an affected version of Cisco IOS will process IPC messages that are sent to UDP port 1975 from outside of the device. This behavior may be exploited by an attacker to cause a reload of the device, linecards, or both, resulting in a DoS condition.

Filtering unauthorized traffic destined to 127.0.0.0/8 or UDP port 1975 will mitigate this vulnerability.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability may result in a reload of the device, linecards, or both, resulting in a DoS condition.

Suggested Fix
Workarounds consist of filtering packets that are sent to 127.0.0.0/8 range and UDP packets that are sent to port 1975.

Using Interface Access Control Lists
Access lists that filter UDP packets destined to port 1975 can be used to mitigate this vulnerability. UDP port 1975 is a registered port number that can be used by certain applications. However, filtering all packets that are destined to UDP port 1975 may cause some applications to malfunction. Therefore, access lists need to explicitly deny UDP 1975 packets that are sent to any router interface IP addresses and permit transit traffic. Such access lists need to be applied on all interfaces to be effective. Since the IPC channel uses addresses from the 127.0.0.0/8 range, it is also necessary to filter packets that are sourced from or destined to this range. An example is given below:

```
access-list 100 deny udp any host <router-interface 1> eq 1975
access-list 100 deny udp any host <router-interface 2> eq 1975
access-list 100 deny udp any host <router-interface ...> eq 1975
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip any 127.0.0.0 0.255.255.255
access-list 100 permit ip any any
```

```
interface Serial 0/0
   ip access-group 100 in
```

Using Control Plane Policing
Control Plane Policing (CoPP) can be used to block untrusted UDP port 1975 access to the affected device. Cisco IOS software releases 12.2BC and 12.2SCA support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to your network.

```
```

Note
CoPP is not supported on uBR10012 series devices.
Understanding Compliance and Audit Manager (CAAM) Policies

!-- Permit all UDP/1975 traffic so that it
!-- will be policed and dropped by the CoPP feature

! access-list 111 permit udp any any eq 1975
access-list 111 permit ip any 127.0.0.0 0.255.255.255
access-list 111 permit ip 127.0.0.0 0.255.255.255 any
!
!-- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and
!-- Layer 4 traffic in accordance with existing security policies
!-- and configurations for traffic that is authorized to be sent
!-- to infrastructure devices

!
!-- Create a Class-Map for traffic to be policed by the CoPP
!-- feature

! class-map match-all drop-IPC-class
  match access-group 111
!
!-- Create a Policy-Map that will be applied to the Control-Plane
!-- of the device

! policy-map drop-IPC-traffic
  class drop-IPC-class
    drop
!
!-- Apply the Policy-Map to the Control-Plane of the device

! control-plane
  service-policy input drop-IPC-traffic
!
In the above CoPP example, the access control list entries (ACEs) which match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function.

Please note that in the Cisco IOS 12.2S and 12.0S trains the policy-map syntax is different:

```
! policy-map drop-IPC-traffic class drop-IPC-class
   police 32000 1500 1500 conform-action drop exceed-action drop
!
```

**Using Infrastructure ACLs at Network Boundary**

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. iACLs are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example shown below should be included as part of the deployed infrastructure access-list which will protect all devices with IP addresses in the infrastructure IP address range:

```
!-- Note: IPC packets sent to UDP destination port 1975 must not
!-- be permitted from any trusted source as this traffic
!-- should only be sent and received internally by the
!-- affected device using an IP address allocated from the
!-- 127.0.0.0/8 prefix.
!
!-- IPC that traffic that is internally generated and sent
!-- and/or received by the affected device is not subjected
!-- to packet filtering by the applied iACL policy.
!
!-- Deny IPC (UDP port 1975) packets from all sources destined to
!-- all IP addresses configured on the affected device.
!
access-list 150 deny udp any host INTERFACE_ADDRESS#1 eq 1975
access-list 150 deny udp any host INTERFACE_ADDRESS#2 eq 1975
access-list 150 deny udp any host INTERFACE_ADDRESS#N eq 1975
!
!-- Deny all IP packets with a source or destination IP address
!-- from the 127.0.0.0/8 prefix.
!
access-list 150 deny ip 127.0.0.0 0.255.255.255 any
```
access-list 150 deny ip any 127.0.0.0 0.255.255.255
!

!-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations.
!

!-- Permit all other traffic to transit the device.
!

access-list 150 permit ip any any
!

!-- Apply iACL to interfaces in the ingress direction.
!

interface GigabitEthernet0/0
  ip access-group 150 in
!

**Note**

iACLs that filter UDP packets destined to port 1975 can be used to mitigate this vulnerability. However, UDP port 1975 is a registered port number that can be used by certain applications. Filtering all packets that are destined to UDP port 1975 may cause some applications to malfunction. Therefore, the iACL policy needs to explicitly deny UDP packets using a destination port of 1975 that are sent to any router interface IP addresses for affected devices, then permit and/or deny all other Layer 3 and Layer 4 traffic in accordance with existing security policies and configurations, and then permit all other traffic to transit the device. iACLs must be applied on all interfaces to be used effectively. Since the IPC channel uses addresses from the 127.0.0.0/8 range, it is also necessary to filter packets that are sourced from or destined to this range as provided in the preceding example.

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists.
Additional Mitigation Techniques

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.

Layer 2 Tunneling Protocol (L2TP) DoS Vulnerability - 107441

Description
A vulnerability exists in the Cisco IOS software implementation of Layer 2 Tunneling Protocol (L2TP), which affects limited Cisco IOS software releases. Several features enable the L2TP mgmt daemon process within Cisco IOS software, including but not limited to Layer 2 virtual private networks (L2VPN), Layer 2 Tunnel Protocol Version 3 (L2TPv3), Stack Group Bidding Protocol (SGBP) and Cisco Virtual Private Dial-Up Networks (VPDN). Once this process is enabled the device is vulnerable. This vulnerability will result in a reload of the device when processing a specially crafted L2TP packet.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(107441 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-107441: Verify Layer 2 Tunneling Protocol(L2TP) Dos Vulnerability [IOS]

Description
A device running affected 12.2 and 12.4 versions of Cisco IOS and that has the L2TP mgmt daemon process running will reload when processing a specially crafted L2TP packet.

Several features leverage the L2TP protocol and start the L2TP mgmt daemon within Cisco IOS. These features have been outlined in this advisory under the Vulnerable Products section.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability will result in a reload of the device. Repeated exploitation may result in an extended denial of service (DoS) condition.

Suggested Fix

Note
L2TP implementations will need to allow UDP 1701, from trusted addresses to infrastructure addresses. This does not provide for a full mitigation as the source addresses may be spoofed.

Note
L2TPv3 over IP only implementations need to deny all UDP 1701 from anywhere to the infrastructure addresses.
Infrastructure Access Control Lists Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure Access Control Lists (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for these specific vulnerabilities. The iACL example below should be included as part of the deployed infrastructure access-list which will protect all devices with IP addresses in the infrastructure IP address range:

```cnf
!--- Permit L2TP UDP 1701 packets from all trusted sources destined to infrastructure addresses.
!--- NOTE: This does not prevent spoofed attacks.
!--- To be a full mitigation, no trusted source addresses should be listed.
!--- Omit this line if using a L2TPv3 over IP implementation only.

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES MASK INFRASTRUCTURE_ADDRESSES MASK eq 1701

!--- Deny L2TP UDP 1701 packets from all sources destined to infrastructure addresses.
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 1701

!--- If using a L2TPv3 over IP implementation ensure to allow L2TPv3
access-list 150 permit 115 <source_ip_address and mask>
<destination_ip_address and mask>

!--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance with existing security policies and configurations
!--- Permit all other traffic to transit the device.
access-list 150 permit ip any any

!--- Apply access-list to all interfaces (only one example shown)
interface serial 2/0
ip access-group 150 in
```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:


Control Plane Policing Control Plane Policing (CoPP) can be used to block L2TP access to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP which will protect all devices with IP addresses in the infrastructure IP address range.
Understanding Compliance and Audit Manager (CAAM) Policies

!--- Deny all trusted source L2TP UDP traffic sent to all IP addresses!
!--- configured on all interfaces of the affected device so that it
!--- will not be policed by the CoPP feature.
!--- NOTE: This does not prevent spoofed attacks.
!--- To be a full mitigation, no trusted source
!--- addresses should be listed.
!--- Omit this line if using an L2TPv3 over IP implementation only.

access-list 111 deny udp TRUSTED_SOURCE_ADDRESSES MASK INFRASTRUCTURE_ADDRESSES MASK eq 1701

access-list 111 permit udp any INFRASTRUCTURE_ADDRESSES MASK eq 1701

access-list 111 deny 115 <source_ip_address and mask>
<destination_ip_address and mask>

access-list 111 deny 115 <source_ip_address and mask>
<destination_ip_address and mask>

--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
--- traffic in accordance with existing security policies and
--- configurations for traffic that is authorized to be sent
--- to infrastructure devices
--- Create a Class-Map for traffic to be policed by
--- the CoPP feature

class-map match-all drop-l2tp-class
match access-group 111

--- Create a Policy-Map that will be applied to the
--- Control-Plane of the device.

policy-map drop-l2tp-traffic
class drop-l2tp-class
drop

--- Apply the Policy-Map to the
--- Control-Plane of the device

control-plane

service-policy input drop-l2tp-traffic

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Please note that the policy-map syntax is different in the 12.2S and 12.0S Cisco IOS trains:
class drop-l2tp-class
police 32000 1500 1500 conform-action drop exceed-action drop

Additional information on the configuration and use of the CoPP feature is available at the following link: http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.

MPLS - 63846  [IOS]

Description
Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on interfaces where MPLS is not configured. A system that supports MPLS is vulnerable even if that system is not configured for MPLS.

See "Crafted Packet Causes Reload on Cisco Routers." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(63846 of 1.1)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 63846: Crafted packet causes reload on devices supporting MPLS. [IOS]

Description
Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on interfaces where MPLS is not configured. A system that supports MPLS is vulnerable even if that system is not configured for MPLS.

See "Crafted Packet Causes Reload on Cisco Routers." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of this vulnerability could result in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

Suggested Fix
Enabling MPLS Traffic Engineering (MPLS TE) globally can be used as a workaround to mitigate this vulnerability. Since MPLS requires Cisco Express Forwarding (CEF) in order to work, CEF needs to be enabled first in order to enable MPLS TE.
Using this workaround may affect the operation of your network and might cause problems. Therefore it is strongly recommended that you do a code upgrade if you are affected. It is not recommended that you use the workaround as a long term solution.

**MPLS Forwarding Infrastructure DoS Vulnerability - 107646**

**Description**
Cisco IOS Software Multi Protocol Label Switching (MPLS) Forwarding Infrastructure (MFI) is vulnerable to a Denial of Service (DoS) attack from specially crafted packets. Only the MFI is affected by this vulnerability. Older Label Forwarding Information Base (LFIB) implementation, which is replaced by MFI, is not affected.

Cisco has released free software updates that address this vulnerability.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices (107646 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT-107646: Verify MPLS Forwarding Infrastructure DoS Vulnerability [IOS]

**Description**
In newer versions of Cisco IOS software, a new packet forwarding infrastructure was introduced to improve scalability and performance. This forwarding infrastructure, called MFI, is transparent to the user. MFI manages MPLS data structures used for forwarding and replaces the older implementation, Label Forwarding Information Base (LFIB). Cisco IOS MFI implementation is vulnerable to a DoS attack from specially crafted packets that are handled in the software path, including transit packets that are handled in the software path. Such packets can be sent from the local segment to the interfaces that are configured for MPLS or via tunnel interfaces that are configured for MPLS. To target a remote system in an MPLS network, an attacker needs to have access to the MPLS network through an MPLS-enabled interface. MPLS packets are dropped on interfaces that are not configured for MPLS.

Devices that support MFI will have `mfi_ios` in the output of the `show subsys` command. Interfaces that are enabled for MPLS can be seen by the `show mpls interface` command.

More information on MFI can be found at the following link:

**Applicable Platforms**
Cisco IOS Devices
Impact
Successful exploitation of this vulnerability may result in the reload of the device, leading to a DoS condition.

Suggested Fix
MPLS is normally enabled on physical and logical interfaces that are shared with other MPLS-enabled devices. It can be disabled on interfaces where MPLS is not necessary and from which a potential attack can be launched. This action may help to limit the exposure of this vulnerability.

If it is not possible to disable MPLS on interfaces from which an attack can be launched, there are no workarounds to mitigate this vulnerability.

MPLS VPN May Leak Information Vulnerability - 107578

Description
Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

Workarounds are available to help mitigate this vulnerability.

This issue is triggered by a logic error when processing extended communities on the PE device.

This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(107578 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 107578: Verify MPLS VPN May Leak Information Vulnerability [IOS]

Description
MPLS VPNs allow for the creation of 'virtual networks' that customers can use to segregate traffic into multiple, isolated VPNs. Traffic within each MPLS VPN is kept separate from the others, thereby maintaining a virtual private network.

More information on MPLS and MPLS VPNs is available at the following link:

A bug exists when processing extended communities with MPLS VPNs. If extended communities are used, MPLS VPN may incorrectly use a corrupted route target (RT) to forward traffic. If this occurs, traffic can leak from one MPLS VPN to another.
This vulnerability exists whenever an affected PE device has a BGP session running in the MPLS VPN Virtual Routing and Forwarding (VRF). The following two examples of this scenario are the most common:

1. MPLS VPN configuration with BGP running inside the VRF between the PE and CE devices.
2. MPLS Inter-AS option A with BGP running between the Autonomous System Border Routers (ASBR).

The mitigation in the Workarounds section filters extended communities on a PE device, preventing them from being received by devices configured for MPLS VPN.

This vulnerability was introduced with Cisco bug ID CSCee83237. Cisco IOS images that do not include CSCee83237 are not vulnerable to this issue.

It is important to note that this condition cannot be triggered by an attacker and that the condition does not provide ways to determine the flow of traffic between VPNs.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
This vulnerability may cause traffic to be improperly routed between MPLS VPNs, which may lead to a breach of confidentiality.

**Suggested Fix**
Customers running versions of Cisco IOS that support filtering of extended communities can prevent the corruption of the route target (RT) by applying a BGP route-map that removes RT entries on inbound BGP sessions.

The following configuration example applied in the ipv4 address family of a PE device removes extended communities from the CE router:

```plaintext
router bgp <Local AS>
  address-family ipv4 vrf one
  neighbor <neighbor IP>
  remote-as <Remote AS>
  neighbor <neighbor IP>
  activate neighbor <neighbor IP>
  route-map FILTER in exit-address-family
  
  ip extcommunity-list 100 permit _RT.*_
  
  route-map FILTER permit 10
  set extcomm-list 100 delete

```

The following configuration example applied in the ipv6 address family of a PE device removes extended communities from the CE router:

```plaintext
router bgp <Local AS>
```
address-family ipv6 vrf one
neighbor <neighbor IP>
remote-as <Remote AS>
neighbor <neighbor IP>
activate neighbor <neighbor IP>
route-map FILTER in exit-address-family
!
ip extcommunity-list 100 permit _RT.*_
!
!
route-map FILTER permit 10
set extcomm-list 100 delete!

Note The capability of filtering extended communities is only available in certain 12.0S and 12.2S based Cisco IOS releases.

BGP session between the PE and the CE needs to cleared to make this configuration change effective.

Mobile IP and IPv6 Vulnerabilities - 109487

Description
Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

Cisco has released free software updates that address these vulnerabilities.

Applicable Platforms
Cisco IOS Devices
References
CISCO PSIRT Advisories and Notices (109487 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 109487 Verify Mobile IP and IPv6 Vulnerabilities [IOS]

Description
Mobile IP is part of both IPv4 and IPv6 standards. Mobile IP allows a host device to be identified by a single IP address even though the device may move its physical point of attachment from one network to another. Regardless of movement between different networks, connectivity at the different points is achieved seamlessly without user intervention. Roaming from a wired network to a wireless or wide-area network is also possible.

More information on Mobile IPv6 can be found at the following link:

The Mobile IP Support NAT Traversal feature is documented in RFC 3519. It introduces an alternative method for tunneling Mobile IP data traffic. New extensions in the Mobile IP registration request and reply messages have been added for establishing User Datagram Protocol (UDP) tunneling. This feature allows mobile devices in collocated mode that use a private IP address (RFC 1918) or foreign agents (FAs) that use a private IP address for the care-of address (CoA) to establish a tunnel and traverse a NAT-enabled router with mobile node (MN) data traffic from the home agent (HA).

More information on Mobile IP NAT Traversal feature can be found at the following link:

Devices that are running an affected version of Cisco IOS Software and configured for Mobile IPv6 or Mobile IP NAT Traversal feature are affected by a DoS vulnerability. A successful exploitation of this vulnerability could cause an interface to stop processing traffic until the system is restarted. Offending packets need to be destined to the router for a successful exploit.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability may result in an interface to stop processing traffic, causing a DoS condition.

Suggested Fix
The following mitigation and identification methods have been identified for these vulnerabilities:
Infrastructure Access Control Lists

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure Access Control Lists (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for these specific vulnerabilities. The iACL example below should be included as part of the deployed infrastructure access-list which will protect all devices with IP addresses in the infrastructure IP address range:
IPv4 example:
!--- Anti-spoofing entries are shown here.
!--- Deny special-use address sources.
!--- Refer to RFC 3330 for additional special use addresses.

access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any
access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any

!--- Filter RFC 1918 space.

access-list 110 deny ip 10.0.0.0 0.255.255.255 any
access-list 110 deny ip 172.16.0.0 0.15.255.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any

!--- Deny your space as source from entering your AS.
!--- Deploy only at the AS edge.

access-list 110 deny ip YOUR_CIDR_BLOCK any

!--- Permit BGP.

access-list 110 permit tcp host bgp_peer host router_ip eq bgp
access-list 110 permit tcp host bgp_peer eq bgp host router_ip

!--- Deny access to internal infrastructure addresses.

access-list 110 deny ip any INTERNAL_INFRASTRUCTURE_ADDRESSES
!--- Permit transit traffic.

access-list 110 permit ip any any

IPv6 example:

!--- Configure the access-list.

ipv6 access-list iacl

!--- Deny your space as source from entering your AS.
!--- Deploy only at the AS edge.
deny ipv6 YOUR_CIDR_BLOCK_IPV6 any

!--- Permit multiprotocol BGP.

permit tcp host bgp_peer_ipv6 host router_ipv6 eq bgp
permit tcp host bgp_peer_ipv6 eq bgp host router_ipv6

!--- Deny access to internal infrastructure addresses.

deny ipv6 any INTERNAL_INFRASTRUCTURE_ADDRESSES_IPV6

!--- Permit transit traffic.

permit ipv6 any any

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Cisco IOS Embedded Event Manager

It is possible to detect blocked interface queues with a Cisco IOS Embedded Event Manager (EEM) policy. EEM provides event detection and reaction capabilities on a Cisco IOS device. EEM can alert administrators of blocked interfaces with email, a syslog message, or a Simple Network Management Protocol (SNMP) trap.

A sample EEM policy that uses syslog to alert administrators of blocked interfaces is available at Cisco Beyond, an online community dedicated to EEM. A sample script is available at the following link: https://supportforums.cisco.com/community/netpro/network-infrastructure/eem

More information about EEM is available from Cisco.com at the following link: http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.

Multicast Virtual Private Network (MVPN) Date Leak - 100374 [IOS]

Description
A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

Applicable Platforms
Cisco IOS Devices
References
CISCO PSIRT Advisories and Notices(100374 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability

Rule 1

Rule
PSIRT -100374: Verify Virtual MVPN Data Leak Vulnerability [IOS]

Description
Devices that run Cisco IOS and are configured for MVPN are affected.
An IOS device that is configured for MVPN has a line that is similar to this in the running configuration example:
mdt default <group-address>
A vulnerability exists in the implementation of MVPN that allows an attacker to send specially crafted Multicast Distribution Tree (MDT) Data Join messages that can cause the creation of extra multicast states on the core routers. MDT Data Join messages can be sent in unicast or multicast. The vulnerability can also allow leaking multicast traffic from different MPLS VPNs. It is possible to receive multicast traffic from VPNs that are not connected to the same Provider Edge (PE) router. In order to successfully exploit this vulnerability, an attacker needs to know or guess the Border Gateway Protocol (BGP) peering IP address of a remote PE router and the address of the multicast group that is used in other MPLS VPNs.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability can result in the creation of extra multicast states on the core routers or the leaking of multicast traffic from one MPLS VPN to another.

Suggested Fix
The workaround for this vulnerability consists of filtering MDT Data Join packets on the PE device.
The workarounds need to be applied on all Virtual Routing and Forwarding (VRF) interfaces of all PE routers. Otherwise, attackers can target remote PE routers and can still exploit this vulnerability.
Even if only one PE router in the network runs an unfixed version of IOS code, it is vulnerable to packets that come from systems that are connected to remote PE routers. In such a case, workarounds need to be deployed on all PE routers to successfully mitigate this vulnerability.
The mdt data <group> <mask> or mdt data <group> <mask> threshold <n> list <acl> commands do not mitigate this vulnerability.
Multiple Crafted IPv6 Packets - 63844

Description
Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

See "Multiple Crafted IPv6 Packets Cause Reload." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(63844 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-63844: Verify Multiple Crafted IPv6 Packets Cause Reload. [IOS]

Description
IPv6 is the "Internet Protocol Version 6", designed by the Internet Engineering Task Force (IETF) to replace the current version Internet Protocol, IP Version 4 (IPv4).

A vulnerability exists in the processing of IPv6 packets that can be exploited to cause the reload of a system. Crafted packets received on logical interfaces (that is, tunnels including 6to4 tunnels) as well as physical interfaces can trigger this vulnerability.

Multiple crafted IPv6 packets need to be sent to exploit this vulnerability. Such crafted packets can be sent remotely.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of this vulnerability results in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

Suggested Fix
In networks where IPv6 is not needed but enabled, disabling IPv6 processing on an IOS device will eliminate exposure to this vulnerability. On a router which is configured for IPv6, this must be done by issuing the command no ipv6 enable and no ipv6 address on each interface.
Multiple DNS Cache Poisoning Attacks - 107064 [IOS]

Description
Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

Cisco has released free software updates that address these vulnerabilities.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(107064 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-107064: Verify Multiple DNS Cache Poisoning Attacks Vulnerability [IOS]

Description
A device that is running Cisco IOS Software will be affected if it is running a vulnerable version and if it is acting as a DNS server.

All Cisco IOS Software releases that support the DNS server functionality and that have not had their DNS implementation improved are affected.

A device that is running Cisco IOS Software is configured to act as a DNS server if the command `ip dns server` is present in the configuration. This command is not enabled by default.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability described in this document may result in invalid hostname-to-IP address mappings in the cache of an affected DNS server. This may lead users of this DNS server to contact the wrong provider of network services. The ultimate impact varies greatly, ranging from a simple denial of service (for example, making www.example.com resolve to 127.0.0.1) to phishing and financial fraud.

Suggested Fix
Disable DNS server using the command

`no ip dns server`

Multiple Features Crafted TCP Sequence Vulnerability - 109337

Description
Cisco IOS Software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.
Cisco has released free software updates that address this vulnerability.
Several mitigation strategies are outlined in the workarounds section of this advisory.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(109337 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 109337: Verify Crafted TCP Sequence Vulnerability [IOS]

Description
Devices running affected versions of Cisco IOS Software and Cisco IOS XE Software are affected when configured to use any of the following features within Cisco IOS:
• Airline Product Set (ALPS)
• Serial Tunnel Code (STUN) and Block Serial Tunnel Code (BSTUN)
• Native Client Interface Architecture support (NCIA)
• Data-link switching (DLSw)
• Remote Source-Route Bridging (RSRB)
• Point to Point Tunneling Protocol (PPTP)
• X.25 for Record Boundary Preservation (RBP)
• X.25 over TCP (XOT)
• X.25 Routing
Information on how to determine whether an affected feature is enabled on a device are provided in the Details section of this advisory.

Applicable Platforms
Cisco IOS Devices
Impact
Successful exploitation of this vulnerability will cause the device to reload. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition.

Suggested Fix
The following mitigations have been identified for this vulnerability, which may help protect an infrastructure until an upgrade to a fixed version of Cisco IOS software can be scheduled:

Infrastructure Access Control Lists
Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure Access Control Lists (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for these specific vulnerabilities.

Receive ACLs (rACL)
For distributed platforms, Receive ACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the 12000 (GSR), 12.0(24)S for the 7500, and 12.0(31)S for the 10720. The Receive ACL protects the device from harmful traffic before the traffic can impact the route processor. Receive ACLs are designed to only protect the device on which it is configured. On the 12000, 7500, and 10720, transit traffic is never affected by a receive ACL. Because of this, the destination IP address "any" used in the example ACL entries below only refer to the router's own physical or virtual IP addresses. Receive ACLs are considered a network security best practice, and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml.

Control Plane Policing
Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations.

Additional mitigations that can be deployed on Cisco devices within the network are available in the "Cisco Applied Mitigation Bulletin" companion document.

Multiple Features IP Sockets Vulnerability - 109333 [IOS]

Description
A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS Software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

- The configured feature may stop accepting new connections or sessions.
- The memory of the device may be consumed.
- The device may experience prolonged high CPU utilization.
- The device may reload.

Cisco has released free software updates that address this vulnerability.
Several mitigation strategies are outlined in the "Workarounds" section of this advisory.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices(109333 of 1.1)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT- 109333: Verify Multiple Features IP Sockets Vulnerability  [IOS]

**Description**
Devices that are running affected versions of Cisco IOS Software and Cisco IOS XE Software are affected if they are running any of the following features. Details about confirming whether the affected feature is enabled on a device are in the "Details" section of this advisory.

- Cisco Unified Communications Manager Express
- SIP Gateway Signaling Support Over Transport Layer Security (TLS) Transport
- Secure Signaling and Media Encryption
- Blocks Extensible Exchange Protocol (BEEP)
- Network Admission Control HTTP Authentication Proxy
- Per-user URL Redirect for EAPoUDP, Dot1x, and MAC Authentication Bypass
- Distributed Director with HTTP Redirects
- DNS (TCP mode only)

**Applicable Platforms**
Cisco IOS Devices

**Impact**
Successful exploitation of the vulnerability may result in the any of the following occurring:

- The configured feature may stop accepting new connections or sessions.
- The memory of the device may be consumed.
- The device may experience prolonged high CPU utilization.
- The device may reload.

Repeated attempts to exploit this vulnerability could result in a sustained DoS condition.
Suggested Fix

The following mitigations have been identified for this vulnerability:

Infrastructure Access Control Lists

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure Access Control Lists (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for these specific vulnerabilities.

Receive ACLs (rACL)

For distributed platforms, Receive ACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the 12000 (GSR), 12.0(24)S for the 7500, and 12.0(31)S for the 10720. The Receive ACL protects the device from harmful traffic before the traffic can impact the route processor. Receive ACLs are designed to only protect the device on which it is configured. On the 12000, 7500, and 10720, transit traffic is never affected by a receive ACL. Because of this, the destination IP address "any" used in the example ACL entries below only refer to the router's own physical or virtual IP addresses. Receive ACLs are considered a network security best practice, and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The white paper entitled "GSR: Receive Access Control Lists" will help you identify and allow legitimate traffic to your device and deny all unwanted packets. This white paper is available at the following link http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml.

Control Plane Policing

Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations.

Additional mitigations that can be deployed on Cisco devices within the network are available in the "Cisco Applied Mitigation Bulletin" companion document.

Multiple Multicase Vulnerabilities - 107550

Description

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

Applicable Platforms

Cisco IOS Devices

References

CISCO PSIRT Advisories and Notices(107550 of 1.1)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Rule 1

Rule
PSIRT - 107550: Verify Multiple Multicast Vulnerabilities in Cisco IOS Software [IOS]

Description
Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS Software that may lead to a denial of service (DoS) condition. Devices that run Cisco IOS Software and are configured for PIM are affected by the first vulnerability. Only Cisco 12000 Series (GSR) routers that are configured for PIM are affected by the second vulnerability.

Available PIM modes on a Cisco IOS device are dense mode, sparse mode, or sparse-dense mode. The mode determines how the device populates its multicast routing table and how multicast packets are forwarded. PIM must be enabled in one of these modes for an interface to perform IP multicast routing.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation may cause a reload of the affected device. Repeated exploitation could result in a sustained denial of service (DoS) condition.

Suggested Fix
There are no workarounds for the second vulnerability. The following workarounds only apply to the vulnerability addressed in Cisco bug ID CSCsd95616. A PIM router must receive PIM Hellos to establish PIM neighborship. PIM neighborship is also the basis for designated router (DR) election, DR failover, and accepting/sending PIM Join/Prune/Assert messages. To specify trusted PIM neighbors, use the `ip pim neighbor-filter` command, as shown in the following example:

Router(config)#access-list 1 permit host 10.10.10.123
! -- An access control list is created to allow a trusted PIM neighbor
! -- in this example the neighbor is 10.10.10.123
!
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip pim neighbor-filter 1
! -- The PIM neighbor filter is then applied to the respective interface(s)

The `ip pim neighbor-filter` command filters PIM packets from untrusted devices including Hellos, Join/Prune, and BSR packets.

Note
The vulnerabilities described in this document can be exploited by spoofed IP packets if the attacker knows the IP address of the trusted PIM neighbors listed in the `ip pim neighbor-filter` implementation.

To protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators are advised to deploy ACLs to perform policy enforcement of traffic sent to core infrastructure equipment. PIM is IP protocol 103. As an additional workaround, administrators can explicitly permit only authorized PIM (IP protocol 103) traffic sent to infrastructure devices in accordance with existing security policies and configurations. An ACL can be deployed as shown in the following example:
ip access-list extended Infrastructure-ACL-Policy

!!-- When applicable, include explicit permit statements for trusted
!-- sources that require access on the vulnerable protocol
!-- PIM routers need to communicate with the rendezvous point (RP).
!-- In this example, 192.168.100.1 is the IP address of the
!-- rendezvous point, which is a trusted host that requires access
!-- to and from the affected PIM devices.
!

permit pim host 192.168.100.1 192.168.60.0 0.0.0.255
permit pim 192.168.60.0 0.0.0.255 host 192.168.100.1

!
!-- Permit PIM segment traffic, packets have destination of:
!-- 224.0.0.13 (PIMv2)
!-- 224.0.0.2  (Required only by legacy PIMv1)
!

permit pim 192.168.60.0 0.0.0.255 host 224.0.0.13
permit pim 192.168.60.0 0.0.0.255 host 224.0.0.2
!
!-- The following vulnerability-specific access control entries
!-- (ACEs) can aid in identification of attacks
!

deny pim any 192.168.60.0 0.0.0.255
!
!-- Explicit deny ACE for traffic sent to addresses configured within
!-- the infrastructure address space
!

deny ip any 192.168.60.0 0.0.0.255
!
!-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Apply iACL to interfaces in the ingress direction
interface GigabitEthernet0/0
ip access-group Infrastructure-ACL-Policy in

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.

Multiple SIP DoS Vulnerabilities - 107617

Description
Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(107617 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 107617: Verify Multiple CISCO SIP DoS Vulnerabilities [IOS]

Description
SIP is a popular signaling protocol used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination. Voice and video are the most popular types of sessions that SIP handles, but the protocol is flexible to accommodate for other applications that require call setup and termination. SIP call signaling can use UDP (port 5060), TCP (port 5060), or TLS (TCP port 5061) as the underlying transport protocol.

Multiple denial of service vulnerabilities exist in the SIP implementation in Cisco IOS. In all cases vulnerabilities can be triggered by processing valid SIP messages.

Applicable Platforms
Cisco IOS Devices
Impact
Successful exploitation of the vulnerabilities described in this document may result in a reload of the device. The issue could be repeatedly exploited to result in an extended Denial Of Service (DoS) condition.

Suggested Fix
If the affected Cisco IOS device needs to provide voice over IP services and therefore SIP cannot be disabled then none of the listed vulnerabilities have workarounds. Users are advised to apply mitigation techniques to limit exposure to the listed vulnerabilities. Mitigation consists of only allowing legitimate devices to connect to the routers. To increase effectiveness, the mitigation must be coupled with anti-spoofing measures on the network edge. This action is required because SIP can use UDP as the transport protocol.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.

Disable SIP Listening Ports
For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. Some versions of Cisco IOS allow administrators to accomplish this with the following commands:

```plaintext
sip-ua
no transport udp
no transport tcp
```

Warning
When applying this workaround to devices processing MGCP or H.323 calls, the device will not allow you to stop SIP processing while active calls are being processed. Under these circumstances, this workaround should be implemented during a maintenance window when active calls can be briefly stopped.

It is recommended that after applying this workaround, the `show` commands discussed in the Vulnerable Products section be used to confirm that the Cisco IOS device is no longer processing SIP messages.

Control Plane Policing
For devices that need to offer SIP services it is possible to use Control Plane Policing (CoPP) to block SIP traffic to the device from untrusted sources. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to your network:

```plaintext
!-- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.
!-- Everything else is not trusted. The following access list is used
!-- to determine what traffic needs to be dropped by a control plane
!-- policy (the CoPP feature.) If the access list matches (permit)
!-- then traffic will be dropped and if the access list does not
!-- match (deny) then traffic will be processed by the router.

access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060
```
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5061
access-list 100 deny udp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5061
access-list 100 permit udp any any eq 5060
access-list 100 permit tcp any any eq 5060
access-list 100 permit tcp any any eq 5061

!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices.

!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature.

class-map match-all drop-sip-class
  match access-group 100

!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.

policy-map drop-sip-traffic
  class drop-sip-class
    drop

!-- Apply the Policy-Map to the Control-Plane of the
!-- device.

control-plane
  service-policy input drop-sip-traffic

Warning Because SIP can utilize UDP as a transport protocol, it is possible to easily spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses.
In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Additional information on the configuration and use of the CoPP feature can be found at http://www.cisco.com/en/US/products/ps6642/products_white_paper0900aecd804fa16a.shtml and http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a008052446b.html.

Multiple SSH Vulnerabilities - 8118

Description
Four different Cisco product lines are susceptible to multiple vulnerabilities discovered in the Secure Shell (SSH) protocol version 1.5. These issues have been addressed, and fixes have been integrated into the Cisco products that support this protocol.

By exploiting the weakness in the SSH protocol, it is possible to insert arbitrary commands into an established SSH session, collect information that may help in brute force key recovery, or brute force a session key.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(8118 of 1.6)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 8118: Verify Multiple SSH Vulnerabilities [IOS]

Description
An implementation of SSH in multiple Cisco products are vulnerable to three different vulnerabilities. These vulnerabilities are:

• CRC-32 integrity check vulnerability -- This vulnerability has been described in a CORE SDI S.A. paper entitled "An attack on CRC-32 integrity checks of encrypted channels using CBC and CFB modes". In order for this attack to succeed, an attacker must possess one or two known ciphertext/plaintext pairs. This should not be difficult since every session starts with a greeting screen which is fixed and which can be determined. This also implies that an attacker must be somewhere along the session path in order to be able to sniff the session and collect corresponding ciphertext. While fixing this vulnerability, we have not made the implementation mistake described by VU#945216 (see http://www.kb.cert.org/vuls/id/945216) which is being actively exploited.
• Traffic analysis -- This issue has been described in an analysis jointly made by Dug Song and Solar Designer. It can be found at: http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt, and is entitled "Passive Analysis of SSH (Secure Shell) Traffic". To exploit this vulnerability, an attacker must be able to capture packets. When sending a packet using the SSH protocol, it is padded to the next 8-byte boundary, but the exact length of the data (without the padding) is sent unencrypted. The timing between packets may yield additional information, such as the relative position of a letter on the keyboard, but that depends on overall jitter in the network and the typing habits of the person. For additional information, please see http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt.

• Key recovery in SSH protocol 1.5 -- This has been discovered by CORE SDI S.A. and the paper describing it can be viewed at http://www.securityfocus.com/archive/1/161150. The subject line is "SSH protocol 1.5 session key recovery vulnerability". In order to exploit this vulnerability, an attacker must be able to sniff the SSH session and be able to establish a connection to the SSH server. In order to recover the server key, an attacker must perform an additional $2^{20} + 2^{19} = 1572864$ connections. Since the key has a lifespan of about an hour, this means that an attacker must perform around 400 connections per second. For further details, please see http://www.securityfocus.com/archive/1/161150.

Applicable Platforms
Cisco IOS Devices

Impact

• CRC-32 integrity check vulnerability -- By exploiting this protocol weakness, the attacker can insert arbitrary commands in the session after the session has been established.

• Traffic analysis -- This vulnerability exposes the exact lengths of the passwords used for login authentication. This is only applicable to an interactive session that is being established over the tunnel protected by SSH. This can significantly help an attacker in guessing the password using the brute force attack.

• Key recovery in SSH protocol 1.5 -- This vulnerability may lead to the compromise of the session key. Once the session key is determined, the attacker can proceed to decrypt the stored session using any implementation of the crypto algorithm used. This will reveal all information in an unencrypted form.

Suggested Fix
There are no workarounds for these vulnerabilities.

Multiprotocol Label Switching Packet Vulnerability - 111458

Description
A device running Cisco IOS1/2 Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service (DoS) condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

Cisco has released free software updates that address this vulnerability.
Workarounds that mitigate this vulnerability are available.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices (111458 of 1.1)

Security Advisories: For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices: For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT - 111458: Verify IOS Software Multiprotocol Label Switching Packet Vulnerability [IOS]

**Description**
MPLS LDP enables peer label switch routers (LSRs) in an MPLS network to exchange label binding information for supporting hop-by-hop forwarding in an MPLS network.

A vulnerability exists in Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software when processing a specially crafted LDP packet. For the device to be vulnerable, it has to be configured to process LDP hello messages, as explained within the Affected Products section of this advisory.

The crafted LDP packet, can be received as either a unicast or multicast UDP packet on port UDP 646 on any listening IP address of the device. Transit traffic will not trigger this vulnerability.

**Note**
Devices configured with TDP will also process the crafted LDP packet and are vulnerable.

For further information regarding MPLS and LDP please consult the "Multiprotocol Label Switching (MPLS) Introduction" home page available at this link:

**Applicable Platforms**
Cisco IOS Devices

**Impact**
Successful exploitation of this vulnerability on a device running a vulnerable version of Cisco IOS Software or Cisco IOS XE Software will cause the affected device to reload.

Exploitation on a router running a vulnerable version of Cisco IOS XR Software will result in a restart of the mpls_ldp process.

The issue could be repeatedly exploited to cause an extended DoS condition.
### Suggested Fix

Users are advised to apply mitigation techniques to help limit exposure to the vulnerability. Mitigation consists of allowing only legitimate devices to connect to the device. To increase effectiveness, the mitigation must be coupled with anti-spoofing measures on the network edge. This action is required because LDP will use UDP as the hello transport protocol.

If LDP is not required on the device, then MPLS forwarding can be disabled with the global configuration command `no mpls ip`.

---

### Note

LDP password or MD5 protection, does not protect against this vulnerability.

---

Transit traffic will not exploit this vulnerability. Only packets destined to the device may be used to exploit this vulnerability.

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco IOS Software Multiprotocol Label Switching Packet Vulnerability,"

**Infrastructure Access Control Lists**

---

**Warning**

Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should also be considered, to offer a comprehensive solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of the network. Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. This iACL example should be included as part of the deployed infrastructure access list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```plaintext
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD INFRASTRUCTURE_ADDRESSES WILDCARD eq 646
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 224.0.0.2 eq 646
```

Access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD infrastructures ADDRESSES WILDCARD eq 646

Access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 224.0.0.2 eq 646

---

Deny LDP traffic from all other sources destined to infrastructure addresses.

---
access-list 150 deny udp any
   INFRASTRUCTURE_ADDRESSES WILDCARD eq 646
!---
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations. Permit all other traffic to transit the
!--- device.
!---
access-list 150 permit ip any any
!---
!--- Apply access-list to all interfaces (only one example
!--- shown)
!---
interface fastEthernet 2/0
ip access-group 150 in

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists and is available at this link:

Control Plane Policing

⚠️ Warning  Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should also be considered, to offer a comprehensive solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS Software Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP policy, which will help protect all devices with IP addresses in the infrastructure IP address range.

!---
!--- Feature: Label Distribution Protocol (LDP)
!---
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES
   WILDCARD any eq 646
!---
!--- Deny LDP traffic from all other sources destined
!--- to the device control plane.
!---
access-list 150 permit udp any any eq 646
!---
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
!---
class-map match-all drop-ldp-class
  match access-group 150
!---
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!---
policy-map control-plane-policy
class drop-ldp-class
  drop
!---
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
!---
control-plane
  service-policy input control-plane-policy

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets
with the "permit" action result in these packets being discarded by the policy-map "drop" function, while
packets that match the "deny" action (not shown) are not affected by the policy-map drop function.
Please note that the policy-map syntax is different in the 12.2S and 12.0S Cisco IOS Software trains:

policy-map control-plane-policy
class drop-udp-class
  police 32000 1500 1500 conform-action drop exceed-action drop

Additional information on the configuration and use of the CoPP feature can be found in the documents,
"Control Plane Policing Implementation Best Practices" and "Cisco IOS Software Releases 12.2 S -
Control Plane Policing" at these links:
http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html and
Receive ACLs (rACL)

Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should also be considered, to offer a comprehensive solution.

For distributed platforms, Receive ACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the 12000 (GSR), 12.0(24)S for the 7500, and 12.0(31)S for the 10720. The Receive ACL protects the device from harmful traffic before the traffic can impact the route processor. Receive ACLs are designed to only protect the device on which it is configured. On the 12000, 7500, and 10720, transit traffic is never affected by a receive ACL. Because of this, the destination IP address "any" used in the example ACL entries below only refer to the router's own physical or virtual IP addresses. Receive ACLs are considered a network security best practice, and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The white paper entitled "GSR: Receive Access Control Lists" will help you identify and allow legitimate traffic to your device and deny all unwanted packets. This white paper is available at the following link http://www.cisco.com/en/US/docs/ios/redirect/eol.html.

This is the receive path ACL written to permit this type of traffic from trusted hosts:

```
!---
!--- Feature: Label Distribution Protocol (LDP)
!---

!---
!--- Permit LDP traffic from all trusted sources allowed
!--- to infrastructure addresses.
!---
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
 any eq 646
!---

!--- Deny LDP traffic from all other sources destined
!--- to infrastructure addresses.
!---
access-list 150 deny udp any any eq 646
!---

!--- Permit all other traffic to the RP.
!--- according to security policy and configurations.
!---
```
access-list 150 permit ip any any
!---
!--- Apply this access list to the 'receive' path.
!---
ip receive access-list 150

NAM (Network Analysis Module) Vulnerability - 81863

Description
Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Internetwork Operating System (IOS) or Catalyst Operating System (CatOS). Cisco has made free software available to address this vulnerability for affected customers.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(81863 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 81863: NAM Vulnerability [IOS]

Description
NAMs are deployed in Catalyst 6000, 6500 series and Cisco 7600 series to monitor and analyze network traffic by using Remote Monitoring (RMON), RMON2, and other MIBs. NAMs communicate with the Catalyst system by using the Simple Network Management Protocol (SNMP). By spoofing the SNMP communication between the Catalyst system and the NAM an attacker may obtain complete control of the Catalyst system.

Devices running both Cisco IOS and Cisco CatOS are affected by this vulnerability. This vulnerability is introduced in CatOS at 7.6(15) and 8.5(1). Older CatOS images are not vulnerable.

Applicable Platforms
Cisco IOS Devices

Impact
By successfully exploiting this vulnerability, an attacker may gain complete control of the device.

Suggested Fix
No workarounds exist for this vulnerability.
This vulnerability requires an attacker to spoof SNMP packets from the IP address of the NAM. Filtering SNMP traffic to an affected device can be used as a mitigation. Filtering SNMP traffic needs to be done on systems that are deployed in front of an affected device, since it is ineffective to filter against such spoofed packets on the device itself.

Anti-spoofing measures and infrastructure access-lists can also be deployed at your network edge as a potential mitigation technique. Refer to http://www.cisco.com/warp/public/707/iacl.html for examples on how to apply ACLs on Cisco routers for infrastructure protection.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document.

**NAT - 13659**

**Description**
A group of related software bugs create an undesired interaction between network address translation (NAT) and input access list processing. This may cause input access list filters to "leak" packets in certain NAT configurations, creating a security exposure. Configurations without NAT are not affected. The failure does not happen at all times, and is less likely under laboratory conditions than in installed networks. This may cause administrators to believe that filtering is working when it is not. See "Cisco IOS Software Input Access List Leakage with NAT." at Cisco Security Advisories website.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices(13659 of 1.3)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT - 13659: Verify Input Access List Leakage with NAT [IOS]

**Description**
A group of related software bugs create an undesired interaction between network address translation (NAT) and input access list processing. This may cause input access list filters to "leak" packets in certain NAT configurations, creating a security exposure. Configurations without NAT are not affected. The failure does not happen at all times, and is less likely under laboratory conditions than in installed networks. This may cause administrators to believe that filtering is working when it is not. See "Cisco IOS Software Input Access List Leakage with NAT." at Cisco Security Advisories website.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
This vulnerability may allow users to circumvent network security filters, and therefore security policies.
Suggested Fix
None

NAT Skinny Call Control Protocol Vulnerability - 111268

Description
Skinny Client Control Protocol (SCCP) crafted messages may cause a Cisco IOS device that is configured with the Network Address Translation (NAT) SCCP Fragmentation Support feature to reload. Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(111268 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 111268: Verify NAT Skinny Call Control Protocol Vulnerability [IOS]

Description
The Skinny Client Control Protocol (SCCP) enables voice communication between an SCCP client and a Call Manager (CM). Typically, the CM provides service to the SCCP clients on TCP Port 2000 by default. Initially, an SCCP client connects to the CM by establishing a TCP connection; the client will also establish a TCP connection with a secondary CM, if available.

The NAT SCCP Fragmentation Support feature enables the Skinny Application Layer Gateway (ALG) to reassemble skinny control messages. Since this feature was introduced in Cisco IOS version 12.4(6)T, SCCP payloads requiring reassembly and NAT are no longer dropped.

A series of crafted SCCP packets may cause a Cisco IOS router that is running the NAT SCCP Fragmentation Support feature to reload.

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of this vulnerability may cause the affected device to reload. Repeated exploitation will result in a denial of service (DoS) condition.

Suggested Fix
As workaround, an administrator can disable SCCP NAT support using the no ip nat service skinny tcp port 2000 command, as shown in the following example:

Router(config)# no ip nat service skinny tcp port 2000
Note: If your Cisco CallManager is using a TCP port for skinny signaling different from the default port (2000), you need to adjust this command accordingly.

Caution: This workaround is only feasible on networks where SCCP traffic does not need to be processed by NAT. Please confirm before implementing this workaround.

NAT Skinny Call Control Protocol Vulnerability - 99866

Description
A series of segmented Skinny Call Control Protocol (SCCP) messages may cause a Cisco IOS device that is configured with the Network Address Translation (NAT) SCCP Fragmentation Support feature to reload.

Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (99866 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 99866: Verify Cisco IOS NAT Skinny Call Control Protocol Vulnerability [IOS]

Description
The Skinny Call Control Protocol (SCCP) enables voice communication between an SCCP client and a Call Manager (CM). Typically, the CM provides service to the SCCP clients on TCP Port 2000 by default. Initially, an SCCP client connects to the CM by establishing a TCP connection; the client will also establish a TCP connection with a secondary CM, if available.

The NAT SCCP Fragmentation Support feature prevents skinny control message exchanges from failing in a TCP segmentation scenario because the NAT Skinny Application Layer Gateway (ALG) is able to reassemble the skinny control messages. A segmented payload that requires an IP or port translation will no longer be dropped. The NAT SCCP Fragmentation Support feature was introduced in Cisco IOS version 12.4(6)T.

A series of fragmented SCCP messages may cause a Cisco IOS router that is running the NAT SCCP Fragmentation Support feature to reload.

Applicable Platforms
Cisco IOS Devices
Impact
Successful exploitation of this vulnerability may cause the affected device to reload. Repeated exploitation will result in a denial of service (DoS) condition.

Suggested Fix
As workaround, an administrator can disable SCCP NAT support using the `no ip nat service skinny tcp port 2000` command, as shown in the following example:

```
Router(config)# no ip nat service skinny tcp port 2000
```

Note
If your Cisco CallManager is using a TCP port for skinny signaling different from the default port (2000), you need to adjust this command accordingly.

NTP - 23445

Description
Network Time Protocol (NTP) is used to synchronize time on multiple devices. A vulnerability has been discovered in the NTP daemon query processing functionality. This vulnerability has been publicly announced.

See "NTP Vulnerability" at Cisco Security Advisories website for more information

Applicable Platforms
Cisco IOS Devices
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability

References
CISCO PSIRT Advisories and Notices(23445 of 2.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 23445: Verify NTP Vulnerabilities [IOS]

Description
Network Time Protocol (NTP) is used to synchronize time on multiple devices. A vulnerability has been discovered in the NTP daemon query processing functionality. This vulnerability has been publicly announced.

See "NTP Vulnerability" at Cisco Security Advisories website for more information

Applicable Platforms
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability
Impact
The successful exploitation may cause arbitrary code to be executed on the target machine. More often, an attempt to exploit this vulnerability will result in a daemon or device crash.

Suggested Fix
There are methods available to mitigate the exposure. You can combine these methods or use them individually.

Prevent IOS from processing NTP queries at all. Depending on whether you are acting as a server or a client, the configuration is different.

It is possible to mitigate the exposure by using ACLs and dropping all NTP packets that are not from the legitimate servers.

Additionally, if you are not using NTP servers external from your network, you can drop all NTP packets on the network boundary.

NTP Packet Vulnerability - 110447

Description
Cisco IOS Software with support for Network Time Protocol (NTP) version (v4) contains a vulnerability processing specific NTP packets that will result in a reload of the device. This results in a remote denial of service (DoS) condition on the affected device.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(110447 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 110447: Verify NTP Packet Vulnerability [IOS]

Description
Cisco IOS Software devices are vulnerable if they support NTPv4 and are configured for NTP operations. NTP is not enabled in Cisco IOS Software by default.

To see if a device supports NTPv4, log into the device and via configuration mode of the command line interface (CLI), enter the command `ntp peer 127.0.0.1 version` ?. If the output has the number 4 as an option, then the device supports NTPv4. The following example identifies a Cisco device that is running a Cisco IOS Software release that does support NTPv4:

Router#configure terminal
Router(config)#ntp peer 127.0.0.1 version ?
<2-4> NTP version number
The following example identifies a Cisco device that is running a Cisco IOS Software release that does not support NTPv4:

Router(config)#ntp peer 127.0.0.1 version?

<1-3> NTP version number

To see if a device is configured with NTP, log into the device and issue the CLI command `show running-config | include ntp`. If the output returns either of the following commands listed then the device is vulnerable:

ntp master <any following commands>
ntp peer <any following commands>
ntp server <any following commands>
ntp broadcast client
ntp multicast client

The following example identifies a Cisco device that is configured with NTP:

router#show running-config | include ntp
ntp peer 192.168.0.12

The following example identifies a Cisco device that is not configured with NTP:

router#show running-config | include ntp

---

**Applicable Platforms**

Cisco IOS Devices

**Impact**

Successful exploitation of the vulnerability may result in a reload of the device. The vulnerability could be repeatedly exploited to cause an extended DoS condition.

**Suggested Fix**

There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

---

**Note**

NTP peer authentication is not a workaround and is still a vulnerable configuration.

---

**NTP Access Group**

---

**Warning**

Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

---

!--- Configure trusted peers for allowed access
access-list 1 permit 171.70.173.55

!--- Apply ACE to the NTP configuration
ntp access-group 1
For additional information on NTP access control groups, consult the document titled "Performing Basic System Management" at the following link:

**Infrastructure Access Control Lists**

---

**Warning**

Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```plaintext
-- Feature: Network Time Protocol (NTP)

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

Note: If the router is acting as a NTP broadcast client
-- via the interface command "ntp broadcast client"
-- then broadcast and directed broadcasts must be
-- filtered as well. The following example covers
-- an infrastructure address space of 192.168.0.X
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 255.255.255.255 eq ntp

Note: If the router is acting as a NTP multicast client
-- via the interface command "ntp multicast client"
-- then multicast IP packets to the multicast group must
-- be filtered as well. The following example covers
-- a NTP multicast group of 239.0.0.1 (Default is
-- 224.0.1.1)
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 239.0.0.1 eq ntp

Deny NTP traffic from all other sources destined
-- to infrastructure addresses.
```
access-list 150 deny udp any
   INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations. Permit all other traffic to transit the
!--- device.
access-list 150 permit ip any any
!--- Apply access-list to all interfaces (only one example
!--- shown)
interface fastEthernet 2/0
   ip access-group 150 in

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents
guidelines and recommended deployment techniques for infrastructure protection access lists and is
available at the following link

**Control Plane Policing**

---

**Warning** Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the
sender's IP address, which may defeat ACLs that permit communication to these ports from
trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better
mitigation solution.
Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```plaintext
!--- Feature: Network Time Protocol (NTP)
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD any eq 123
!--- Deny NTP traffic from all other sources destined to the device control plane.
access-list 150 permit udp any any eq 123
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4 traffic in accordance with existing security policies and configurations for traffic that is authorized to be sent to infrastructure devices
!--- Create a Class-Map for traffic to be policed by the CoPP feature
class-map match-all drop-udp-class
  match access-group 150
!--- Create a Policy-Map that will be applied to the Control-Plane of the device.
policy-map drop-udp-traffic
  class drop-udp-class
    drop
!--- Apply the Policy-Map to the Control-Plane of the device
control-plane
  service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Please note that the policy-map syntax is different in the 12.2S and 12.0S Cisco IOS Software trains:

```plaintext
policy-map drop-udp-traffic
  class drop-udp-class
  police 32000 1500 1500 conform-action drop exceed-action drop
```

Network Address Translation Vulnerability - 112028

**Description**
The Cisco IOS® Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

Cisco has released free software updates that address these vulnerabilities.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices(112028 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT - 112028: Verify Cisco IOS Software Network Address Translation Vulnerability [IOS]

**Description**
Cisco devices running Cisco IOS Software that are configured for NAT and that support NAT for SIP, H.323, or H.225.0 call signaling for H.323 packets are affected.

To verify whether NAT is enabled on a Cisco IOS device log in to the device and issue the show ip nat statistics command. The following example shows a device that is configured with NAT:

Router#show ip nat statistics

*Total translations*: 2 (0 static, 2 dynamic; 0 extended)
*Outside interfaces*: Serial0
*Inside interfaces*: Ethernet1
*Hits*: 135 *Misses*: 5
*Expired translations*: 2
*Dynamic mappings*:
  -- Inside Source
  access-list 1 pool mypool refcount 2
  pool mypool: netmask 255.255.255.0
  start 192.168.10.1 end 192.168.10.254
type generic, total addresses 14, allocated 2 (14%), misses 0

Alternatively, administrators can use the `show running-config | include ip nat` command to verify if NAT has been enabled on the router interfaces.

For NAT to be enabled in a router either the `ip nat inside` and `ip nat outside` commands must be present in different interfaces or, in the case of NAT Virtual Interface, if the `ip nat enable interface` command is present.

In order to determine the software that runs on a Cisco IOS product, log in to the device and issue the `show version` command to display the system banner. Cisco IOS software identifies itself as "Internetwork Operating System Software" or simply "IOS." On the next line of output, the image name displays between parentheses, followed by "Version" and the Cisco IOS release name. Other Cisco devices do not have the show version command or give different output.

The following example shows output from a device that runs an IOS image:

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
<More output removed for brevity>
```

**Applicable Platforms**

Cisco IOS Devices

**Impact**

Successful exploitation of any of the vulnerabilities described in this document may cause the affected device to reload. Repeated exploitation will result in an extended denial of service (DoS) condition.

**Suggested Fix**

The mitigations for the NAT vulnerabilities disable the respective Application Layer Gateway NAT processing. That is, packets will continue to be translated at the network and transport layers, but the embedded IP addresses will not be translated.

**NAT for Session Initiation Protocol DoS Vulnerability**

Mitigation for this vulnerability consists of disabling NAT for SIP over the UDP transport by using the `no ip nat service sip udp port 5060` global configuration command.

**NAT for H.323 DoS Vulnerability**

Mitigation for this vulnerability consists of disabling NAT for H.323 and H.225.0 using the `no ip nat service h225` global configuration command.

**NAT for H.225.0 DoS vulnerability**

Mitigation for this vulnerability consists of disabling NAT for H.323 and H.225.0 using the `no ip nat service h225` global configuration command.
Next Hop Resolution Protocol Vulnerability - 91766

Description
The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature. NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

NHRP is not enabled by default for Cisco IOS.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (91766 of 1.2)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 91766: Verify Next Hop Resolution Protocol Vulnerability [IOS]

Description
NHRP is a standards-based protocol that is aimed at providing Layer 2 to Layer 3 resolution for Nonbroadcast Multiaccess networks (NBMA).

Network devices and hosts can use NHRP to discover the addresses of other devices connected to an NBMA network.

For more information on NHRP, see

NHRP is an open standard and the public RFC is on the web at:
http://www.rfc-editor.org/rfc/rfc2332.txt

NHRP has extended uses in DMVPNs, can be carried in GRE and mGRE tunnels or can be transported directly within IP datagrams as IP protocol number 54.

Workarounds are available for protecting routers from NHRP packets sent over GRE or mGRE tunnels or sent as NHRP directly in IP datagrams.

No workarounds exist for blocking Layer 2 NHRP packets. However, Layer 2 NHRP packets are not routable and must be sent by a Layer 2-adjacent device.

Applicable Platforms
Cisco IOS Devices
Impact
Successful exploitation of the vulnerability may result in a restart of the device or remote code execution. Repeated exploitation may result in an extended denial of service (DoS) condition.

Suggested Fix
Customers who do not need NHRP functionality may disable the NHRP service and eliminate the exposure to this vulnerability.
If NHRP is required, the only complete resolution to this issue is to upgrade to a fixed version of software.
Additional mitigations that can be deployed on Cisco devices within the network are discussed in the Cisco Applied Intelligence companion document.
Because this attack can be sent from spoofed source addresses, anti-spoofing techniques are required for the workarounds in this section to be most effective.

OSPF Malformed Packet- 61365 [IOS]

Description
A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(61365 of 1.4)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-61365: Verify Malformed OSPF Packet Causes Reload Vulnerability[IOS]

Description
A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

Applicable Platforms
Cisco IOS Devices
Impact
Successful exploitation of this vulnerability results in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

Suggested Fix
OSPF authentication may be used as a workaround. OSPF packets without a valid key will not be processed. MD5 authentication is highly recommended, due to inherent weaknesses in plain text authentication.

OSPF, MPLS VPN Vulnerability - 100526 [IOS]

Description
Certain Cisco Catalyst 6500 Series and Cisco 7600 Router devices that run branches of Cisco IOS based on 12.2 can be vulnerable to a denial of service vulnerability that can prevent any traffic from entering an affected interface. For a device to be vulnerable, it must be configured for Open Shortest Path First (OSPF) Sham-Link and Multi Protocol Label Switching (MPLS) Virtual Private Networking (VPN). This vulnerability only affects Cisco Catalyst 6500 Series or Catalyst 7600 Series devices with the Supervisor Engine 32 (Sup32), Supervisor Engine 720 (Sup720) or Route Switch Processor 720 (RSP720) modules. The Supervisor 32, Supervisor 720, Supervisor 720-3B, Supervisor 720-3BXL, Route Switch Processor 720, Route Switch Processor 720-3C, and Route Switch Processor 720-3CXL are all potentially vulnerable.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices (100526 of 1.1)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-100526: Verify Vulnerability in Cisco IOS with OSPF, MPLS VPN[IOS]

Description
CVE ID CVE-2008-0537.
The following combination of hardware and software configuration must be present for the device to be vulnerable:
Cisco Catalyst Sup32, Sup720, or RSP720 is present
MPLS VPN is configured
OSPF sham-link is configured
In order to determine whether you are running this feature, use the show running-config command and search for the **address-family vpnv4** and **area sham-link** router configuration commands. The following command displays all configuration lines that meet the following criteria:
Begins with the word "router," OR
Includes "address-family vpnv4," OR
Includes "sham-link"
Router# show run | include ^router |address-family vpnv4|sham-link
router bgp 1
    address-family vpnv4
router ospf 1 vrf VRFNAME
    area 0 sham-link  192.168.1.1 192.168.100.1
Router#

For customers that run versions of IOS that support the section modifier, an additional option is available to view the relevant sections of the running configuration:
Router# show run | section ^router
router bgp 1
    [snip]
    address-family vpnv4
router ospf 1 vrf VRFNAME
    area 0 sham-link  192.168.1.1 192.168.100.1
    [snip]
If certain packets are received by a device that meets the above requirements, the input queue of the interface that receives these packets can become blocked, which can prohibit additional traffic from entering the interface and cause a denial of service condition. In addition to a potential blocked interface queue, the device can also suffer a memory leak or restart. In the event of a memory leak, the device is unable to forward traffic once available memory is depleted.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
Exploitation of this vulnerability may result in a blocked interface input queue, memory leak, and/or restart of the device. Repeated exploitation of this vulnerability may result in an extended denial of service.

**Suggested Fix**
Once a device interface queue has been exhausted, only a device restart can clear OSPF packets in the blocked queue.

Due to the manner in which these packets are processed, the queue block occurs prior to the OSPF MD5 check. The OSPF MD5 configuration does not protect a device from this vulnerability.

Increasing the SPD headroom provides additional buffering for OSPF packets. In the event of a blocked queue, the SPD headroom can be increased to allow more control plane traffic buffer space.

It is possible to expand the queue size to accommodate more packets, but packets can still accumulate until the expanded queue is exhausted. As a temporary workaround that allows traffic to continue to flow, the input hold queue can be increased. Any additional malformed packets still fill the queue, but...
increasing the input queue depth can extend the amount of time before the input queue fills and traffic ceases flowing. The following example demonstrates how to set the input queue size from the default of 75 to the maximum of 4096:

```
Router# configure terminal
Router(configure)# interface FastEthernet 0/0
Router(config-if)# hold-queue 4096 in
```

Because OSPF Sham-Link configuration is required for the vulnerability to be present, removing Sham-Link functionality eliminates exposure to this vulnerability. In order to remove the OSPF Sham-Link configuration from a device, the OSPF configuration must be changed on each interface where Sham-Link is configured.

Cisco IOS Embedded Event Manager (EEM) provides event detection and reaction capabilities on a Cisco IOS device. It is possible to detect blocked interface queues with an EEM policy. EEM can alert administrators of blocked interfaces with email, a syslog message, or a Simple Network Management Protocol (SNMP) trap.

### Object-Group ACL Bypass Vulnerability - 110398 [IOS]

**Description**

A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature.

**Applicable Platforms**

Cisco IOS Devices

**References**

CISCO PSIRT Advisories and Notices (110398 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PSIRT-110398: Verify Object-Group ACL Bypass Vulnerability [IOS]

**Description**

In Cisco IOS Software an object group can contain a single object (such as a single IP address, network, or subnet) or multiple objects (such as a combination of multiple IP addresses, networks, or subnets). In an ACL that is based on an object group, administrators can create a single access control entry (ACE) that uses an object group name instead of creating many ACEs, which each would require a different IP address. A similar object group, such as a protocol port group, can be extended to limit access to a set of applications for a user group to a server group.

Note: The Cisco Catalyst 6500 Object Groups feature for policy-based ACLs (PBACLs) is not affected by this vulnerability.
A vulnerability exists in Cisco IOS Software that could allow an unauthenticated attacker to bypass access control policies when the Object Groups for ACLs feature is used.

Note: The Object Groups for ACLs feature was introduced in Cisco IOS software version 12.4(20)T.

**Applicable Platforms**
Cisco IOS Devices

**Impact**
Successful exploitation of the vulnerability may allow an attacker to access resources that should be protected by the Cisco IOS device.

**Suggested Fix**
There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature.

**OpenSSL Implementation DoS Vulnerability - 45643 [IOS]**

**Description**
An affected network device running an SSL server based on an affected OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client. The network device may be vulnerable to this vulnerability even if it is configured to not authenticate certificates from the client.

See "SSL Implementation Vulnerabilities." at Cisco Security Advisories website

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices(45643 of 2.2)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT-45643: Verify SSL Implementation Vulnerabilities [IOS]

**Description**
An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client. The network device is vulnerable to this vulnerability even if it is configured to not authenticate certificates from the client.

**Applicable Platforms**
Cisco IOS Devices
Impact
An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client regardless of whether it is configured to process client certificates or not.

Suggested Fix
The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code as soon as it is available.
- Restrict access to the HTTPS server on the network device. Allow access to the network device only from trusted workstations by using access lists / MAC filters that are available on the affected platforms.
- Disable the SSL server / service on the network device. This workaround must be weighed against the need for secure communications with the vulnerable device.

Cisco SIP Proxy Server (SPS) - Disable SSL/TLS functionality. One can do this using the Provisioning GUI. Log in, then select Farm/Proxies from the Configuration options. Select Advanced, and then the SIP Server Core tab. Turn the Enable TLS directive to Off.

OpenSSL Implementation Vulnerability - 49898 [IOS]

Description
An affected network device running an SSL server based on an affected OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack. See "Cisco OpenSSL Implementation Vulnerability" at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

References
CISCO PSIRT Advisories and Notices(49898 of 1.6)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT-49898: Verify Open SSL Implementation Vulnerability [IOS]

Description
Secure Sockets Layer (SSL), is a protocol used to encrypt the data transferred over a TCP session. SSL in Cisco products is mainly used by the HyperText Transfer Protocol Secure (HTTPS) web service for which the default TCP port is 443. The affected products, listed above, are only vulnerable if they have the HTTPS service enabled and the access to the service is not limited to trusted hosts or network management workstations. They are not vulnerable to transit traffic, only traffic that is destined to them may exploit this vulnerability.
To check if the HTTPS service is enabled one can do the following:

1. Check the configuration on the device to verify the status of the HTTPS service.
2. Try to connect to the device using a standard web browser that supports SSL using a URL similar to https://ip_address_of_device/.
3. Try and connect to the default HTTPS port, TCP 443, using Telnet. telnet ip_address_of_device 443. If the session connects the service is enabled and accessible.

Applicable Platforms
Cisco IOS Devices

Impact
An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack.

Suggested Fix
The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code as soon as it is available.

- Restrict access to the HTTPS server on the network device. Allow access to the network device only from trusted workstations by using access lists / MAC filters that are available on the affected platforms.
- Disable the SSL server / service on the network device. This workaround must be weighed against the need for secure communications with the vulnerable device.

PIX Crafted MGCP Packet - 98711 [PIX, ASA]

Description
Two crafted packet vulnerabilities exist in the Cisco PIX 500 Series Security Appliance (PIX) and the Cisco 5500 Series Adaptive Security Appliance (ASA) that may result in a reload of the device. These vulnerabilities are triggered during processing of Media Gateway Control Protocol (MGCP) packets, or during processing of Transport Layer Security (TLS) traffic that terminates on the PIX or ASA security appliance. The Cisco PIX and ASA security appliances are affected by a crafted MGCP packet vulnerability if MGCP application layer protocol inspection is enabled and the device is running certain 7.x software versions. Version 6.3.x is not affected. MGCP inspection is not enabled by default. For specific affected versions, refer to the Software Versions and Fixes section. The PIX and ASA security appliances are also affected by a crafted TLS packet vulnerability that affects devices running certain 7.x software versions if the software has one or more features configured that cause TLS sessions to terminate on the PIX or ASA security appliance. These functions include, but are not limited to, clientless WebVPN, client connections with AnyConnect and the SSL VPN client, HTTPS management, cut-through proxy for network access, and TLS proxy for encrypted voice inspection. Version 6.3.x is not affected. Features that cause TLS sessions to terminate on the PIX and ASA security appliances are not enabled by default. For specific affected versions, please refer to the Software Versions and Fixes section. In addition to the PIX and ASA security appliances, the crafted MGCP packet vulnerability also affects the Cisco Firewall Services Module (FWSM). More information regarding the FWSM can be found in the companion advisory http://www.cisco.com/warp/public/707/cisco-sa-20071017

Applicable Platforms
Cisco PIX and ASA Firewalls
Rule 1

Rule
PIX PSIRT-98711: Verify Crafted MGCP Packet Vulnerabilities [PIX, ASA]

Description
A PIX or ASA security appliance with the Media Gateway Control Protocol (MGCP) application layer protocol inspection feature enabled may reload when the device processes a crafted MGCP packet. MGCP application layer protocol inspection is not enabled by default. MGCP messages are transmitted over the User Datagram Protocol (UDP), which does allow the crafted MGCP messages to be sourced from a spoofed address. Only the MGCP for gateway application (MGCP traffic on UDP port 2427) is affected.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the vulnerabilities described in this advisory will result in a reload of the affected device. Repeated exploitation can result in a sustained denial of service (DoS) condition.

Suggested Fix
There is no workaround for this vulnerability other than disabling MGCP application layer protocol inspection on the device. Leveraging anti-spoofing techniques will help mitigate spoofed packets from triggering this vulnerability. Limiting MGCP application layer inspection to traffic between MGCP gateways may help to mitigate this vulnerability since it would require an attacker to have additional information (the addresses of the MGCP gateways) to launch a successful attack. To limit MGCP application layer inspection to traffic between certain devices, a class map that matches only traffic between the gateways must be created. Then, MGCP inspection must be performed on traffic in that class. The following example shows how to accomplish this:

ASA(config)# access-list mgcp_traffic permit udp host 192.168.0.1 host 172.16.0.1 eq 2427
ASA(config)# access-list mgcp_traffic permit udp host 172.16.0.1 host 192.168.0.1 eq 2427
ASA(config)# class-map MGCP ASA(config-cmap)# match access-list mgcp_traffic
ASA(config-cmap)# exit
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# no inspect mgcp
ASA(config-pmap-c)# exit
ASA(config-pmap)# class MGCP
ASA(config-pmap-c)# inspect mgcp
ASA(config-pmap-c)# exit
ASA(config-pmap)# exit
ASA(config)#
Note that MGCP inspection is applied only to UDP traffic between hosts 192.168.0.1 and 172.16.0.1. See the Cisco Applied Intelligence companion document for additional mitigation possibilities.

**PIX Crafted TLS Packet - 98711 [PIX, ASA]**

**Description**

Two crafted packet vulnerabilities exist in the Cisco PIX 500 Series Security Appliance (PIX) and the Cisco 5500 Series Adaptive Security Appliance (ASA) that may result in a reload of the device. These vulnerabilities are triggered during processing of Media Gateway Control Protocol (MGCP) packets, or during processing of Transport Layer Security (TLS) traffic that terminates on the PIX or ASA security appliance. Note: These vulnerabilities are independent of each other; a device may be affected by one and not by the other.

**Applicable Platforms**

Cisco PIX and ASA Firewalls

**References**

CISCO PSIRT Advisories and Notices (98711 of 1.1)

Security Advisories: For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices: For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PIX PSIRT-98711: Verify Crafted TSL Packet Vulnerabilities [PIX, ASA]

**Description**

Transport Layer Security (TLS) is the replacement for the Secure Socket Layer (SSL) protocol. It is a protocol that provides, via cryptography, secure communications between two end-points. The PIX and ASA security appliances rely on TLS to protect the confidentiality of communications in a variety of scenarios. In all these scenarios, the PIX and ASA may be affected by a vulnerability in the handling of the TLS protocol that may lead to a reload of the device when it processes specially crafted TLS packets. The scenarios affected by this vulnerability are clientless WebVPN connections, HTTPS management sessions, cut-through proxy for network access, and TLS proxy for encrypted voice inspection.

**Applicable Platforms**

Cisco PIX and ASA Firewalls

**Impact**

Successful exploitation of the vulnerabilities described in this advisory will result in a reload of the affected device. Repeated exploitation can result in a sustained denial of service (DoS) condition.

**Suggested Fix**

ASDM is used to manage the Cisco PIX or ASA security appliance. Access to ASDM should be allowed only on trusted interfaces and only from authorized hosts. Restricting ASDM access to trusted hosts limits the ability of an attacker to conduct these attacks. For example, to limit ASDM access to a single...
Understanding Compliance and Audit Manager (CAAM) Policies

Chapter 4  Using Compliance and Audit Manager Feature

host on the inside interface with an address of 192.168.1.2, enter the following command:
hostname(config)# http 192.168.1.2 255.255.255.255 inside Additional information is available at:

There are no workarounds if the clientless WebVPN, client connections with AnyConnect and the SSL
VPN client, cut-through proxy for network access, and TLS proxy for encrypted voice inspection
features are in use.

PIX Erroneous SIP Processing Vulnerabilities - 107475 [PIX, ASA]

Description
Erroneous SIP Processing Vulnerabilities exist in the Cisco ASA 5500 Series Adaptive Security
Appliances and Cisco PIX Security Appliances that may result in a reload of the device or disclosure of
confidential information.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
CISCO PSIRT Advisories and Notices(107475 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to
repair the Cisco product. Security Notices For issues that require a response to information posted to a
public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT-107475: Verify Erroneous SIP Processing Vulnerabilities [PIX, ASA]

Description
Cisco PIX and Cisco ASA devices configured for SIP inspection are vulnerable to multiple processing
errors that may result in denial of service attacks. Cisco PIX and ASA software versions prior to
7.0(7)16, 7.1(2)71, 7.2(4)7, 8.0(3)20, and 8.1(1)8 are vulnerable to these SIP processing errors.
Cisco PIX and Cisco ASA devices configured for SIP inspection are vulnerable to multiple processing
errors that may result in denial of service attacks. All Cisco PIX and Cisco ASA software releases may
be vulnerable to these SIP processing vulnerabilities. A successful attack may result in a reload of the
device.

SIP inspection is enabled with the inspect sip command.

To determine whether the Cisco PIX or Cisco ASA security appliance is configured to support inspection
of sip packets, log in to the device and issue the CLI command show service-policy | include sip. If the
output contains the text Inspect: sip and some statistics, then the device has a vulnerable configuration.
The following example shows a vulnerable Cisco ASA Security Appliance:

asa#show service-policy | include sip
    Inspect: sip, packet 0, drop 0, reset-drop 0
asa#
Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the Erroneous SIP Processing Vulnerabilities may result in the device reloading. This can be repeatedly exploited and may lead to a denial of service attack.

Suggested Fix
SIP inspection should be disabled if it is not needed and temporarily disabling the feature will mitigate the SIP processing vulnerabilities. SIP inspection can be disabled with the command no inspect sip.

PIX Buffer overflow - 28947 [PIX, ASA]

Description
The Cisco PIX Firewall provides robust, enterprise-class security services including stateful inspection firewalls, standards-based IP Security (IPsec) Virtual Private Networking (VPN), intrusion protection and much more in cost-effective, easy to deploy solutions.

Two vulnerabilities have been resolved for the PIX firewall for which fixes are available. These vulnerabilities are documented as Cisco bug ID CSCdv83490 and CSCdx35823. There are no workarounds available to mitigate the effects of these vulnerabilities.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
CISCO PSIRT Advisories and Notices(28947_2 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT-28947: Verify Buffer overflow Vulnerability [PIX, ASA]

Description
CSCdv83490

When a user establishes a VPN session upon successful peer and user authentication, the PIX creates an ISAKMP SA associating the user and his IP address.

If an attacker is now able to block the logged-in user's connection and establish a connection to the PIX using the same IP address as that of the user, he will be able to establish a VPN session with the PIX, using only peer authentication, provided he already has access to the peer authentication key also known as the group pre-shared key (PSK) or group password key.

CSCdx35823
Understanding Compliance and Audit Manager (CAAM) Policies

Chapter 4 Using Compliance and Audit Manager Feature

A user starting a connection via FTP, Telnet, or over the World Wide Web (HTTP) is prompted for their user name and password. If the user name and password are verified by the designated TACACS+ or RADIUS authentication server, the PIX Firewall unit will allow further traffic between the authentication server and the connection to interact independently through the PIX Firewall unit's "cut-through proxy" feature.

The PIX may crash and reload due to a buffer overflow vulnerability while processing HTTP traffic requests for authentication using TACACS+ or RADIUS.

These vulnerabilities are documented in the Bug Toolkit as Bug IDs CSCdv83490 and CSCdx35823, and can be viewed after 2002 November 21 at 1600 UTC. To access this tool, you must be a registered user and you must be logged in.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact

<table>
<thead>
<tr>
<th>DDTs - Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCdv83490—While processing initial contact notify messages the PIX does not delete duplicate ISAKMP SA's with the peer</td>
<td>This vulnerability can be exploited to initiate a Man-In-The-Middle attack for VPN sessions to the PIX</td>
</tr>
<tr>
<td>CSCdx35823 - Buffer overflow while doing HTTP traffic authentication using TACACS+ or RADIUS</td>
<td>This vulnerability can be exploited to initiate a Denial-of-Service attack</td>
</tr>
</tbody>
</table>

Suggested Fix
There are no workarounds for this vulnerability. The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code.

PIX CBAC - 23885 [PIX, ASA]

Description
Neither Cisco's PIX Firewall, nor the Context-Based Access Control (CBAC) feature of Cisco's IOS Firewall Feature Set, protects hosts against certain denial of service attacks involving fragmented IP packets. This vulnerability does not permit network "break-ins". The vulnerability is most severe in configurations involving static Network Address Translation (NAT) entries, or in configurations not involving any use of NAT.

The vulnerability is present in Cisco PIX Firewall software up to and including version 4.2(1), and in CBAC versions of Cisco IOS software through 11.2P and 11.3T, and will be present in initial 12.0 revisions of CBAC software.

The Cisco Centri Firewall does not share this vulnerability.

Stateless packet filtering products, such as the extended access lists available in non-CBAC versions of Cisco IOS software, share the vulnerability because of the inherent limitations of stateless operation. This it is not considered a defect in stateless filtering. More information is in the section on "Stateless Packet Filters" in this document.
This vulnerability will be fixed in Cisco PIX Firewall software version 4.2(2), which is tentatively scheduled for release on or after September 16, 1998. The vulnerability is scheduled to be fixed for CBAC in Cisco IOS software release 12.0(2) and 12.0(3)T, which are tentatively scheduled for release in late November 1998, and in late January 1999, respectively. All schedules are subject to change.

The possibility of IP fragmentation attacks against packet filters, from Cisco and other vendors, has been widely known for a very long time. However, exploitation does not seem to be increasing. Therefore, Cisco does not believe that the majority of its customers are critically exposed by this vulnerability. Cisco is, however, prepared to support any customers who suffer actual attacks, or who have specific reason to think that they are likely to be attacked in this way.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
CISCO PSIRT Advisories and Notices(23885 of 1.2)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PIX PSIRT-23885 : Verify for PIX CBAC Vulnerability [PIX, ASA]

**Description**
This vulnerability on the PIX Firewall has been assigned Cisco bug ID CSCdk36273.

Note: If you are a registered CCO user and you have logged in, you can view bug details.
View CSCdk36273 (registered customers only)

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**Impact**
Even though the firewall keeps an attacker from making actual connections to a given host, he or she may still be able to disrupt services provided by that host. This is done by sending many unmatched non-initial IP fragments, which use reassembly resources on the target host. Hosts vary widely in the quality of their resource management and in their response to this attack. Some hosts can be made nearly useless by traffic levels that might realistically be available to attackers.

The attack can be launched only against hosts to which the attackers can address packets. If dynamic NAT is being used, attack packets can be sent only to hosts which are actively communicating with the Internet, since NAT translation table entries will not exist for other hosts.

Because the firewall drops only the initial fragments of blocked datagrams, attackers can exploit this vulnerability by sending streams of complete fragmented packets. The attacker in this case deliberately intends the initial fragments to be blocked by the firewall. Since only the non-initial fragments will be forwarded, the effect on the target host will be similar to the effect of sending only the non-initial fragments to begin with. This method involves some waste of the attacker's resources, and is therefore
slightly less effective than simply sending the non-initial fragments alone. This method is of interest because it allows attacks to be launched using relatively standard networking tools, without any special exploit program.

**Suggested Fix**

There are no workarounds for this vulnerability. The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code.

**PIX Control Plane Access Control List Vulnerability - 105444 [PIX, ASA]**

**Description**

A vulnerability exists in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances. This security advisory outlines details of the vulnerability:

Control-plane Access Control List Vulnerability

The Control-plane Access Control List Vulnerability may allow an attacker to bypass control-plane access control lists (ACL).

**Applicable Platforms**

Cisco PIX and ASA Firewalls

**References**

CISCO PSIRT Advisories and Notices(105444 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PSIRT- 105444 : Verify Control Plane Access Control List Vulnerability [PIX, ASA]

**Description**

Cisco ASA and Cisco PIX devices are affected by a vulnerability if the device is configured to use control-plane ACLs and if it is running software versions prior to 8.0(3)9 on the 8.0.x release. Devices running software versions 7.x or 8.1.x are not vulnerable.

Note: Control-plane ACLs were first introduced in software version 8.0(2). The control-plane ACLs are not enabled by default.

The show version command-line interface (CLI) command can be used to determine if a vulnerable version of the Cisco PIX or Cisco ASA software is running. The following example shows a Cisco ASA Security Appliance that runs software release 8.0(2):

ASA# show version

Cisco Adaptive Security Appliance Software Version 8.0(2)
Device Manager Version 6.0(1)
Customers who use the Cisco Adaptive Security Device Manager (ASDM) to manage their devices can find the version of the software displayed in the table in the login window or in the upper left corner of the ASDM window.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**Impact**
Successful exploitation of the this vulnerabilities may cause a reload of the affected device. Repeated exploitation could result in a sustained Denial-of-Service (DoS) condition.

**Suggested Fix**
There are no workarounds for this vulnerability.

---

**PIX Crafted TCP ACK Packet Vulnerability - 105444 [PIX, ASA]**

**Description**
A vulnerability exists in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances. This security advisory outlines details of the vulnerability:

Crafted TCP ACK Packet Vulnerability

The Crafted TCP ACK Packet Vulnerability may lead to a denial of service (DoS) condition.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
CISCO PSIRT Advisories and Notices (105444 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

---

**Rule 1**

**Rule**
PSIRT- 105444 : Verify Crafted TCP ACK Packet Vulnerability [PIX, ASA]

**Description**
**Crafted TCP ACK Packet Vulnerability**
Cisco ASA and Cisco PIX devices are affected by a crafted TCP acknowledgment (ACK) packet vulnerability. Software versions prior to 7.1(2)70 on the 7.1.x release, 7.2(4) on the 7.2.x release, and 8.0(3)10 on the 8.0.x release are affected. Cisco ASA or Cisco PIX security appliances running software version 7.0.x, or 8.1.x are not vulnerable.

Cisco ASA and Cisco PIX devices running versions 7.1.x and 7.2.x with WebVPN, SSL VPN, or ASDM enabled are affected by this vulnerability. Devices running software versions on the 8.0 release that are configured for Telnet, Secure Shell (SSH), WebVPN, SSL VPN, or ASDM enabled are affected by this vulnerability.
Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the this vulnerabilities may cause a reload of the affected device. Repeated exploitation could result in a sustained Denial-of-Service (DoS) condition.

Suggested Fix
Crafted TCP ACK Packet Vulnerability
As a workaround and best practice allow Telnet, SSH, and ASDM connections from only trusted hosts in your network.
Additionally, filters that deny TCP ports 22, 23, 80, and 443 packets may be deployed throughout the network as part of a transit ACL (tACL) policy for protection of traffic which enters the network at ingress access points. This policy should be configured to protect the network device where the filter is applied and other devices behind it. Filters for packets using TCP ports 22, 23, 80, and 443 should also be deployed in front of vulnerable network devices so that traffic is only allowed from trusted clients.
Additional information about tACLs is available in "Transit Access Control Lists : Filtering at Your Edge":

PIX Crafted TLS Packet Vulnerability - 105444 [PIX, ASA]

Description
A vulnerability exists in the Cisco ASA 5500 Series Adaptive Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances. This security advisory outlines details of the vulnerability:
Crafted TLS Packet Vulnerability
The Crafted TLS Packet Vulnerability may lead to a denial of service (DoS) condition.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
CISCO PSIRT Advisories and Notices(105444 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT- 105444 : Verify Crafted TLS Packet Vulnerability [PIX, ASA]

Description
Crafted TLS Packet Vulnerability
Cisco ASA and Cisco PIX devices are affected by a crafted TLS request vulnerability if the HTTPS server on the Cisco ASA or Cisco PIX device is enabled and is running software versions prior to 8.0(3)9 on the 8.0.x release or prior to version 8.1(1)1 on the 8.1.x release. Cisco ASA and Cisco PIX appliances running software versions 7.x are not vulnerable.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**Impact**
Successful exploitation of this vulnerability may cause a reload of the affected device. Repeated exploitation could result in a sustained Denial-of-Service (DoS) condition.

**Suggested Fix**
There are no workarounds for this vulnerability.

### PIX Crypto - 23886 [PIX, ASA]

**Description**
PIX Private Link is an optional feature that can be installed in Cisco PIX firewalls. PIX Private Link creates IP virtual private networks over untrusted networks, such as the Internet, using tunnels encrypted with Data Encryption Standard (DES). PIX Private Link in versions up to 4.1 uses DES in ECB ("electronic codebook") mode.

An error in parsing of configuration file commands reduces the effective key length for the PIX Private Link DES encryption to 48 bits from the nominal 56 bits.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
CISCO PSIRT Advisories and Notices(23886 of 1.1)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

### Rule 1

**Rule**
PIX PSIRT- 23886 : Verify for private link crypto Vulnerabilities [PIX, ASA]

**Description**
This vulnerability has been assigned Cisco bug ID CSCdk11848. The use of ECB mode is Cisco bug ID CSCdj23353.

**Applicable Platforms**
Cisco PIX and ASA Firewalls
Impact

If attackers know the details of the key-parsing error in the PIX Private Link software, they will know 8 bits of the key ahead of time. This reduces the effective key length from the attacker's point of view from 56 to 48 bits. This reduction of the effective key length reduces the work involved in a brute-force attack on the encryption by a factor of 256. That is, knowledgeable attackers can, on the average, find the right key 256 times faster than they would be able to find it with a true 56-bit key.

In addition to this key-length issue, some customers have expressed concern over the use of DES ECB mode for PIX Private Link encryption. Although the use of ECB mode is intentional, ECB is not generally considered to be the best mode in which to employ DES, because it tends to simplify certain forms of cryptanalysis and may permit certain replay attacks. Technical details of the relative merits of various encryption modes are beyond the scope of this document. Any interested reader should refer to a good cryptography text for more information, such as Bruce Schneier's *Applied Cryptography*.

Suggested Fix

There is no workaround is available for this vulnerability and user needs upgrade the PIX OS.

**PIX Crypto - 91890 [PIX, ASA]**

**Description**

A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker to decrypt any previously encrypted information.

**Applicable Platforms**

Cisco PIX and ASA Firewalls

**References**

CISCO PSIRT Advisories and Notices(91890_1 of 1.3)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PIX PSIRT- 91890 : Verify For Vulnerabilities In Crypto Library [PIX, ASA]

**Description**

A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).
Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker to decrypt any previously encrypted information.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**Impact**
Successful exploitation of the vulnerability listed in this advisory may result in the crash of a vulnerable device. Repeated exploitation can result in a sustained DoS attack.

**Suggested Fix**
The only way to prevent a device being susceptible to the listed vulnerabilities is to disable the affected service(s). However, if regular maintenance and operation of the device relies on these services then there is no workaround.

It is possible to mitigate these vulnerabilities by preventing unauthorized hosts to access the affected devices. Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document.

### PIX DoS - 13635 [PIX, ASA]

**Description**
The Cisco Secure PIX Firewall AAA authentication feature, introduced in version 4.0, is vulnerable to a Denial of Service (DoS) attack initiated by authenticating users on the system. This vulnerability affects specific configurations and has been resolved in released versions of the PIX Firewall.

This vulnerability has been assigned Cisco bug ID CSCdt92339.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com
- firewalls@lists.gnac.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

**Applicable Platforms**
Cisco PIX and ASA Firewalls
Rule 1

PIX PSIRT- 13635 : Verify for AAA authentication DoS Vulnerability [PIX, ASA]

Description
When AAA authentication services are configured on the Cisco Secure PIX Firewall, it is possible for a single source address to consume all of the authentication resources, preventing other legitimate users from authenticating. This is a denial of service strictly for the authentication resources; other established traffic continues unaffected, and only new authentication requests are prevented.

This vulnerability has been resolved in the recent versions of the PIX Firewall by creating a maximum limit of three open authentication requests per user.

Cisco Bug ID CSCdv09731 amends this limitation to allow system administrators to modify this limit, depending on their network requirements.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
This issue causes a PIX Firewall to be vulnerable to a DoS attack in which the availability of the unit is degraded. This does not result in a loss in confidentiality or in loss of integrity of the traffic being filtered.

Suggested Fix
No known workarounds. Upgrade the software version.

PIX Device Reload with SIP Inspection Vulnerability - 107475 [PIX, ASA]

Description
Device reload possible when SIP inspection is enabled exist in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances that may result in a reload of the device or disclosure of confidential information.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
CISCO PSIRT Advisories and Notices(107475 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Rule 1

Rule
PSIRT- 107475 : Verify Device Reload with SIP Inspection Vulnerability [PIX, ASA]

Description
Device reload possible when SIP inspection is enabled
Cisco PIX and Cisco ASA devices configured for SIP inspection are vulnerable to multiple processing errors that may result in denial of service attacks. Cisco PIX and ASA software versions prior to 7.0(7)16, 7.1(2)71, 7.2(4)7, 8.0(3)20, and 8.1(1)8 are vulnerable to these SIP processing errors.
Cisco PIX and Cisco ASA devices configured for SIP inspection are vulnerable to multiple processing errors that may result in denial of service attacks. All Cisco PIX and Cisco ASA software releases may be vulnerable to these SIP processing vulnerabilities. A successful attack may result in a reload of the device.
SIP inspection is enabled with the `inspect sip` command.
To determine whether the Cisco PIX or Cisco ASA security appliance is configured to support inspection of sip packets, log in to the device and issue the CLI command `show service-policy | include sip`. If the output contains the text `Inspect: sip` and some statistics, then the device has a vulnerable configuration. The following example shows a vulnerable Cisco ASA Security Appliance:

```
asa#show service-policy | include sip
Inspect: sip, packet 0, drop 0, reset-drop 0
```

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the Erroneous SIP Processing Vulnerabilities may result in the device reloading. This can be repeatedly exploited and may lead to a denial of service attack.

Suggested Fix
SIP inspection should be disabled if it is not needed and temporarily disabling the feature will mitigate the SIP processing vulnerabilities. SIP inspection can be disabled with the command `no inspect sip`.

PIX Enhanced inspection of Malformed HTTP traffic - 77853 [PIX, ASA]

Description
Vulnerability is found in Cisco PIX 500 Series Security Appliances and the Cisco ASA 5500 Series Adaptive Security Appliances that affects enhanced inspection of malformed Hypertext Transfer Protocol (HTTP) traffic.

Applicable Platforms
Cisco PIX and ASA Firewalls
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

References
CISCO PSIRT Advisories and Notices(77853 of 1.4)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT- 77853 : Verify Enhanced inspection of Malformed HTTP traffic [PIX, ASA]

Description
Cisco PIX and ASA Security Appliances may crash when inspecting a malformed HTTP request when enhanced HTTP inspection is enabled. If enhanced HTTP application inspection is enabled your configuration will contain a line like "inspect http " where is the name of a specific HTTP map. Please note that regular HTTP inspection (configured via the command "inspect http" without an HTTP map) is not affected by this vulnerability. This vulnerability affects only 7.x

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the first three vulnerabilities listed in this Advisory may crash the affected device. Repeated exploitation can result in a sustained DoS attack. Successful exploitation of CSCsh33287 can result in the escalation of user privileges and complete compromise of the affected Cisco PIX and ASA Appliances.

Suggested Fix
Disabling HTTP application inspection (appfw) will prevent Cisco PIX and ASA Appliances from being vulnerable to the issue listed in this Advisory. By leaving inspect http statement configured, some level of protection for the end devices (for example, computers protected by Cisco PIX and ASA Appliance) will remain. However, since this level of inspection is less granular, it may have negative impact on devices terminating HTTP sessions. Devices which terminate HTTP sessions may be exposed to packets that may cause these devices to crash or become compromised.

PIX FTP - 13638 [PIX, ASA]

Description
The Cisco Secure PIX Firewall interprets FTP (File Transfer Protocol) commands out of context and inappropriately opens temporary access through the firewall. This is an interim notice describing two related vulnerabilities.

The first vulnerability is exercised when the firewall receives an error message from an internal FTP server containing an encapsulated command such that the firewall interprets it as a distinct command. This vulnerability can be exploited to open a separate connection through the firewall. This vulnerability is documented as Cisco Bug ID CSCdp86352.

The second vulnerability is exercised when a client inside the firewall browses to an external server and selects a link that the firewall interprets as two or more FTP commands. The client begins an FTP connection as expected and at the same time unexpectedly executes another command opening a separate connection through the firewall. This vulnerability is documented as Cisco Bug ID CSCdr09226.
Either vulnerability can be exploited to transmit information through the firewall without authorization. Both vulnerabilities are addressed more completely in this updated interim security advisory.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
CISCO PSIRT Advisories and Notices (13638 of 1.7)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

---

**Rule 1**

**Rule**
PIX PSIRT- 13638: Verify FTP Vulnerability[PIX, ASA]

**Description**
The first vulnerability has been assigned Cisco bug ID CSCdp86352. The second vulnerability has been assigned Cisco bug ID CSCdr09226.

The behavior is due to the command `fixup protocol ftp [portnum]`, which is enabled by default on the Cisco Secure PIX Firewall.

If you do not have protected FTP hosts with the accompanying configuration (configuration example below) you are not vulnerable to the attack which causes a server to send a valid command, encapsulated within an error message, and causes the firewall to read the encapsulated partial command as a valid command (CSCdp86352).

To exploit this vulnerability, attackers must be able to make connections to an FTP server protected by the PIX Firewall. If your Cisco Secure PIX Firewall has configuration lines similar to the following:

```plaintext
fixup protocol ftp 21
and either
conduit permit tcp host 192.168.0.1 eq 21 any
or
conduit permit tcp 192.168.0.1 255.255.255.0 eq 21 any
```

It is possible to fool the PIX stateful inspection into opening up arbitrary TCP ports, which could allow attackers to circumvent defined security policies.

If you permit internal clients to make arbitrary FTP connections outbound, you may be vulnerable to the second vulnerability (CSCdr09226). This is an attack based on CERT advisory CA-2000-02: Malicious HTML Tags Embedded in Client Web Requests [http://www.cert.org/advisories/CA-2000-02.html](http://www.cert.org/advisories/CA-2000-02.html).

The recommendation in the workarounds section of this document will provide protection against this vulnerability.

**Applicable Platforms**
Cisco PIX and ASA Firewalls
Impact
Any Cisco Secure PIX Firewall that has enabled the fixup protocol ftp command is at risk of unauthorized transmission of data through the firewall.

Suggested Fix
Disable ftp protocol inspection by using "no fixup protocol ftp" CLI on the vulnerable device.

PIX Firewall Unintentional Password Modification - 70811 [PIX, ASA]

Description
Certain versions of the software for the Cisco PIX 500 Series Security Appliances, the Cisco ASA 5500 Series Adaptive Security Appliances (ASA), and the Firewall Services Module (FWSM) are affected by a software bug that may cause the EXEC password, passwords of locally defined usernames, and the enable password in the startup configuration to be changed without user intervention.

Unauthorized users can take advantage of this bug to try to gain access to a device that has been reloaded after passwords in its startup configuration have been changed. In addition, authorized users can be locked out and lose the ability to manage the affected device.

Cisco has made free software available to address this issue for affected customers.

Applicable Platforms
Cisco PIX Devices Running >= 7.x and ASA devices

References
CISCO PSIRT Advisories and Notices(70811 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT- 70811: Unintentional Password Modification Vulnerability in Cisco Firewall Products[PIX, ASA]

Description
The Cisco PIX 500 Series Security Appliances, the Cisco ASA 5500 Series Adaptive Security Appliances, and the Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Switches and Cisco 7600 Series Routers are part of Cisco's security portfolio. All of these products offer firewall services with stateful packet filtering and deep packet inspection. The PIX and ASA devices also offer other services like Virtual Private Networking (VPN), Content Filtering, and Intrusion Prevention.

On these devices, authentication for both EXEC mode and enable mode can be performed based on Authentication, Authorization, and Accounting (AAA) methods (Remote Authentication Dial-In User Service [RADIUS], Terminal Access Controller Access Control System Plus [TACACS+], or LOCAL). If a device does not have any AAA method (i.e., RADIUS, TACACS+, or LOCAL) configured, authentication for EXEC mode is performed using the password configured with the passwd command, and authentication for enable mode is performed using the password configured with the enable password command.
A software bug exists in certain versions of the software used by these devices that may cause, under some circumstances, the EXEC password, passwords of locally defined users, and the enable password that are stored in the startup configuration to be changed without user intervention. The startup configuration is stored in a non-volatile medium such as flash memory.

The affected passwords are set using the following configuration commands:

- **passwd** - configures the EXEC password. For example:
  ```
pix(config)# passwd xxxxxxxxx
  ```
- **username** - configures local users and their associated passwords. For example:
  ```
pix(config)# username admin password xxxxxxxx
  ```
- **enable password** - configures the password used to enter enable mode. For example:
  ```
pix(config)# enable password xxxxxxxx
  ```
The software bug is known to be triggered in only two scenarios:

- A software crash, normally caused by a software bug. Please note that not all software crashes may cause the undesired results discussed above.
- Two or more users making concurrent configuration changes on a device, regardless of the method (command-line interface [CLI], Adaptive Security Device Manager [ASDM], Firewall Management Center, etc.) used to access the device.

Please note that the passwords in the startup configuration will be changed when the configuration is saved, to the non-volatile medium where the startup configuration is stored, via the `write memory` or `copy running-config startup-config` commands. During normal operation, if the running configuration is not saved, passwords in the startup configuration will not change.

Once the passwords in the startup configuration are changed, administrators will be locked out after the next device reload if authentication for EXEC and for enable privilege depends on the passwords or local accounts stored in the startup configuration. If a AAA server (RADIUS or TACACS+) is used for authentication, the change of passwords in the startup configuration will only cause the undesired results when the AAA server is unavailable, regardless of whether the "LOCAL" authentication method is configured as a fallback, e.g. `aaa authentication enable console RADIUS LOCAL`.

Passwords are changed to a non-random value. This behavior is not due to a hardcoded default password or other explicitly induced set of password values, but rather the result of a coding error related to configuration parsing.

Devices configured in multiple context mode are also affected by this software bug.

**Applicable Platforms**
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**

The software issue may cause the EXEC password, password of locally defined users, and the enable password in the startup configuration to change without user's intervention. This will prevent administrators from logging in to the device if authentication is configured to use the passwords stored in the startup configuration.

If a malicious user were able to guess the new password, and the device reloads, either automatically because of a software crash, or manually by the network administrator, unauthorized access to the device may be possible.

**Suggested Fix**

Configuring authentication against an external RADIUS/TACACS+ server, per network security best practices, mitigates this issue.

If the passwords in the startup configuration have been modified as a result of software crash or concurrent configuration update, the administrators will need to perform a password recovery procedure, unless external AAA authentication is configured.
The password recovery procedure for the PIX and the ASA is documented at the following URL:

In addition, it is possible to limit the exposure of the firewall device by permitting remote connections only from known, trusted IP addresses. This is accomplished via the ssh, telnet, and http commands for Secure Shell (SSH), Telnet, and Secure Hyper-Text Transfer Protocol (HTTPS) access, respectively.

In the case of the FWSM, please note that remote access to it can also be obtained via the Cisco Catalyst 6500 switch or Cisco 7600 Series router that hosts the FWSM blade. For this reason, the switch or router needs to be configured, using access control lists, to permit remote connections only from known, trusted IP addresses.

**PIX IPSec Client Authentication Processing Vulnerability - 107475 [PIX, ASA]**

**Description**
IPSec Client Authentication Processing Vulnerability exist in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances that may result in a reload of the device or disclosure of confidential information.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
CISCO PSIRT Advisories and Notices(107475 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability

**Rule 1**

**Rule**
PSIRT- 107475: Verfiy IPSec Client Authentication Processing Vulnerability[PIX, ASA]

**Description**
IPSec Client Authentication Processing Vulnerability
Cisco PIX and Cisco ASA devices that terminate remote access VPN connections are vulnerable to a denial of service attack if the device is running software versions prior to 7.2(4)2, 8.0(3)14, and 8.1(1)4. Cisco PIX and Cisco ASA devices that run software versions 7.0 and 7.1 are not affected by this vulnerability.

A successful attack may result in a reload of the device.

Remote access VPN connections will have Internet Security Association and Key Management Protocol (ISAKMP) enabled on an interface with the crypto command, such as: crypto isakmp enable outside.

**Applicable Platforms**
Cisco PIX and ASA Firewalls
Impact
Successful exploitation of the IPSec Client Authentication Processing Vulnerability may result in the device reloading. This can be repeatedly exploited and may lead to a denial of service attack.

Suggested Fix
Use strong group credentials for remote access VPN connections and do not give out the group credentials to end users.

PIX ISAKMP - 28947 [PIX, ASA]

Description
The Cisco PIX Firewall provides robust, enterprise-class security services including stateful inspection firewalls, standards-based IP Security (IPsec) Virtual Private Networking (VPN), intrusion protection and much more in cost-effective, easy to deploy solutions.

Two vulnerabilities have been resolved for the PIX firewall for which fixes are available. These vulnerabilities are documented as Cisco bug ID CSCdv83490 and CSCdx35823. There are no workarounds available to mitigate the effects of these vulnerabilities.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
CISCO PSIRT Advisories and Notices(28947_1 of 1.0)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT- 28947: Verify ISAKMP Vulnerability[PIX, ASA]

Description
CSCdv83490

When a user establishes a VPN session upon successful peer and user authentication, the PIX creates an ISAKMP SA associating the user and his IP address.

If an attacker is now able to block the logged-in user's connection and establish a connection to the PIX using the same IP address as that of the user, he will be able to establish a VPN session with the PIX, using only peer authentication, provided he already has access to the peer authentication key also known as the group pre-shared key (PSK) or group password key.

CSCdx35823

A user starting a connection via FTP, Telnet, or over the World Wide Web (HTTP) is prompted for their user name and password. If the user name and password are verified by the designated TACACS+ or RADIUS authentication server, the PIX Firewall unit will allow further traffic between the authentication server and the connection to interact independently through the PIX Firewall unit's "cut-through proxy" feature.
The PIX may crash and reload due to a buffer overflow vulnerability while processing HTTP traffic requests for authentication using TACACS+ or RADIUS.

These vulnerabilities are documented in the Bug Toolkit as Bug IDs CSCdv83490 and CSCdx35823, and can be viewed after 2002 November 21 at 1600 UTC. To access this tool, you must be a registered user and you must be logged in.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**Impact**

<table>
<thead>
<tr>
<th>DDTs—Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCdv83490—While processing initial contact notify messages the PIX does not delete duplicate ISAKMP SA’s with the peer.</td>
<td>This vulnerability can be exploited to initiate a Man-In-The-Middle attack for VPN sessions to the PIX.</td>
</tr>
<tr>
<td>CSCdx35823 - Buffer overflow while doing HTTP traffic authentication using TACACS+ or RADIUS.</td>
<td>This vulnerability can be exploited to initiate a Denial-of-Service attack.</td>
</tr>
</tbody>
</table>

**Suggested Fix**
There is no workaround for this vulnerability. The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code.

**PIX Inspection of a stream of malformed TCP packets - 77853 [PIX, ASA]**

**Description**
Vulnerability is found in Cisco PIX 500 Series Security Appliances and the Cisco ASA 5500 Series Adaptive Security Appliances that affects inspection of a stream of malformed Transmission Control Protocol (TCP) packets.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
CISCO PSIRT Advisories and Notices(77853 of 1.4)

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PIX PSIRT- 77853: Verify Inspection of a stream of malformed TCP packets [PIX, ASA]
Description
By processing a stream of malformed packet in a TCP-based protocol Cisco PIX and ASA Appliances may crash. Processing of the protocol must be done by inspect feature. The packets can be addressed to the device itself or just transiting it.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the vulnerability described in this advisory will result in a reload of the affected device. Repeated exploitation can result in a sustained denial of service (DoS) condition.

Suggested Fix
The workaround is to increase the minimum TCP segment size (MSS) to 64. This is accomplished with a global sysopt command: `sysopt connection tcpmss minimum 64`

PIX Inspection of malformed SIP packets - 77853 [PIX, ASA]

Description
Vulnerability is found in Cisco PIX 500 Series Security Appliances and the Cisco ASA 5500 Series Adaptive Security Appliances that affects inspection of malformed Session Initiation Protocol (SIP) packets.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT- 77853: Verify Inspection of malformed SIP packets [PIX, ASA]

Description
The inspection of a malformed SIP packet may crash Cisco PIX and ASA appliances. In order to trigger this vulnerability, SIP fixup (for 6.x software) or inspect (for 7.x software) feature must be enabled. SIP fixup (in 6.x and earlier) and SIP inspection (in 7.x and later) are enabled by default. Note that SIP can use TCP and UDP as transport protocol. When UDP protocol is used, spoofing SIP messages is possible.

Applicable Platforms
Cisco PIX and ASA Firewalls
Impact
Successful exploitation of the first three vulnerabilities listed in this Advisory may crash the affected device. Repeated exploitation can result in a sustained DoS attack. Successful exploitation of CSCsh33287 can result in the escalation of user privileges and complete compromise of the affected Cisco PIX and ASA Appliances.

Suggested Fix
Disabling SIP inspection will prevent Cisco PIX and ASA Appliances from being vulnerable to the issue listed in this Advisory. However, this may have a negative impact on end devices terminating SIP sessions. Devices which terminate SIP sessions could be exposed to packets that may cause these devices to crash or become compromised. If you run a 7.x software release, the alternative is to only allow traffic from trusted hosts. The configuration needed to accomplish this is as follows:

```plaintext
access-list sip-acl extended permit udp 10.1.1.0 255.255.255.0 host 192.168.5.4 eq sip
access-list sip-acl extended permit udp host 192.168.5.4 10.1.1.0 255.255.255.0 eq sip
class-map sip-traffic
match access-list sip-acl
!
!
policy-map global_policy
class inspection_default inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras inspect rsh inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect netbios
inspect tftp
class sip-traffic
inspect sip
!

service-policy global_policy global
```
In this example, the SIP endpoints are any host within the 10.1.1.0 network (inside the trusted network) and a host with the IP address of 192.168.5.4 (outside of the trusted network). You have to substitute these IP addresses with the ones that are used in your network. Note that SIP is an UDP-based protocol, so spoofing SIP messages is possible.
PIX Instant Message Inspection Vulnerability - 105444 [PIX, ASA]

Description
A vulnerability exists in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances. This security advisory outlines details of the vulnerability:

Instant Messenger Inspection Vulnerability

The Instant Messenger Inspection Vulnerability may lead to a denial of service (DoS) condition.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT- 105444: Verify Instant Message Inspection Vulnerability [PIX, ASA]

Description
Cisco ASA and Cisco PIX devices are affected by a crafted packet vulnerability if Instant Messaging Inspection is enabled and the device is running software versions prior to 7.2(4) on the 7.2.x release, 8.0(3)10 on the 8.0.x release, or 8.1(1)2 on the 8.1.x release. Devices running software versions in the 7.0.x and 7.1.x releases are not vulnerable. Additionally, devices that do not have Instant Messaging Inspection enabled are not vulnerable.

Note: Instant Messaging Inspection is disabled by default.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the this vulnerabilities may cause a reload of the affected device. Repeated exploitation could result in a sustained Denial-of-Service (DoS) condition.

Suggested Fix
The only workaround for this vulnerability is to disable IM inspection on the security appliance.

PIX LDAP Authentication Bypass - 82451 [PIX, ASA]

Description
The Lightweight Directory Access Protocol (LDAP) authentication bypass vulnerabilities are caused by a specific processing path followed when the device is setup to use a Lightweight Directory Access Protocol (LDAP) authentication server. These vulnerabilities may allow unauthenticated users to access either the internal network or the device itself.
Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT- 82451: Verfiy PIX LDAP Authentication bypass vulnerability [PIX, ASA]

Description
The Lightweight Directory Access Protocol (LDAP) authentication bypass vulnerabilities are caused by a specific processing path followed when the device is setup to use a Lightweight Directory Access Protocol (LDAP) authentication server. These vulnerabilities may allow unauthenticated users to access either the internal network or the device itself. Devices configured to use a LDAP authentication server and use an authentication protocol other than PAP may be vulnerable. The LDAP server is specified in the configuration via the `aaa-server ldap server host <ip address>` command line interface (CLI) configuration command. The authentication protocol is specified via the `authentication <protocol>` command within the `tunnel-group <tunnel-group> ppp-attributes` section of the configuration.

Applicable Platforms
Cisco PIX and ASA Firewalls
Impact
Cisco ASA and PIX devices leveraging LDAP AAA servers for authentication of terminating L2TP IPSec tunnels or remote management sessions may be vulnerable to an authentication bypass attack. See the following bullets for more details:

- Layer 2 Tunneling Protocol (L2TP) Devices terminating L2TP IPSec tunnels must be configured to use LDAP in conjunction with CHAP, MS-CHAPv1, or MS-CHAPv2 authentication protocols to be vulnerable. If LDAP authentication is used in conjunction with PAP, the device is not vulnerable to the LDAP L2TP authentication bypass.
- Remote Management Access
Cisco ASA and PIX devices leveraging LDAP AAA servers for authentication of management sessions (telnet, SSH and HTTP) may be vulnerable to an authentication bypass attack. Access for management sessions must be explicitly enabled and is limited to the defined source IP address within the device configuration.

Suggested Fix
The following workarounds may be a useful reference for some customers to mitigate the LDAP authentication bypass vulnerabilities.

- L2TP
For Cisco ASA or PIX devices configured to use a LDAP authentication server for L2TP over IPSec connections, configuring the device to use PAP as an authentication protocol may mitigate this vulnerability. It is important to note that PAP transmits passwords in clear-text. PAP authentication is encrypted via IPSec when it is used for the L2TP connection. Communications between the security appliance and the LDAP server are not encrypted by default and can be secured with SSL using the `ldap-over-ssl` command. Configuration of PAP authentication can be done using the following example as a guide or by referring to the security appliance configuration guides listed:

```
ciscoasa#configure terminal
ciscoasa(config)#tunnel-group l2tp_group ppp-attributes
ciscoasa(config-ppp)#authentication pap
```
```
ciscoasa(config-ppp)#no authentication ms-chap-v1
ciscoasa(config-ppp)#no authentication ms-chap-v2
```
```
ciscoasa(config-ppp)#no authentication chap
```

- Remote Management Cisco ASA or PIX devices that authenticate remote management sessions with either the local database or an AAA server other than a LDAP server are not affected by this vulnerability. More information on changing the AAA server protocol used with remote management sessions is available at the following link: [http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_2/conf_gd/sysadmin/mgaccess.htm](http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_2/conf_gd/sysadmin/mgaccess.htm). Remote management sessions must be explicitly enabled before the Cisco ASA or PIX will accept sessions. The source IP addresses are defined within the command that enables remote management access.
Below are examples of enabling remote management sessions (Note that other commands are required, but these commands control the source IP address of the device that is allowed access to the Cisco ASA or PIX device): For remote telnet, ssh and http access:

```
ciscoasa#configure terminal
ciscoasa(config)#telnet source_IP_address mask source_interface
ciscoasa(config)#ssh source_IP_address mask source_interface
ciscoasa(config)#http source_IP_address mask source_interface
```

**PIX Mailguard - 13636 [PIX, ASA]**

**Description**
The Cisco Secure PIX firewall feature "mailguard," which limits SMTP commands to a specified minimum set of commands, can be bypassed.

This vulnerability can be exploited to bypass SMTP command filtering.

This vulnerability has been assigned Cisco bug ID CSCdr91002 and CSCds30699.

A new aspect of this vulnerability has been assigned Cisco bug ID CSCds38708.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PIX PSIRT- 13636: Verfiy mailguard vulnerability [PIX, ASA]
Description
The behavior is a failure of the command **fixup protocol smtp [portnum]**, which is enabled by default on the Cisco Secure PIX Firewall.

If you do not have protected Mail hosts with the accompanying configuration (configuration example below) you are not affected by this vulnerability.

To exploit this vulnerability, attackers must be able to make connections to an SMTP mail server protected by the PIX Firewall. If your Cisco Secure PIX Firewall has configuration lines similar to the following:

```
fixup protocol smtp 25
```

and either

```
conduit permit tcp host 192.168.0.1 eq 25 any
```

or

```
conduit permit tcp 192.168.0.1 255.255.255.0 eq 25 any
```

or

```
access-list 100 permit tcp any host 192.168.0.1 eq 25 access-group 100 in interface outside
```

The expected filtering of the Mailguard feature can be circumvented by an attacker.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
The Mailguard feature is intended to help protect weakly secured mail servers. The workaround for this issue is to secure the mail servers themselves, or upgrade to fixed PIX firewall code.

In order to exploit this vulnerability, an attacker would need to also exploit the mailserver that is currently protected by the PIX. If that server is already well configured, and has the latest security patches and fixes from the SMTP vendor, that will minimize the potential for exploitation of this vulnerability.

Suggested Fix
There is not a direct work around for this vulnerability. The potential for exploitation can be lessened by ensuring that mail servers are secured without relying on the PIX functionality.

**PIX Multiple SSH Vulnerabilities - 8118 [PIX, ASA]**

Description
Four different Cisco product lines are susceptible to multiple vulnerabilities discovered in the Secure Shell (SSH) protocol version 1.5. These issues have been addressed, and fixes have been integrated into the Cisco products that support this protocol.

By exploiting the weakness in the SSH protocol, it is possible to insert arbitrary commands into an established SSH session, collect information that may help in brute force key recovery, or brute force a session key.

Applicable Platforms
Cisco PIX and ASA Firewalls
References

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT- 8118: Verfiy PIX Multiple SSH Vulnerabilities [PIX, ASA]

Description
An implementation of SSH in multiple Cisco products are vulnerable to three different vulnerabilities. These vulnerabilities are:

• **CRC-32 integrity check vulnerability** -- This vulnerability has been described in a CORE SDI S.A. paper entitled "An attack on CRC-32 integrity checks of encrypted channels using CBC and CFB modes". In order for this attack to succeed, an attacker must possess one or two known ciphertext/plaintext pairs. This should not be difficult since every session starts with a greeting screen which is fixed and which can be determined. This also implies that an attacker must be somewhere along the session path in order to be able to sniff the session and collect corresponding ciphertext. While fixing this vulnerability, we have not made the implementation mistake described by VU#945216 (see http://www.kb.cert.org/vuls/id/945216) which is being actively exploited.

• **Traffic analysis** -- This issue has been described in an analysis jointly made by Dug Song and Solar Designer. It can be found at: http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt, and is entitled "Passive Analysis of SSH (Secure Shell) Traffic". To exploit this vulnerability, an attacker must be able to capture packets. When sending a packet using the SSH protocol, it is padded to the next 8-byte boundary, but the exact length of the data (without the padding) is sent unencrypted. The timing between packets may yield additional information, such as the relative position of a letter on the keyboard, but that depends on overall jitter in the network and the typing habits of the person. For additional information, please see http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt.

• **Key recovery in SSH protocol 1.5** -- This has been discovered by CORE SDI S.A. and the paper describing it can be viewed at: http://www.securityfocus.com/archive/1/161150. The subject line is "SSH protocol 1.5 session key recovery vulnerability". In order to exploit this vulnerability, an attacker must be able to sniff the SSH session and be able to establish a connection to the SSH server. In order to recover the server key, an attacker must perform an additional $2^{20}+2^19=1572864$ connections. Since the key has a lifespan of about an hour, this means that an attacker must perform around 400 connections per second. For further details, please see http://www.securityfocus.com/archive/1/161150.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact

• **CRC-32 integrity check vulnerability** -- By exploiting this protocol weakness, the attacker can insert arbitrary commands in the session after the session has been established.

• **Traffic analysis** -- This vulnerability exposes the exact lengths of the passwords used for login authentication. This is only applicable to an interactive session that is being established over the tunnel protected by SSH. This can significantly help an attacker in guessing the password using the brute force attack.
• **Key recovery in SSH protocol 1.5** - This vulnerability may lead to the compromise of the session key. Once the session key is determined, the attacker can proceed to decrypt the stored session using any implementation of the crypto algorithm used. This will reveal all information in an unencrypted form.

**Suggested Fix**
There are no workarounds for these vulnerabilities.

### PIX OpenSSL Implementation DoS Vulnerability - 45643 [PIX, ASA]

#### Description
An affected network device running an SSL server based on an affected OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client. The network device may be vulnerable to this vulnerability even if it is configured to not authenticate certificates from the client.

See "SSL Implementation Vulnerabilities." at Cisco Security Advisories website

#### Applicable Platforms
Cisco PIX and ASA Firewalls

#### References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

### Rule 1

#### Rule
PIX PSIRT-45643: Verify SSL Implementation Vulnerabilities [PIX, ASA]

#### Description
An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client. The network device is vulnerable to this vulnerability even if it is configured to not authenticate certificates from the client.

#### Applicable Platforms
Cisco PIX and ASA Firewalls

#### Impact
An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client regardless of whether it is configured to process client certificates or not.

#### Suggested Fix
The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code as soon as it is available.
• Restrict access to the HTTPS server on the network device. Allow access to the network device only from trusted workstations by using access lists / MAC filters that are available on the affected platforms.

• Disable the SSL server / service on the network device. This workaround must be weighed against the need for secure communications with the vulnerable device.

Cisco SIP Proxy Server (SPS) - Disable SSL/TLS functionality. One can do this using the Provisioning GUI. Log in, then select Farm/Proxies from the Configuration options. Select Advanced, and then the SIP Server Core tab. Turn the Enable TLS directive to Off.

PIX OpenSSL Implementation Vulnerability - 49898[PIX, ASA]

Description
An affected network device running an SSL server based on an affected OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack... See "Cisco OpenSSL Implementation Vulnerability." at Cisco Security Advisories website

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT- 49898: Verify OpenSSL Implementation Vulnerability [PIX, ASA]

Description
Secure Sockets Layer (SSL), is a protocol used to encrypt the data transferred over a TCP session. SSL in Cisco products is mainly used by the HyperText Transfer Protocol Secure (HTTPS) web service for which the default TCP port is 443. The affected products, listed above, are only vulnerable if they have the HTTPS service enabled and the access to the service is not limited to trusted hosts or network management workstations. They are not vulnerable to transit traffic, only traffic that is destined to them may exploit this vulnerability.

To check if the HTTPS service is enabled one can do the following:
1. Check the configuration on the device to verify the status of the HTTPS service.
2. Try to connect to the device using a standard web browser that supports SSL using a URL similar to https://ip_address_of_device/.
3. Try and connect to the default HTTPS port, TCP 443, using Telnet. telnet ip_address_of_device 443. If the session connects the service is enabled and accessible.

Applicable Platforms
Cisco PIX and ASA Firewalls
Impact
An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack.

Suggested Fix
The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code as soon as it is available.

- Restrict access to the HTTPS server on the network device. Allow access to the network device only from trusted workstations by using access lists / MAC filters that are available on the affected platforms.
- Disable the SSL server / service on the network device. This workaround must be weighed against the need for secure communications with the vulnerable device.

PIX Potential Information Disclosure in Clientless VPNs - 107475 [PIX, ASA]

Description
Potential Information Disclosure in Clientless VPNs exist in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances that may result in a reload of the device or disclosure of confidential information.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT- 107475: Verify Potential Information Disclosure in Clientless VPNs Vulnerability [PIX, ASA]
Description

Potential Information Disclosure in Clientless VPNs

Cisco ASA devices that terminate clientless remote access VPN connections are vulnerable to potential information disclosure if the device is running affected 8.0 or 8.1 software versions. Cisco ASA devices running software versions 7.0, 7.1, or 7.2 are not affected by this vulnerability. Cisco ASA devices running software versions prior to 8.0(3)15 and 8.1(1)4, or after 8.0(3)16 and 8.1(1)5 are also not affected by this vulnerability.

On Cisco ASA devices configured to terminate clientless VPN connections, an attacker may be able to discover potentially sensitive information such as usernames and passwords. This attack requires an attacker to convince a user to visit a rogue web server, reply to an e-mail, or interact with a service to successfully exploit the vulnerability.

Cisco ASA devices running software versions 8.0 or 8.1 with clientless VPNs enabled may be affected by this vulnerability. Cisco ASA devices running that run software versions 7.0, 7.1, or 7.2 are not vulnerable to this vulnerability.

Clientless SSL VPN connections are enabled via the `webvpn` command. For example, the following configuration shows a Cisco ASA device with Clientless VPNs configured and enabled. In this case the Cisco ASA device will listen for VPN connections on the default port, TCP port 443:

```
http server enable
!
webvpn
enable outside
```

Note that with this particular configuration, the device is vulnerable to attacks coming from the outside interface due to the `enable outside` command within the webvpn group configuration.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact

The Potential Information Disclosure in Clientless SSL VPNs vulnerability may allow an attacker to obtain user and group credentials if the user interacts with a rogue system or document.

Suggested Fix

Client based VPN connections are not vulnerable to the information disclosure vulnerability. If you are running 8.0(3)15, 8.0(3)16, 8.1(1)4, or 8.1(1)5, you may safely use client based VPN connections as an alternative to clientless VPNs.

PIX Privilege escalation - 77853 [PIX, ASA]

Description

Vulnerability is found in Cisco PIX 500 Series Security Appliances and the Cisco ASA 5500 Series Adaptive Security Appliances that affects privilege escalation.

Applicable Platforms
Cisco PIX and ASA Firewalls
References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT- 77853: Verify Privilege escalation [PIX, ASA]

Description
Using the LOCAL method for user authentication may result in privilege escalation. In order to exploit this vulnerability, a user must be defined in the local database with a privilege of zero and be able to successfully authenticate to the affected device. Only if these conditions are met can the user escalate assigned privileges to level 15 and become an administrator. After that, the user can change every aspect of the configuration and operation of the device. A device is vulnerable to this issue if these lines are present in the device's configuration:

```
pixfirewall(config)# aaa authentication enable console LOCAL
pixfirewall(config)# username xxxxx password xxxxxx privilege 0
```

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the vulnerability described in this advisory will result in a reload of the affected device. Repeated exploitation can result in a sustained denial of service (DoS) condition.

Suggested Fix
There are two workarounds for this vulnerability. One consists of the use of TACACS+ or Radius for authentication, and another is to change the minimum privilege of the user from zero to one. Use TACACS+ or Radius for authentication. Do not use the LOCAL method for user authentication, but use TACACS+ or Radius instead. This example shows how to configure the Cisco PIX appliance to use TACACS+ or Radius to authenticate Secure Shell (SSH) access to the device.

```
pixfirewall(config)#aaa-server AuthOutbound protocol radius (or tacacs+)
pixfirewall(config)#aaa authentication ssh console AuthOutbound
pixfirewall(config)#aaa-server AuthOutbound host 10.0.0.1 radius_key
```

In this example, 10.0.0.1 is the IP address of the Radius server and radius_key is the shared key between the Radius server and the appliance. More information on how to configure TACACS+ or Radius on Cisco PIX and ASA appliances can be found at


Changing user's minimum privilege level

The second workaround consists of the change of the user minimum privilege level from zero to one.
In that case, your configuration may look like this:

```
 pixfirewall(config)# aaa authentication enable console LOCAL
 pixfirewall(config)# username xxxxx password xxxxxx privilege 1
```

It is possible to use any other level as long as it is not zero or 15. If it is 15, the user has all privileges, and that is what we want to avoid in the first place.

**PIX SMTP - 15235 [PIX, ASA]**

**Description**
The Cisco Secure PIX firewall feature "mailguard" which limits SMTP commands to a specified minimum set of commands can be bypassed.

This vulnerability can be exploited to bypass SMTP command filtering.

This vulnerability has been assigned Cisco bug ID CSCdu47003.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's Worldwide Web server, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PIX PSIRT- 15235: Verfiy SMTP vulnerability [PIX, ASA]

**Description**
The behavior is a failure of the command `fixup protocol smtp [portnum]`, which is enabled by default on the Cisco Secure PIX Firewall. If you do not have protected Mail hosts with the accompanying configuration (configuration example below) you are not vulnerable to the attack.
To exploit this vulnerability, attackers must be able to make connections to an SMTP mail server protected by the PIX Firewall. If your Cisco Secure PIX Firewall has configuration lines similar to the following:

```plaintext
fixup protocol smtp 25
```

and either

```plaintext
conduit permit tcp host 192.168.0.1 eq 25 any
```

or

```plaintext
conduit permit tcp 192.168.0.1 255.255.255.0 eq 25 any
```

or

```plaintext
access-list 100 permit tcp any host 192.168.0.1 eq 25
access-group 100 in interface outside
```

The expected filtering of the Mailguard feature can be circumvented by an attacker.

### Applicable Platforms
Cisco PIX and ASA Firewalls

### Impact
If the mail server itself is not properly secured, an attacker may be able to collect information about existing e-mail accounts and aliases, or may be able to execute arbitrary code on the mail server. In order to exploit this vulnerability, an attacker would need to also exploit the mailserver that is currently protected by the PIX. If that server is already well configured, and has the latest security patches and fixes from the SMTP vendor, that will minimize the potential for exploitation of this vulnerability.

Please note that Cisco strongly recommends that security on all servers, workstations and network infrastructure gear is maintained as part of Standard Operating Procedures. Internet Firewalls do not protect against risk factors internal to a Firewalled network such as social engineering, rogue internal users or additional external access points to the internal network (i.e. modem pools or network fax machines) and as such should not be viewed as the only security measure necessary to ensure network integrity.

### Suggested Fix
There is not a direct workaround for this vulnerability. The potential for exploitation can be lessened by ensuring that mail servers are secured without relying on the PIX functionality

---

**PIX SNMP - 19296 [PIX, ASA]**

### Description
Multiple Cisco products contain vulnerabilities in the processing of Simple Network Management Protocol (SNMP) messages. These vulnerabilities can be repeatedly exploited to produce a denial of service. In most cases, workarounds are available that may mitigate the impact. Some of these vulnerabilities are identified by various groups as VU#617947, VU#107186, OUSPG #0100, CAN-2002-0012, and CAN-2002-0013.

See [Cisco non-IOS Malformed SNMP Message-Handling Vulnerability](https://security advisories website). at Cisco Security Advisories website

### Applicable Platforms
Cisco PIX and ASA Firewalls
References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT- 19296: Verfiy For Vulnerabilities In Malformed SNMP Message-Handling [PIX, ASA]

Description
Malformed SNMP messages received by affected systems can cause various parsing and processing functions to fail, which may result in a system crash and reload (or reboot) in most circumstances. Some Cisco products may not reload but will become unresponsive instead. Some of the affected products are not directly vulnerable to malformed SNMP messages, but fail under extended testing or large volumes of SNMP messages due to memory leaks or other unrelated problems.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
The vulnerabilities can be exploited to produce a Denial of Service (DoS) attack. When the vulnerabilities are exploited, they can cause an affected Cisco product to crash and reload.

SNMP messages are transported using User Datagram Protocol (UDP) and are subject to IP source address spoofing which could be used to circumvent the access control mechanisms.

If an attacker is able to guess or otherwise obtain a read-only community string for an affected device, then he or she could bypass SNMP access control relying on the community string.

Suggested Fix
Customers should review configuration for lines such as the following: snmp-server host outside ip-address which would permit SNMP queries from the unprotected interface. If they find these commands in the configuration, they should carefully evaluate the necessity for them and the protection offered by other devices upstream to ensure that spoofing of the SNMP host cannot take place.

Disable SNMP. You can do this by removing all snmp-server host commands.

no snmp-server host inside ip-address
no snmp-server host inside ip-address
no snmp-server location
no snmp-server contact
no snmp-server community community-string
no snmp-server enable traps

Note: Other PIX SNMP commands including the snmp-server community may still appear in the PIX configuration after the no snmp-server host ... command has been executed.
PIX SNMPv3 - 47284 [PIX, ASA]

Description
This advisory documents two vulnerabilities for the Cisco PIX firewall. These vulnerabilities are documented as CSCeb20276 (SNMPv3) and CSCec20244 (VPNC).

There are workarounds available to mitigate the effects of CSCeb20276 (SNMPv3). No workaround is available for CSCec20244 (VPNC).

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT- 47284: Verify SNMPv3 vulnerability[PIX, ASA]

Description
- **CSCeb20276 (SNMPv3)**
  
  The Cisco PIX firewall crashes and reloads while processing a received SNMPv3 message when `snmp-server host <if_name> <ip_addr> or snmp-server host <if_name> <ip_addr> poll` is configured on the Cisco PIX firewall. This happens even though the Cisco PIX firewall does not support SNMPv3.
  
  A Cisco PIX firewall configured to only generate and send traps using the `snmp-server host <if_name> <ip_addr> trap` command is not vulnerable.

- **CSCec20244 (VPNC)**
  
  Under certain conditions an established VPNC IPSec tunnel connection is dropped if another IPSec client attempts to initiate an IKE Phase I negotiation to the outside interface of the VPN Client configured Cisco PIX firewall.
  
  Only a Cisco PIX firewall configured as a VPN Client is vulnerable to this vulnerability. A device reload of the VPN Client configured PIX is required to recover from this unstable state. No action is required on the headend VPN concentrator.
  
  A VPNC, also referred to as Easy VPN or ezVPN, connection is created when the Cisco PIX firewall is used as a VPN client to connect to a VPN server. An IKE Phase I negotiation is a step in the establishment of an IPSec session. CSCec20244 resolved this issue for the 6.2 (3.100) and later software releases.

  These vulnerabilities are documented in the CiscoBug Toolkit as Bug ID CSCeb20276 (SNMPv3) and CSCec20244 (VPNC). To access this tool, you must be a registered user and you must be logged in.

Applicable Platforms
Cisco PIX and ASA Firewalls
Impact

- **CSCeb20276 (SNMPv3)**
  This vulnerability can be exploited to initiate a Denial of Service attack on the Cisco PIX firewall.

- **CSCec20244 (VPNC)**
  This vulnerability can be exploited to initiate a Denial of Service attack on sessions established between a Cisco PIX configured as a VPN Client and a VPN server.

**Suggested Fix**
Disable the SNMP server on the Cisco PIX firewall.

**PIX SSH - 24862 [PIX, ASA]**

**Description**
While fixing vulnerabilities mentioned in the Cisco Security Advisory: Multiple SSH Vulnerabilities Cisco has inadvertently introduced an instability in some products. When an attacker tries to exploit the vulnerability VU#945216 (described in the CERT/CC Vulnerability Note at http://www.kb.cert.org/vuls/id/945216) the SSH module will consume too much of the processor's time, effectively causing a DoS. In some cases the device will reboot. In order to be exposed SSH must be enabled on the device.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PIX PSIRT- 24862: Verify Scanning For SSH Can Cause a Crash Vulnerability[PIX, ASA]

**Description**
While fixing the vulnerabilities an instability is introduced in some products. When exposed to an overly large packet, the SSH process will consume a large portion of the processor's instruction cycles, effectively causing a DoS. The capability to create such a packet is available in publicly available exploit code. In some cases this availability attack may result in a reboot of the device. In order to be exposed SSH must be enabled on the device.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**Impact**
By repeatedly exploiting this vulnerability an attacker can cause a denial of service, though Cisco products remain unaffected to the exploits that are trying to exploit vulnerabilities.
Suggested Fix
It is possible to mitigate this vulnerability in two ways:
Block all SSH connections on the border on your network, or
On each individual device allow SSH connections only from the required IP addresses and block all others.

PIX SSL VPN DOS - 82451 [PIX, ASA]

Description
The two DoS vulnerabilities may be triggered when devices are terminating Virtual Private Networks (VPN). These denial of service vulnerabilities may allow an attacker to disconnect VPN users, prevent new connections, or prevent the device from transmitting traffic.
Cisco ASAs using clientless SSL VPNs are vulnerable to a denial of service attack via the SSL VPN HTTP server. A successful attack must exploit a race condition in the processing non-standard SSL sessions and may result in a reload of the device.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT -82541: Verify SSL VPN DOS Vulnerability [PIX, ASA]

Description
The two DoS vulnerabilities may be triggered when devices are terminating Virtual Private Networks (VPN). These denial of service vulnerabilities may allow an attacker to disconnect VPN users, prevent new connections, or prevent the device from transmitting traffic.
Cisco ASAs using clientless SSL VPNs are vulnerable to a denial of service attack via the SSL VPN HTTP server. A successful attack must exploit a race condition in the processing non-standard SSL sessions and may result in a reload of the device.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Cisco ASAs using clientless SSL VPNs are vulnerable to a denial of service attack via the SSL VPN HTTP server. A successful attack must exploit a race condition in the processing non-standard SSL sessions and may result in a reload of the device.

Suggested Fix
If clientless SSL VPNs are used, there is no workaround for the SSL VPN vulnerability. Client-based VPNs are not affected, and may be used as an alternative to the clientless VPN connections.
More information on configuring clientless SSL VPNs on the ASA is available in the configuration example at the following link:

**PIX SSL VPN Memory Leak Vulnerability - 107475 [PIX, ASA]**

**Description**
SSL VPN Memory Leak Vulnerability exist in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances that may result in a reload of the device or disclosure of confidential information.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT -107475: Verfiy SSL VPN Memory Leak Vulnerability [PIX, ASA]

**Description**
SSL VPN Memory Leak Vulnerability
Cisco ASA devices that terminate clientless remote access VPN connections are vulnerable to a denial of service attack affecting the SSL processing software if the device is running a software version prior to 7.2(4)2, 8.0(3)14, or 8.1(1)4. Cisco ASA devices that run software versions 7.0 and 7.1 are not affected by this vulnerability.

A crafted SSL or HTTP packet may cause a denial of service condition on a Cisco ASA device that is configured to terminate clientless VPN connections. A successful attack may result in a reload of the device.

Cisco ASA devices that run versions 7.2, 8.0, or 8.1 with clientless SSL VPNs enabled may be affected by this vulnerability. Devices that run software versions 7.0 and 7.1 are not affected by this vulnerability.

Clientless VPN, SSL VPN Client, and AnyConnect connections are enabled via the webvpn command. For example, the following configuration shows a Cisco ASA with Clientless VPNs configured and enabled. In this case the ASA will listen for VPN connections on the default port, TCP port 443:

```
http server enable
!
webvpn
   enable outside
```

Note that with this particular configuration, the device is vulnerable to attacks coming from the outside interface due to the enable outside command within the webvpn group configuration.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**Impact**
Successful exploitation of the SSL VPN Memory Leak Vulnerability may result in the device reloading. This can be repeatedly exploited and may lead to a denial of service attack.

**Suggested Fix**
IPSec clients are not vulnerable to this issue and may be used in conjunction with strong group credentials until the device can be upgraded.

**PIX Scan Denial of Service Vulnerability - 105444 [PIX, ASA]**

**Description**
A vulnerability exists in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances. This security advisory outlines details of the vulnerability:

**Vulnerability Scan Denial of Service**
Vulnerability Scan Denial of Service may lead to a denial of service (DoS) condition.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT -105444: Verfiy Scan Denial of Service Vulnerability [PIX, ASA]

**Description**

**Vulnerability Scan Denial of Service**
Cisco ASA and Cisco PIX devices are affected by a vulnerability (port) scan denial of service vulnerability if the device is running software versions prior to 7.2(3)2 on the 7.2.x release or 8.0(2)17 on the 8.0.x release. Cisco ASA and Cisco PIX devices running software versions 7.0.x, 7.1.x, or 8.1.x are not vulnerable.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**Impact**
Successful exploitation of this vulnerability may cause a reload of the affected device. Repeated exploitation could result in a sustained Denial-of-Service (DoS) condition.

**Suggested Fix**
There are no workarounds for this vulnerability.
PIX TCP Conn Reset - 50961 [PIX, ASA]

Description
A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer), and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, the attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain a TCP stack are susceptible to this vulnerability.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT -50961: Verify TCP connection reset vulnerabilities [PIX, ASA]

Description
TCP is the transport layer protocol designed to provide connection-oriented reliable delivery of a data stream. To accomplish this, TCP uses a mixture of flags to indicate state and sequence numbers to identify the order in which the packets are to be reassembled. TCP also provides a number, called an acknowledgement number, that is used to indicate the sequence number of the next packet expected. The packets are reassembled by the receiving TCP implementation only if their sequence numbers fall within a range of the acknowledgement number (called a "window"). The acknowledgement number is not used in a packet with the reset (RST) flag set because a reset does not expect a packet in return.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
The impact is different for each specific protocol. While, in the majority of cases, a TCP connection will be automatically re-established, in some specific protocols a second order of consequences may have a larger impact than tearing down the connection itself.

Suggested Fix
There are no workarounds available to mitigate the effects of this vulnerability. It is possible to mitigate the exposure on this vulnerability by applying anti-spoofing measures on the edge of the network.
PIX TCP Prevention - 68268 [PIX, ASA]

Description
TCP connections through the firewall may be silently blocked.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT -68268: Verify TCP prevention vulnerability [PIX, ASA]

Description
TCP connections through the firewall may be silently blocked. By sending a TCP SYN packet with an incorrect checksum through a PIX firewall, the PIX will block new TCP connections using the same source and destination TCP ports and IP addresses. Connections will remain blocked for approximately two minutes after which connections will be allowed. This behavior may be seen on all firewall interfaces but can be expected to have the most impact on TCP connections originating from higher security level interfaces.

Since the spoofed packets have an incorrect checksum, they are silently discarded by the destination and the firewall will not see a RST packet from either the destination or the legitimate source and will hold the embryonic connection open until the embryonic connection timeout which is 2 minutes by default.

The root cause is due to the spoofed packet creating an embryonic connection which sets up the TCP sliding window. A valid packet from a real host using the same connection as the spoofed packet sends a SYN over the same connection. The sequence number of the valid packet is out-of-window and rejected by the firewall's TCP sequence number check. Any subsequent retransmissions of the valid packet are also out-of-window and are rejected by TCP sequence number check.

Other spoofed TCP SYN packets that create embryonic connections can also cause this behavior, blocking legitimate TCP connections until the embryonic connection times out.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
By sending a TCP SYN packet with an invalid checksum through a PIX firewall, the PIX will block new TCP connections using the same source and destination TCP ports and IP addresses. Connections will remain blocked until the embryonic connection timeout which is 30 seconds by default. Also, PIX software version 6.3 does not verify the TCP checksum of packets transiting through the firewall. Because the PIX does not verify the TCP checksum, the malformed TCP packet is allowed through the firewall in a half-opened, embryonic state.
Suggested Fix
Issuing the commands clear xlate or clear local-host will allow the firewall to pass connections again.

**PIX TCP Reset - 13639 [PIX, ASA]**

**Description**
The Cisco Secure PIX Firewall cannot distinguish between a forged TCP Reset (RST) packet and a genuine TCP RST packet. Any TCP/IP connection established through the Cisco Secure PIX Firewall can be terminated by a third party from the untrusted network if the connection can be uniquely determined. This vulnerability is independent of configuration. There is no workaround.

This vulnerability exists in all Cisco Secure PIX Firewall software releases up to and including 4.2(5), 4.4(4), 5.0(3) and 5.1(1). The defect has been assigned Cisco bug ID CSCdr11711.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com
- firewalls@lists.gnac.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PIX PSIRT -13639: Verify TCP reset vulnerability [PIX, ASA]
Description

When the Cisco Secure PIX Firewall receives a TCP Reset (RST) packet, it evaluates that packet based on data contained in the TCP packet header: source IP address, source port, destination IP address, and destination port. If these four values match an entry in the stateful inspection table, the associated connection will be reset. This affects only TCP sessions. Data exchange based on any other protocol is not affected.

To exploit this vulnerability, an attacker would need to have or infer:

- Detailed knowledge of the connection table in the Cisco Secure PIX Firewall prior to launching the attack, or
- Detailed knowledge of the source and destination IP Address and ports associated with a particular connection to be attacked

This particular vulnerability only affects the connection table (which keeps state regarding the connections being made through the device). It does not affect the translation table (in which address mappings are stored).

Cisco Secure PIX Firewall software has been fixed so that it now checks for a valid sequence number before removing a connection from the connection state table.

Applicable Platforms

Cisco PIX and ASA Firewalls

Impact

Any Cisco Secure PIX Firewall that provides external access to the Internet and for which all of the preceding conditions are met is vulnerable to the disruption of individual sessions.

Suggested Fix

There are no workarounds for this defect. Customers are urged to upgrade to the versions of code containing the fix.

PIX Time-to-Live Vulnerability - 100314 [PIX, ASA]

Description

A crafted IP packet vulnerability exists in the Cisco PIX 500 Series Security Appliance (PIX) and the Cisco 5500 Series Adaptive Security Appliance (ASA) that may result in a reload of the device. This vulnerability is triggered during processing of a crafted IP packet when the Time-to-Live (TTL) decrement feature is enabled. Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0028 has been assigned to this vulnerability.

Applicable Platforms

Cisco PIX and ASA Firewalls

References

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Rule 1

Rule
PIX PSIRT -100314: Verfiy Time-to-Live Vulnerabiltiy [PIX, ASA]

Description
A crafted IP packet vulnerability exists in the Cisco PIX 500 Series Security Appliance (PIX) and the Cisco 5500 Series Adaptive Security Appliance (ASA) that may result in a reload of the device. This vulnerability is triggered during processing of a crafted IP packet when the Time-to-Live (TTL) decrement feature is enabled.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the vulnerability described in this advisory will result in a reload of the affected device. Repeated exploitation can result in a sustained denial of service (DoS) condition.

Suggested Fix
Disable the TTL decrement feature using the no set connection decrement-ttl command in class configuration mode.

PIX Traceback When Processing Malformed SIP Requests - 107475[PIX, ASA]

Description
Traceback when processing malformed SIP requests exist in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances that may result in a reload of the device or disclosure of confidential information.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Description
Traceback when processing malformed SIP requests
Cisco PIX and Cisco ASA devices configured for SIP inspection are vulnerable to multiple processing errors that may result in denial of service attacks. Cisco PIX and ASA software versions prior to 7.0(7)16, 7.1(2)71, 7.2(4)7, 8.0(3)20, and 8.1(1)8 are vulnerable to these SIP processing errors.
Cisco PIX and Cisco ASA devices configured for SIP inspection are vulnerable to multiple processing errors that may result in denial of service attacks. All Cisco PIX and Cisco ASA software releases may be vulnerable to these SIP processing vulnerabilities. A successful attack may result in a reload of the device.
SIP inspection is enabled with the `inspect sip` command.
To determine whether the Cisco PIX or Cisco ASA security appliance is configured to support inspection of sip packets, log in to the device and issue the CLI command `show service-policy | include sip`. If the output contains the text `Inspect: sip` and some statistics, then the device has a vulnerable configuration.

The following example shows a vulnerable Cisco ASA Security Appliance:

```
asa#show service-policy | include sip
   Inspect: sip, packet 0, drop 0, reset-drop 0

asa#
```

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the Erroneous SIP Processing Vulnerabilities may result in the device reloading. This can be repeatedly exploited and may lead to a denial of service attack.

Suggested Fix
SIP inspection should be disabled if it is not needed and temporarily disabling the feature will mitigate the SIP processing vulnerabilities. SIP inspection can be disabled with the command `no inspect sip`.

### PIX URI Processing Error Vulnerability in SSL VPNs - 107475 [PIX, ASA]

**Description**
URI Processing Error Vulnerability in SSL VPNs exist in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances that may result in a reload of the device or disclosure of confidential information.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Rule 1

Rule
PSIRT -107475: Verify URI Processing Error Vulnerability in SSL VPNs [PIX, ASA]

Description
Cisco ASA devices that terminate clientless remote access VPN connections are vulnerable to a denial of service attack in the HTTP server if the device is running software versions prior to 8.0(3)15, and 8.1(1)5. Cisco ASA devices that run software versions 7.0, 7.1, or 7.2 are not affected by this vulnerability.

A crafted SSL or HTTP packet may cause a denial of service condition on a Cisco ASA device that is configured to terminate clientless VPN connections. A successful attack may result in a reload of the device.

Cisco ASA devices that run versions 7.2, 8.0, or 8.1 with clientless SSL VPNs enabled may be affected by this vulnerability. Devices that run software versions 7.0 and 7.1 are not affected by this vulnerability.

Clientless VPN, SSL VPN Client, and AnyConnect connections are enabled via the webvpn command. For example, the following configuration shows a Cisco ASA with Clientless VPNs configured and enabled. In this case the ASA will listen for VPN connections on the default port, TCP port 443:

```
http server enable
!
webvpn
   enable outside
```

Note that with this particular configuration, the device is vulnerable to attacks coming from the outside interface due to the `enable outside` command within the webvpn group configuration.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the URI Processing Error Vulnerability in SSL VPNs may result in the device reloading. This can be repeatedly exploited and may lead to a denial of service attack.

Suggested Fix
IPSec clients are not vulnerable to this issue and may be used in conjunction with strong group credentials until the device can be upgraded.

PIX VPN Password Expiry - 82451 [PIX, ASA]

Description
The two DoS vulnerabilities may be triggered when devices are terminating Virtual Private Networks (VPN). These denial of service vulnerabilities may allow an attacker to disconnect VPN users, prevent new connections, or prevent the device from transmitting traffic.

Cisco ASAs using clientless SSL VPNs are vulnerable to a denial of service attack via the SSL VPN HTTP server. A successful attack must exploit a race condition in the processing non-standard SSL sessions and may result in a reload of the device.

Applicable Platforms
Cisco PIX and ASA Firewalls
Chapter 4 Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT -82451: Verify VPN Password Vulnerability [PIX, ASA]

Description
The two DoS vulnerabilities may be triggered when devices are terminating Virtual Private Networks (VPN). These denial of service vulnerabilities may allow an attacker to disconnect VPN users, prevent new connections, or prevent the device from transmitting traffic. A device may be affected by this vulnerability if the password-management command is present in the tunnel-group section, as shown in the following examples:

```
tunnel-group example_group general-attributes
  address-pool inside_addresses
  default-group-policy example_group
  password-management
```

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Cisco ASA and PIX devices terminating remote access VPN connections may be vulnerable to a DoS attack if the tunnel group is configured with password expiry. To exploit this vulnerability for IPSec VPN connections, an attacker would need to know the group name and group password. An attacker would not need this information for SSL VPN connections. A successful attack may result in a reload of the device.

Suggested Fix
Disabling password expiry for remote access users until a device can be updated with non-vulnerable code can prevent the exposure of this vulnerability. This can be accomplished by removing the password management entry in the general attributes of the tunnel group, as shown in the following example:

```
ciscoasa(config)#tunnel-group remote_access_group general-attributes
  password-management
```

Implementing this workaround will disable the password expiry feature, and users will not be forced to change their passwords.
PIX VPNC - 47284 [PIX, ASA]

Description
This advisory documents two vulnerabilities for the Cisco PIX firewall. These vulnerabilities are documented as CSCeb20276 (SNMPv3) and CSCec20244 (VPNC).

There are workarounds available to mitigate the effects of CSCeb20276 (SNMPv3). No workaround is available for CSCec20244 (VPNC).

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT -47284: Verify VPNC Vulnerability [PIX, ASA]

Description
This section provides detailed information about these vulnerabilities.

- **CSCeb20276 (SNMPv3)** The Cisco PIX firewall crashes and reloads while processing a received SNMPv3 message when `snmp-server host <if_name> <ip_addr> or snmp-server host <if_name> <ip_addr> poll` is configured on the Cisco PIX firewall. This happens even though the Cisco PIX firewall does not support SNMPv3. A Cisco PIX firewall configured to only generate and send traps using the `snmp-server host <if_name> <ip_addr> trap` command is not vulnerable.

- **CSCec20244 (VPNC)** Under certain conditions an established VPNC IPSec tunnel connection is dropped if another IPSec client attempts to initiate an IKE Phase I negotiation to the outside interface of the VPN Client configured Cisco PIX firewall. Only a Cisco PIX firewall configured as a VPN Client is vulnerable to this vulnerability. A device reload of the VPNC Client configured PIX is required to recover from this unstable state. No action is required on the headend VPN concentrator. A VPNC, also referred to as Easy VPN or ezVPN, connection is created when the Cisco PIX firewall is used as a VPN client to connect to a VPN server. An IKE Phase I negotiation is a step in the establishment of an IPSec session. CSCec20244 resolved this issue for the 6.2 (3.100) and later software releases.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
This section describes the impact of the issues described in this document.

- **CSCeb20276 (SNMPv3)** This vulnerability can be exploited to initiate a Denial of Service attack on the Cisco PIX firewall.

- **CSCec20244 (VPNC)** This vulnerability can be exploited to initiate a Denial of Service attack on sessions established between a Cisco PIX configured as a VPN Client and a VPN server.

Suggested Fix
No workaround. Please upgrade.
PIX/ASA ACL Bypass Vulnerability - 109974 [PIX, ASA]

**Description**
Access control list (ACL) bypass vulnerability exist in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PSIRT -109974: Verfiy ACL Bypass Vulnerability [PIX, ASA]

**Description**
Access lists have an implicit deny behavior that is applied to packets that have not matched any of the permit or deny ACEs in an ACL and reach the end of the ACL. This implicit deny is there by design, does not require any configuration and can be understood as an implicit ACE that denies all traffic reaching the end of the ACL. A vulnerability exists in the Cisco ASA and Cisco PIX that may allow traffic to bypass the implicit deny ACE.

Note: This behavior only impacts the implicit deny statement on any ACL applied on the device. Access control lists with explicit deny statements are not affected by this vulnerability. This vulnerability is experienced in very rare occasions and extremely hard to reproduce.

You can trace the lifespan of a packet through the security appliance to see whether the packet is operating correctly with the packet tracer tool. The **packet-tracer** command provides detailed information about the packets and how they are processed by the security appliance. If a command from the configuration did not cause the packet to drop, the **packet-tracer** command will provide information about the cause in an easily readable manner. You can use this feature to see if the implicit deny on an ACL is not taking effect.

The following example shows that the implicit deny is bypassed (result = ALLOW):

<output truncated>

...  
Phase: 2  
Type: ACCESS-LIST  
Subtype:  
Result: ALLOW  
Config:  
Implicit Rule  
Additional Information:  
Forward Flow based lookup yields rule:
in id=0x1a09d350, priority=1, domain=permit, deny=false
hits=1144595557, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the ACL bypass vulnerability may allow an attacker to access resources that should be protected by the Cisco ASA.

Suggested Fix
As a workaround, remove the access-group line applied on the interface where the ACL is configured and re-apply it. For example:

ASA(config)#no access-group acl-inside in interface inside
ASA(config)#access-group acl-inside in interface inside

In the previous example the access group called acl-inside is removed and reapplied to the inside interface. Alternatively, you can add an explicit deny ip any any line in the bottom of the ACL applied on that interface. For example:

ASA(config)#access-list 100 deny ip any any

In the previous example, an explicit deny for all IP traffic is added at the end of access-list 100.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.

PIX/ASA Crafted H.323 Packet DoS Vulnerability - 109974 [PIX, ASA]

Description

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Chapter 4  Using Compliance and Audit Manager Feature

Rule 1

Rule
PSIRT -109974: Verfiy Crafted H.323 Packet DoS Vulnerability [PIX, ASA]

Description
Crafted H.323 Packet DoS Vulnerability
Cisco ASA and Cisco PIX security appliances may experience a device reload that can be triggered by a series of crafted H.323 packets, when H.323 inspection is enabled. H.323 inspection is enabled by default. Cisco ASA and Cisco PIX software versions 7.0, 7.1, 7.2, 8.0, and 8.1 are affected by this vulnerability.

A crafted H.323 packet may cause a DoS condition on a Cisco ASA device that is configured with H.323 inspection. H.323 inspection is enabled by default. A successful attack may result in a reload of the device. A TCP three-way handshake is not needed to exploit this vulnerability.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
The Denial of Service (DoS) vulnerabilities may cause a reload of the affected device.

Suggested Fix
H.323 inspection should be disabled if it is not needed. Temporarily disabling the feature will mitigate this vulnerability. H.323 inspection can be disabled with the command `no inspect h323`

PIX/ASA Crafted HTTP Packet DoS Vulnerability - 109974 [PIX, ASA]

Description
Crafted HTTP packet denial of service (DoS) vulnerability exist in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances:

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT -109974: Verfiy Crafted HTTP Packet DoS Vulnerability [PIX, ASA]

Description
Crafted HTTP Packet DoS Vulnerability
Cisco ASA security appliances may experience a device reload that can be triggered by a series of crafted HTTP packets, when configured for SSL VPNs or when configured to accept Cisco Adaptive Security Device Manager (ASDM) connections. Only Cisco ASA software versions 8.0 and 8.1 are affected by this vulnerability.
A crafted SSL or HTTP packet may cause a DoS condition on a Cisco ASA device that is configured to terminate SSL VPN connections. This vulnerability can also be triggered to any interface where ASDM access is enabled. A successful attack may result in a reload of the device. A TCP three-way handshake is needed to exploit this vulnerability.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**Impact**
The Denial of Service (DoS) vulnerabilities may cause a reload of the affected device.

**Suggested Fix**
Devices configured for SSL VPN (clientless or client-based) or accepting ASDM management connections are vulnerable.

*Note:* IPSec clients are not vulnerable to this vulnerability.

If SSL VPN (clientless or client-based) is not used, administrators should make sure that ASDM connections are only allowed from trusted hosts.

To identify the IP addresses from which the security appliance accepts HTTPS connections for ASDM, configure the `http` command for each trusted host address or subnet. The following example, shows how a trusted host with IP address 192.168.1.100 is added to the configuration:

```
hostname(config)# http 192.168.1.100 255.255.255.255
```
PIX/ASA Crafted TCP Packet DoS Vulnerability - 109974 [PIX, ASA]

Description

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT -109974: Verfiy Crafted TCP Packet DoS Vulnerability [PIX, ASA]

Description
Crafted TCP Packet DoS Vulnerability
A crafted TCP packet may cause a memory leak on a Cisco ASA or Cisco PIX device. A successful attack may result in a sustained DoS condition. A Cisco ASA device configured for any of the following features is affected:

- SSL VPNs
- ASDM Administrative Access
- Telnet Access
- SSH Access
- cTCP for Remote Access VPNs
- Virtual Telnet
- Virtual HTTP
- TLS Proxy for Encrypted Voice Inspection
- Cut-Through Proxy for Network Access
- TCP Intercept

Note: This vulnerability may be triggered when crafted packets are sent to any TCP based service that terminates on the affected device. The vulnerability may also be triggered via transient traffic only if the TCP intercept features has been enabled. A TCP three-way handshake is not needed to exploit this vulnerability.

Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
The Denial of Service (DoS) vulnerabilities may cause a reload of the affected device.

Suggested Fix
There are no workarounds for this vulnerability.
**PIX/ASA IPv6 Denial of Service Vulnerability - 108009 [PIX, ASA]**

**Description**
IPv6 Denial of Service Vulnerability exists in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances.
Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate some of these vulnerabilities are available.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT -108009: Verfiy IPv6 Denial of Service Vulnerabilitiy [PIX, ASA]

**Description**
IP6 Denial of Service Vulnerability
A specially crafted IPv6 packet may cause the Cisco ASA and Cisco PIX security appliances to reload. Devices that are running software version 7.2(4)9 or 7.2(4)10 and configured for IPv6 may be vulnerable. This vulnerability does not affect devices that are configured only for IPv4.

**Note:** Devices that are running software versions in the 7.0, 7.1, 8.0, and 8.1 releases are not vulnerable.
To configure IPv6 on a Cisco ASA or Cisco PIX security appliance, at a minimum, each interface needs to be configured with an IPv6 link-local address. Additionally, you can add a global address to the interface.

**Note:** Only packets that are destined to the device (not transiting the device) may trigger the effects of this vulnerability. These packets must be destined to an interface configured for IPv6.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**Impact**
The Denial of Service (DoS) vulnerabilities may cause a reload of the affected device.

**Suggested Fix**
Customers that do not require IPv6 functionality on their devices can use the no ipv6 address interface sub-command to disable processing of IPv6 packets and eliminate their exposure.

**PIX/ASA SQL *Net Packet DoS Vulnerability - 109974 [PIX, ASA]**

**Description**
Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT -109974: Verfiy SQL *Net Packet DoS Vulnerability [PIX, ASA]

Description
SQL*Net Packet DoS Vulnerability
The SQL*Net protocol consists of different packet types are handled by the security appliance to make the data stream appear consistent to the Oracle version 7.x and earlier implementations on either side of the Cisco ASA and Cisco PIX security appliances. A series of SQL*Net packets may cause a denial of service condition on a Cisco ASA and Cisco PIX device that is configured with SQL*Net inspection. SQL*Net inspection is enabled by default. A successful attack may result in a reload of the device.

The default port assignment for SQL*Net is TCP port 1521. This is the value used by Oracle for SQL*Net. Please note the class-map command can be used in the Cisco ASA or Cisco PIX to apply SQL*Net inspection to a range of different port numbers. A TCP three-way handshake is needed to exploit this vulnerability. The requirement of a TCP three way handshake significantly reduces the possibility of exploitation using packets with spoofed source addresses.
Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Denial of Service (DoS) vulnerabilities may cause a reload of the affected device. Repeated exploitation could result in a sustained DoS condition.

Suggested Fix
SQL*Net inspection should be disabled if it is not needed. Temporarily disabling the feature will mitigate this vulnerability. SQL*Net inspection can be disabled with the command no inspect sqlnet.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.

PIX/ASA TCP State Manipulation DoS Vulnerability - 109444 [PIX, ASA]

Description
Multiple Cisco products are affected by denial of service (DoS) vulnerability that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PIX PSIRT -109444: Verfiy TCP State Manipulation DoS Vulnerabilitiy [PIX, ASA]
Description

Certain Cisco ASA and Cisco PIX Software versions are affected by these vulnerabilities. A device running Cisco ASA and Cisco PIX Software that is under attack will have numerous TCP connections in the established state. The show asp table socket command can be used to display the TCP connections. The following is example output showing a potential attack in progress.

```
FIREWALL# show asp table socket | grep ESTAB
TCP   123a8a6c  192.168.1.10:80           192.168.1.20:46181    ESTAB
TCP   123e6d54  192.168.1.10:80           192.168.1.20:40271    ESTAB
TCP   1244f78c  192.168.1.10:80           192.168.1.20:40271    ESTAB
TCP   124f8d2c  192.168.1.10:80           192.168.1.20:46599    ESTAB
TCP   12507f2c  192.168.1.10:80           192.168.1.20:5607     ESTAB
```

It is possible for normal traffic to cause established TCP connections to appear on Cisco ASA or PIX devices, especially VPN connections terminated to the device. In order to confirm if established TCP connections are part of an attack, administrators should use a monitoring point outside the firewall such as a packet sniffer or Netflow collection agent to examine the profile of the suspicious TCP connections and determine if an attack is occurring.

Note: The `show asp table socket` command was introduced in Cisco ASA and Cisco PIX Software 8.0(1).

Further detail about hung TCP connections can be found with `show conn detail all long` command. The IP address used to qualify the example below is the address of the firewall interface under attack.

```
FIREWALL# show conn detail all long | grep 192.168.1.10
TCP outside:192.168.1.20/62345 (192.168.1.20/62345) NP Identity Ifc:192.168.1.10/80 (192.168.1.10/80), flags UB, idle 0s, uptime 0s, timeout 1m0s, bytes 0
TCP outside:192.168.1.20/56268 (192.168.1.20/56268) NP Identity Ifc:192.168.1.10/80 (192.168.1.10/80), flags UB, idle 0s, uptime 0s, timeout 1m0s, bytes 0
TCP outside:192.168.1.20/63445 (192.168.1.20/63445) NP Identity Ifc:192.168.1.10/80 (192.168.1.10/80), flags UB, idle 0s, uptime 0s, timeout 1m0s, bytes 0
TCP outside:192.168.1.20/49151 (192.168.1.20/49151) NP Identity Ifc:192.168.1.10/80 (192.168.1.10/80), flags UB, idle 0s, uptime 0s, timeout 1m0s, bytes 0
TCP outside:192.168.1.20/57147 (192.168.1.20/57147) NP Identity Ifc:192.168.1.10/80 (192.168.1.10/80), flags UB, idle 0s, uptime 0s, timeout 1m0s, bytes 0
```

Note: Both troubleshooting commands referenced about will display TCP connections that are terminated to a firewall interface and transiting through the firewall.
Applicable Platforms
Cisco PIX and ASA Firewalls

Impact
Successful exploitation of the TCP state manipulation vulnerabilities may result in a DoS condition where new TCP connections are not accepted on an affected system. Repeated exploitation may result in a sustained DoS condition. A reboot may be required to recover affected systems.

Suggested Fix
Cisco ASA and Cisco PIX Software provide a method to expire stalled half-closed TCP connections that helps mitigate against the TCP state manipulation vulnerabilities. This method protects against attacks directed to a firewall and devices protected by a firewall. The timeout half-closed command will expire TCP sessions that have remained in a half-closed state beyond a user-configured timeout.

FIREWALL(config)# timeout half-closed 0:5:0
This command will set the TCP half-closed timeout to the smallest permitted value of five minutes. For more information on the TCP half-closed timeout, please consult the following link:

PIX/ASA VPN Authentication Bypass Vulnerability - 109974 [PIX, ASA]

Description
VPN Authentication Bypass when Account Override Feature is Used vulnerability exist in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances

Applicable Platforms
Cisco PIX and ASA Firewalls

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT -109974: Verfiy VPN Authentication Bypass Vulnerabilitiy [PIX, ASA]

Description
VPN Authentication Bypass Vulnerability
Cisco ASA or Cisco PIX security appliances that are configured for IPsec or SSL-based remote access VPN and have the Override Account Disabled feature enabled are affected by this vulnerability.

Note: The Override Account Disabled feature was introduced in Cisco ASA software version 7.1(1). Cisco ASA and PIX software versions 7.1, 7.2, 8.0, and 8.1 are affected by this vulnerability. This feature is disabled by default.
The Cisco ASA or Cisco PIX security appliance can be configured to override an account-disabled indication from a AAA server and allow the user to log on anyway. However, the user must provide the correct credentials in order to login to the VPN. A vulnerability exists in the Cisco ASA and Cisco PIX security appliances where VPN users can bypass authentication when the override account feature is enabled.

**Note:** The override account feature was introduced in Cisco ASA software version 7.1(1).

The override account feature is enabled with the `override-account-disable` command in `tunnel-group general-attributes` configuration mode, as shown in the following example. The following example allows overriding the "account-disabled" indicator from the AAA server for the WebVPN tunnel group "testgroup":

```
hostname(config)#tunnel-group testgroup type webvpn
hostname(config)#tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#override-account-disable
```

**Note:** The override account feature is disabled by default.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**Impact**
Successful exploitation of the VPN Authentication Bypass when Account Override Feature is Used vulnerability may allow an attacker to successfully connect to the Cisco ASA via remote access IPSec or SSL-based VPN.

**Suggested Fix**
VPN Authentication Bypass Vulnerability

The override account feature is enabled with the `override-account-disable` command in `tunnel-group general-attributes` configuration mode. As a workaround, disable this feature using the `no override-account-disable` command.

**PIX/ASA Windows NT Domain Authentication Bypass Vulnerability - 108009**

**Description**

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate some of these vulnerabilities are available.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Rule 1

**Rule**
PSIRT -108009: Verfiy Windows NT Domain Authentication Bypass Vulnerability [PIX, ASA]

**Description**
Windows NT Domain Authentication Bypass Vulnerability

Because of a Microsoft Windows NT Domain authentication issue the Cisco ASA and Cisco PIX devices may be susceptible to a VPN authentication bypass vulnerability. Cisco ASA or Cisco PIX security appliances configured for IPSec or SSL-based remote access VPN may be vulnerable.

**Note:** Cisco ASA or Cisco PIX security appliances that are configured for IPSec or SSL-based remote access VPN using any other type of external authentication (that is, LDAP, RADIUS, TACACS+, SDI, or local database) are not affected by this vulnerability.

The Cisco ASA security appliance supports Microsoft Windows server operating systems that support NTLM version 1, collectively referred to as "NT servers". NT Domain authentication is supported only for remote access VPNs.

**Applicable Platforms**
Cisco PIX and ASA Firewalls

**Impact**
Successful exploitation of the VPN Authentication Bypass Vulnerability may allow an attacker to successfully connect to the Cisco ASA via remote access IPSec or SSL-based VPN.

**Suggested Fix**
LDAP authentication is not affected by this vulnerability. As a workaround, you can enable a different type of external authentication for Remote Access VPN instead of Windows NT Domain authentication.

Note: For more information about support for a specific AAA server type, refer to the following link: http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/aaa.html#wp1069492

**PPTP - 13640 [IOS]**

**Description**
Point-to-Point Tunneling Protocol (PPTP) allows users to tunnel to an Internet Protocol (IP) network using a Point-to-Point Protocol (PPP). The protocol is described in RFC2637.

PPTP implementation using Cisco IOS software releases contains a vulnerability that will crash a router if it receives a malformed or crafted PPTP packet. To expose this vulnerability, PPTP must be enabled on the router. PPTP is disabled by default. No additional special conditions are required.

**Applicable Platforms**
Cisco IOS Devices
References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT -13640: Verify Malformed PPTP Packet Vulnerability [IOS]

Description
By sending a crafted PPTP packet to port 1723, a control PPTP port, it is possible to crash the router. This vulnerability does not require special router configuration. Enabling PPTP is sufficient to expose the vulnerability. The router will crash after it receives a single packet.

Applicable Platforms
Cisco IOS Devices.

Impact
By repeatedly exploiting this vulnerability, it is possible to cause permanent Denial of Service (DoS). This denial is not only of the PPTP functionality but the whole router will stop functioning.

Suggested Fix
There is no workaround for this vulnerability.

Radius - 65328 [IOS]

Description
There is a vulnerability in AAA RADIUS authentication if none is used as a fallback method. Sending a sufficiently long username will bypass the RADIUS authentication and succeed. "RADIUS Authentication Bypass." at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT -65328: Verify RADIUS Authentication Bypass [IOS]
Description
There is a vulnerability in AAA RADIUS authentication if none is used as a fallback method. Sending a sufficiently long username will bypass the RADIUS authentication and succeed. "RADIUS Authentication Bypass." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of the vulnerability may result in bypassing the RADIUS authentication.

Suggested Fix
Removing none as a fallback to RADIUS or putting an additional method other than local between RADIUS and none will mitigate this vulnerability.

Reload After Scanning - 13632[IOS]

Description
Security Scanning software can cause a memory error in Cisco IOS Software that will cause a reload to occur. This vulnerability affects only Cisco IOS software version 12.1(2)T and 12.1(3)T, and limited deployment releases based on those versions.

See "IOS Reload after Scanning Vulnerability." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT -13632: Verfiy IOS Reload after Scanning Vulnerability [IOS]

Description
An attempt to make a TCP connection to ports 3100-3999, 5100-5999, 7100-7999, and 10100-10999 will cause the router to unexpectedly reload at the next show running-config, or write memory, or any command that causes the configuration file to be accessed. Cisco IOS software cannot be configured to support any services that might listen at those port addresses, and cannot be configured to accept connections on those ports, however, connection attempts to these ports in the affected version will cause memory corruption, later leading to an unexpected reload.

Software packages are available from various commercial and free sites that perform automated remote tests for computer security vulnerabilities by scanning computers on a network for known security flaws. A common log message in environments that experienced security scan related crashes was the "attempt to connect to RSHELL." error message.
Understanding Compliance and Audit Manager (CAAM) Policies

Applicable Platforms
Cisco IOS Devices.

Impact
The described defect can be used to mount a denial of service (DoS) attack on any vulnerable Cisco product, which may result in violations of the availability aspects of a customer's security policy. This defect by itself does not cause the disclosure of confidential information nor allow unauthorized access.

Suggested Fix
This vulnerability can be mitigated by configuring access lists and applying access groups on all interfaces or on external devices or firewalls to prevent connection attempts to affected routers, and to eliminate router addresses in any planned security scanning exercises.

SAA Packets - 42744 [IOS]

Description
The router is vulnerable only if the RTR responder is enabled. When the router receives a malformed RTR packet, it will crash. RTR is disabled by default. Although RTR was introduced in Cisco IOS Software Release 11.2, only the following main releases are vulnerable:

- See "Cisco IOS Software Processing of SAA Packets." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT -42744: Verify SAA Packets Processing Vulnerability [IOS]

Description
The Service Assurance Agent (SAA) is the new name for the Response Time Reporter (RTR) feature. The RTR feature allows you to monitor network performance, network resources, and applications by measuring response times and availability. With this feature you can perform troubleshooting, problem notifications, and problem analysis based on response time reporter statistics. A router is vulnerable only if the RTR responder is enabled.

Applicable Platforms
Cisco IOS Devices.

Impact
By sending malformed RTR packets, it is possible to crash the router.
Suggested Fix
There is no workaround short of disabling the RTR responder. It is possible to mitigate the vulnerability by applying the ACL on the router.

SGBP Packet - 68793 [IOS]

Description
The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

(See "IOS Stack Group Bidding Protocol Crafted Packet DoS" at Cisco Security Advisories website for more information.)

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule

Description
The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

This vulnerability affects any device that runs Cisco IOS and has enabled the SGBP protocol. SGBP is enabled by defining a stack group, which is done using the global IOS command sgbp group . The presence of this command will cause the device to begin listening on port 9900, even if the remaining SGBP parameters are not fully configured.

(See "IOS Stack Group Bidding Protocol Crafted Packet DoS" at Cisco Security Advisories website for more information.)

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of this vulnerability may cause the affected device to become unresponsive and trigger a hardware reset, resulting in a denial of service condition.

Suggested Fix
Disable SGBP Protocol on the device. For sites that require the SGBP protocol to be enabled, it may be possible to apply Access Control Lists (ACLs) to prevent untrusted hosts from exploiting this vulnerability. The Control Plane Policy (CoPP) feature, if available, may also be used to mitigate this vulnerability.
SIP - 81825 [IOS]

Description
Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.

There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

Workarounds exist to mitigate the effects of this problem on devices which do not require SIP.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT -81825: Verify SIP Packet Reloads IOS Devices Not Configured for SIP [IOS]

Description
SIP is a protocol designed for use in IP voice networks and is widely used for Voice over Internet Protocol (VoIP) communications worldwide.

Cisco devices running certain versions of IOS with support for SIP services may be affected by a vulnerability that leads to a reload of the device with a crafted series of SIP packets to either TCP port 5060 or UDP port 5060. This vulnerability affects routers that contain any SIP configuration, including SIP gateways. This issue is being tracked as Cisco Bug ID CSCsh58082 (registered customers only).

In addition, certain versions of IOS with support for SIP services may process SIP messages even if they are not configured for SIP operation. To process SIP messages IOS will open UDP port 5060 and TCP port 5060 for listening. The Cisco Bug ID that documents the issue of IOS processing SIP messages without being configured for SIP operation is CSCsb25337 (registered customers only). The fix for this bug turns off the listening ports TCP 5060 and UDP 5060.

A device must have an open SIP port to be vulnerable to this issue. Devices which do not listen on TCP 5060 or UDP 5060 are not vulnerable. Because SIP utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of the vulnerability may result in a reload of the device. The issue may be repeatedly exploited, leading to an extended Denial Of Service (DoS) condition.
Suggested Fix

Disable SIP listening ports

For devices which do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device with the following commands.

Warning: When applying this workaround to devices which are processing MGCP or H.323 calls, the device will not allow you to stop SIP processing while active calls are being processed. Under these circumstances, this workaround should be implemented during a maintenance window when active calls can be briefly stopped.

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#sip-ua
Router(config-sip-ua)#no transport udp
Router(config-sip-ua)#no transport tcp
Router(config-sip-ua)#end

After applying this workaround the commands show ip sockets and show tcp brief all will not show the device listening on UDP and TCP port 5060:

Router#show ip sockets
Proto Remote Port Local Port In Out Stat TTY
17 --listen-- 9.13.32.18 2887 0 0 11 0

Router#show tcp brief all
TCB Local Address Foreign Address (state)
6649A5A4 *.1720 *. LESTEN
66CDC764 *.1723 *. LISTEN

Control Plane Policing

For devices which do not need to run SIP, you can use Control Plane Policing (CoPP) to block all SIP access to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to your network.

Warning: Because SIP utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses.

!-- Permit all TCP and UDP SIP traffic sent to all IP addresses
!-- configured on all interfaces of the affected device so that it
!-- will be policed and dropped by the CoPP feature.
access-list 100 permit tcp any any eq 5060
access-list 100 permit udp any any eq 5060

!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
Understanding Compliance and Audit Manager (CAAM) Policies

!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices.

!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature.

class-map match-all drop-sip-class
  match access-group 100

!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.

policy-map drop-sip-traffic
  class drop-sip-class
    drop

!-- Apply the Policy-Map to the Control-Plane of the
!-- device.

control-plane
  service-policy input drop-sip-traffic

In the above CoPP example, the access control list entries (ACEs) which match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function.

SIP DoS Vulnerabilities - 109322 [IOS]

Description
A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that can be exploited remotely to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate the vulnerability apart from disabling SIP, if the Cisco IOS device does not need to run SIP for VoIP services. However, mitigation techniques are available to help limit exposure to the vulnerability.
Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 109322: Verfiy SIP DoS Vulnerabilities [IOS]

Description
SIP is a popular signaling protocol that is used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination. Voice and video are the most popular types of sessions that SIP handles, but the protocol has the flexibility to accommodate other applications that require call setup and termination. SIP call signaling can use UDP (port 5060), TCP (port 5060), or TLS (TCP port 5061) as the underlying transport protocol.

A denial of service (DoS) vulnerability exists in the SIP implementation in Cisco IOS Software. This vulnerability is triggered by processing a specific and valid SIP message.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of the vulnerabilities described in this document may result in a reload of the device. The issue could be repeatedly exploited to result in an extended Denial Of Service (DoS) condition.

Suggested Fix
If the affected Cisco IOS device requires SIP for VoIP services, SIP cannot be disabled, and therefore, no workarounds are available. Users are advised to apply mitigation techniques to help limit exposure to the vulnerability. Mitigation consists of allowing only legitimate devices to connect to the routers. To increase effectiveness, the mitigation must be coupled with anti-spoofing measures on the network edge. This action is required because SIP can use UDP as the transport protocol.

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document “Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco IOS SIP and Crafted UDP Vulnerabilities”.

Disable SIP Listening Ports
For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. Some versions of Cisco IOS Software allow administrators to accomplish this with the following commands:
sip-ua
no transport udp
no transport tcp
**Warning:** When applying this workaround to devices that are processing Media Gateway Control Protocol (MGCP) or H.323 calls, the device will not stop SIP processing while active calls are being processed. Under these circumstances, this workaround should be implemented during a maintenance window when active calls can be briefly stopped.

After applying this workaround, administrators are advised to use the show commands, as discussed in the Affected Products section of this advisory, to confirm that the Cisco IOS device is no longer processing SIP messages.

**Control Plane Policing**

For devices that need to offer SIP services it is possible to use Control Plane Policing (CoPP) to block SIP traffic to the device from untrusted sources. Cisco IOS Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to the network:

```
!-- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.
!-- Everything else is not trusted. The following access list is used
!-- to determine what traffic needs to be dropped by a control plane
!-- policy (the CoPP feature.) If the access list matches (permit)
!-- then traffic will be dropped and if the access list does not
!-- match (deny) then traffic will be processed by the router.

access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5061
access-list 100 deny udp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5061
access-list 100 permit udp any any eq 5060
access-list 100 permit tcp any any eq 5060
access-list 100 permit tcp any any eq 5061
!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices.

!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature.
```
class-map match-all drop-sip-class
    match access-group 100

!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.

policy-map drop-sip-traffic
    class drop-sip-class
        drop

!-- Apply the Policy-Map to the Control-Plane of the
!-- device.

control-plane
    service-policy input drop-sip-traffic

*Warning*: Because SIP can use UDP as a transport protocol, it is possible to easily spoof the IP address of the sender, which may defeat access control lists that permit communication to these ports from trusted IP addresses.

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function.

SIP DoS Vulnerability - 110395 [IOS]

Description
A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled.
Cisco has released free software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 110395 Verfiy SIP DoS Vulnerability [IOS]

Description
SIP is a popular signaling protocol that is used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination. Voice and video are the most popular types of sessions that SIP handles, but the protocol has the flexibility to accommodate other applications that require call setup and termination. SIP call signaling can use UDP (port 5060), TCP (port 5060), or TLS (TCP port 5061) as the underlying transport protocol.

The Cisco Unified Border Element (previously known as the Cisco Multiservice IP-to-IP Gateway) is a special Cisco IOS Software image that runs on Cisco multiservice gateway platforms. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking.

For more information about Cisco Unified Border Element refer to the following link:

A DoS vulnerability exists in the SIP implementation in Cisco IOS Software when devices are running a Cisco IOS image that contains the Cisco Unified Border Element feature. This vulnerability is triggered by processing a series of crafted SIP messages.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of the vulnerability described in this document may result in a reload of the device. The issue could be repeatedly exploited to cause an extended DoS condition.
Suggested Fix

If the affected Cisco IOS device requires SIP for VoIP services, SIP cannot be disabled, and therefore, no workarounds are available. Users are advised to apply mitigation techniques to help limit exposure to the vulnerability. Mitigation consists of allowing only legitimate devices to connect to the routers. To increase effectiveness, the mitigation must be coupled with anti-spoofing measures on the network edge. This action is required because SIP can use UDP as the transport protocol.

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Denial of Service Vulnerabilities in Cisco Unified Communications Manager and Cisco IOS Software".

Disable SIP Listening Ports

For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. Some versions of Cisco IOS Software allow administrators to accomplish this with the following commands:

```
sip-ua
no transport udp
no transport tcp
no transport tcp tls
```

**Warning:** When applying this workaround to devices that are processing Media Gateway Control Protocol (MGCP) or H.323 calls, the device will not stop SIP processing while active calls are being processed. Under these circumstances, this workaround should be implemented during a maintenance window when active calls can be briefly stopped.

The `show udp connections`, `show tcp brief all`, and `show processes | include SIP` commands can be used to confirm that the SIP UDP and TCP ports are closed after applying this workaround.

Depending on the Cisco IOS Software version in use, the output of "show ip sockets" still showed UDP port 5060 open, but sending something to that port caused the SIP process to emit the following message:

```
*Feb 2 11:36:47.691: sip_udp_sock_process_read: SIP UDP Listener is DISABLED
```

Control Plane Policing

For devices that need to offer SIP services it is possible to use Control Plane Policing (CoPP) to block SIP traffic to the device from untrusted sources. Cisco IOS Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to the network

```
!-- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.
!-- Everything else is not trusted. The following access list is used
!-- to determine what traffic needs to be dropped by a control plane
!-- policy (the CoPP feature.) If the access list matches (permit)
!-- then traffic will be dropped and if the access list does not
!-- match (deny) then traffic will be processed by the router.

access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5061
```
access-list 100 deny udp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5061
access-list 100 permit udp any any eq 5060
access-list 100 permit tcp any any eq 5060
access-list 100 permit tcp any any eq 5061

!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices.
!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature.

class-map match-all drop-sip-class
    match access-group 100

!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.

policy-map drop-sip-traffic
    class drop-sip-class
        drop

!-- Apply the Policy-Map to the Control-Plane of the
!-- device.

control-plane
    service-policy input drop-sip-traffic

**Warning:** Because SIP can use UDP as a transport protocol, it is possible to easily spoof the IP address of the sender, which may defeat access control lists that permit communication to these ports from trusted IP addresses.

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function.

SIP DoS Vulnerability - 112022 [IOS]

Description
Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 112022 Verfiy Cisco IOS Software SIP DoS Vulnerability [IOS]

Description
Cisco devices are affected when they are running affected Cisco IOS Software versions that are configured to process SIP messages.

Recent versions of Cisco IOS Software do not process SIP messages by default. Creating a dial peer by issuing the dial-peer voice command will start the SIP processes, causing the Cisco IOS device to process SIP messages. In addition, several features within Cisco Unified Communications Manager Express, such as ePhones, will also automatically start the SIP process when they are configured, causing the device to start processing SIP messages. An example of an affected configuration follows:

dial-peer voice <Voice dial-peer tag> voip

...
In addition to inspecting the Cisco IOS device configuration for a **dial-peer** command that causes the device to process SIP messages, administrators can also use the **show processes | include SIP** command to determine whether Cisco IOS Software is running the processes that handle SIP messages. In the following example, the presence of the processes **CCSIP_UDP_SOCKET** or **CCSIP_TCP_SOCKET** indicates that the Cisco IOS device will process SIP messages:

```
Router# show processes | include SIP
149 Mwe 40F48254  4 1 400023108/24000  0 CCSIP_UDP_SOCKET
150 Mwe 40F48034  4 1 400023388/24000  0 CCSIP_TCP_SOCKET
```

**Note:** Because there are several ways a device running Cisco IOS Software can start processing SIP messages, it is recommended that the **show processes | include SIP** command be used to determine whether the device is processing SIP messages instead of relying on the presence of specific configuration commands.

Cisco Unified Border Element images are also affected by two of these vulnerabilities.

**Note:** The Cisco Unified Border Element feature (previously known as the Cisco Multiservice IP-to-IP Gateway) is a special Cisco IOS Software image that runs on Cisco multiservice gateway platforms. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking.

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the **show version** command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

!--- output truncated
```

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.4(20)T with an installed image name of C1841-ADVENTPRISEK9-M:

```
Router# show version
Cisco IOS Software, 1841 Software (C1841-ADVENTPRISEK9-M), Version 12.4(20)T,
RELEASE SOFTWARE (fc3)
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
```
Understanding Compliance and Audit Manager (CAAM) Policies

Chapter 4      Using Compliance and Audit Manager Feature

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide".

Note: CUCM is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of the vulnerabilities in this advisory may result in a reload of the device. Repeated exploitation could result in a sustained denial of service condition.

Suggested Fix
If the affected Cisco IOS device requires SIP for VoIP services, SIP cannot be disabled, and no workarounds are available. Users are advised to apply mitigation techniques to help limit exposure to the vulnerabilities. Mitigation consists of allowing only legitimate devices to connect to affected devices. To increase effectiveness, the mitigation must be coupled with anti-spoofing measures on the network edge. This action is required because SIP can use UDP as the transport protocol.

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco Voice Products".

Disabling SIP Listening Ports
For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. Some versions of Cisco IOS Software allow administrators to disable SIP with the following commands:

```
sip-ua
no transport udp
no transport tcp
no transport tcp tls
```

Warning: When applying this workaround to devices that are processing Media Gateway Control Protocol (MGCP) or H.323 calls, the device will not stop SIP processing while active calls are being processed. Under these circumstances, this workaround should be implemented during a maintenance window when active calls can be briefly stopped.

The `show udp connections`, `show tcp brief all`, and `show processes | include SIP` commands can be used to confirm that the SIP UDP and TCP ports are closed after applying this workaround.

Depending on the Cisco IOS Software version in use, the output from the `show ip sockets` command may still show the SIP ports open, but sending traffic to them will cause the SIP process to emit the following message:

```
*Jun 2 11:36:47.691: sip_udp_sock_process_read: SIP UDP Listener is DISABLED
```

Control Plane Policing
For devices that need to offer SIP services, it is possible to use Control Plane Policing (CoPP) to block SIP traffic to the device from untrusted sources. Cisco IOS Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to specific network configurations:

```plaintext
!-- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.
!-- Everything else is not trusted. The following access list is used
!-- to determine what traffic needs to be dropped by a control plane
!-- policy (the CoPP feature.) If the access list matches (permit)
!-- then traffic will be dropped and if the access list does not
!-- match (deny) then traffic will be processed by the router.

access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5061
access-list 100 deny udp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5061
access-list 100 permit udp any any eq 5060
access-list 100 permit tcp any any eq 5060
access-list 100 permit tcp any any eq 5061

!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices.
!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature.

class-map match-all drop-sip-class
  match access-group 100

!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.

policy-map control-plane-policy
  class drop-sip-class
    drop
```

Configuration Management with Cisco Prime LAN Management Solution 4.2
!-- Apply the Policy-Map to the Control-Plane of the
!-- device.

class (control-plane)
    service-policy input control-plane-policy

Note: Because SIP can use UDP as a transport protocol, it is possible to easily spoof the IP address of
the sender, which may defeat access control lists that permit communication to these ports from trusted
IP addresses.

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets
with the "permit" action result in these packets being discarded by the policy-map "drop" function, while
packets that match the "deny" action (not shown) are not affected by the policy-map drop function.
Additional information on the configuration and use of the CoPP feature can be found at
http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html and

SNMP Malformed Message Handling - 19294 [IOS]

Description
Multiple Cisco products contain vulnerabilities in the processing of Simple Network Management
Protocol (SNMP) messages. The vulnerabilities can be repeatedly exploited to produce a denial of
service. In most cases, workarounds are available that may mitigate the impact. These vulnerabilities are
identified by various groups as VU#617947, VU#107186, OUSPG #0100, CAN-2002-0012, and
CAN-2002-0013.
. See "Malformed SNMP Message-Handling Vulnerabilities" at Cisco Security Advisories website for
more information

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to
repair the Cisco product. Security Notices For issues that require a response to information posted to a
public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 19294: Verfiy Malformed SNMPMessage-Handling Vulnerabilities [IOS]

Description
SNMP messages are transported using User Datagram Protocol (UDP) and are subject to IP source
address spoofing. In any circumstance where ingress and egress source IP address filtering is lacking, it
is more likely that an attacker could spoof the source IP address and circumvent access control
mechanisms to cause a vulnerable system to fail.
If an attacker is able to guess or otherwise obtain a read-only community string for an affected device, then he or she could bypass SNMP access control that depends on the community string.

**Applicable Platforms**
Cisco IOS Devices.

**Impact**
The vulnerability can be exploited to produce a Denial of Service (DoS) attack. When the vulnerability is exploited, it can cause an affected Cisco product to crash and reload.

**Suggested Fix**
Turn SNMP off in the device. This is an effective workaround, but removes management capability to the device.

### SNMP Message Processing - 50980 [IOS]

**Description**
Cisco Internetwork Operating System (IOS) Software release trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

See "Vulnerabilities in SNMP Message Processing." at Cisco Security Advisories website for more information.

**Applicable Platforms**
Cisco IOS Devices

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

### Rule 1

**Rule**
PSIRT - 50980: Verfiy Vulnerabilities in SNMPMessage Processing [IOS]
Description
In this vulnerability, the IOS SNMP process is incorrectly attempting to process SNMP solicited operations on UDP port 162 and the random UDP port. Upon attempting to process a solicited SNMP operation on one of those ports, the device can experience memory corruption and may reload.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of this vulnerability results in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

Suggested Fix
It is possible to disable SNMP processing on the device running IOS by issuing the following command:
no snmp-server
Removing the public community string with the configure command "no snmp-server community ro" is not sufficient as the SNMP server will still be running and the device will be vulnerable. The command "no snmp-server" must be used instead. Verify SNMP server status by using the enable command show snmp. You should see a response of "%SNMP agent not enabled".

SNMP Multiple Community String Vulnerabilities - 13629 [IOS]

Description
Multiple Cisco IOS Software and CatOS software releases contain several independent but related vulnerabilities involving the unexpected creation and exposure of SNMP community strings. These vulnerabilities can be exploited to permit the unauthorized viewing or modification of affected devices. See "Cisco IOS Software Multiple SNMP Community String Vulnerabilities." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 13629: Verify Multiple SNMP Community String Vulnerabilities [IOS]
Description
Multiple Cisco IOS Software and CatOS software releases contain several independent but related vulnerabilities involving the unexpected creation and exposure of SNMP community strings. These vulnerabilities can be exploited to permit the unauthorized viewing or modification of affected devices. See "Cisco IOS Software Multiple SNMP Community String Vulnerabilities." at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices.

Impact
These vulnerabilities could be exploited separately or in combination to gain access to or modify the configuration and operation of any affected devices without authorization.

Suggested Fix
Disable SNMP access to the device.

SNMP Read-Write ILMI Community String - 13630 [IOS]

Description
Cisco IOS Software releases based on versions 11.x and 12.0 contain a defect that allows a limited number of SNMP objects to be viewed and modified without authorization using a undocumented ILMI community string. Some of the modifiable objects are confined to the MIB-II system group, such as "sysContact", "sysLocation", and "sysName", that do not affect the device's normal operation but that may cause confusion if modified unexpectedly. The remaining objects are contained in the LAN-EMULATION-CLIENT and PNNI MIBs, and modification of those objects may affect ATM configuration. An affected device might be vulnerable to a denial-of-service attack if it is not protected against unauthorized use of the ILMI community string. See "Cisco IOS Software SNMP Read-Write ILMI Community String Vulnerability." at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 13630: Verfiy SNMP Read-Write ILMI Community String Vulnerability [IOS]
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Description
Numerous objects can be viewed in the LAN-EMULATION-CLIENT MIB and PNNI MIB, and modification of some of the read-write objects can have an affect on ATM operation of the device. The objects in the LAN-EMULATION-CLIENT MIB can only be viewed or modified if LANE has already been configured on the device.

Applicable Platforms
Cisco IOS Devices.

Impact
If SNMP requests can be received by an affected device, then certain MIB objects can be viewed without proper authorization, causing a violation of confidentiality.

A subset of the readable MIB objects can be modified without authorization to cause a failure of integrity. For example, the hostname can be modified so as to confuse network administrators, or the contact and location information could be changed with a goal of disrupting operations or embarrassing whoever is responsible for the device.

Objects in the LAN-EMULATION-CLIENT and PNNI MIBs can be viewed and modified, thus resulting in changes to the operation of ATM functions. If ATM is in use on the device, this may result in a failure of availability.

Any affected device that is not otherwise protected against the receipt of SNMP packets is vulnerable to a denial-of-service (DoS) attack by flooding the SNMP port with read or write requests.

Suggested Fix
None.

SNMP Trap Reveals WEP Key - 46468 [IOS]

Description
Cisco Aironet Access Points (AP) running Cisco IOS software will send any static Wired Equivalent Privacy (WEP) key in the cleartext to the Simple Network Management Protocol (SNMP) server if the snmp-server enable traps wlan-wep command is enabled. Affected hardware models are the Cisco Aironet 1100, 1200, and 1400 series. This command is disabled by default. The workaround is to disable this command. Any dynamically set WEP key will not be disclosed.

See "SNMP Trap Reveals WEP Key in Cisco Aironet Access Point" at Cisco Security Advisories website for more information

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 46468: Verfiy SNMP Trap Reveals WEP Key Vulnerability [IOS]
Description

If enabled, the snmp-server enable traps wlan-wep command will send static WEP keys in the cleartext to the SNMP server every time a key is changed or the AP is rebooted. This vulnerability is opportunistic, and the following conditions must be met for the vulnerability to be exploited.

The snmp-server enable traps wlan-wep command must be enabled. (It is disabled by default.)

An adversary must be able to intercept SNMP packets sent from the AP to the SNMP server.

The AP in question must be rebooted or the static WEP key must be changed.

Under these circumstances, an adversary will be able to intercept all static WEP keys.

Dynamically configured WEP keys are not affected by this vulnerability and will not be revealed. A WEP key is dynamically configured if you are using one of the Extensible Authentication Protocol (EAP) authentication protocols. The following EAP authentication protocols are currently supported in Cisco APs: LEAP, EAP-TLS, PEAP, EAP-MD5, and EAP-SIM.

This vulnerability is assigned Cisco Bug ID CSCec55538 (registered customers only).

Applicable Platforms
Cisco IOS Devices.

Impact

If SNMP requests can be received by an affected device, then certain MIB objects can be viewed without proper authorization, causing a violation of confidentiality.

A subset of the readable MIB objects can be modified without authorization to cause a failure of integrity. For example, the hostname can be modified so as to confuse network administrators, or the contact and location information could be changed with a goal of disrupting operations or embarrassing whoever is responsible for the device.

Objects in the LAN-EMULATION-CLIENT and PNNI MIBs can be viewed and modified, thus resulting in changes to the operation of ATM functions. If ATM is in use on the device, this may result in a failure of availability.

Any affected device that is not otherwise protected against the receipt of SNMP packets is vulnerable to a denial-of-service (DoS) attack by flooding the SNMP port with read or write requests.

Suggested Fix

None.

SNMP Version 3 Authentication Vulnerability -107408 [IOS]

Description

Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default in Cisco products. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.
Common Vulnerabilities and Exposures (CVE) identifier **CVE-2008-0960** has also been assigned to these vulnerabilities.

**Applicable Platforms**
Cisco IOS Devices

**References**
CISCO PSIRT Advisories and Notices (107408 of 1.0)
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability

**Rule 1**

**Rule**
PSIRT - 107408: Verify SNMP Version 3 Authentication Vulnerability [IOS]

**Description**
SNMP defines a standard mechanism for remote management and monitoring of devices in an Internet Protocol (IP) network.

There are three general types of SNMP operations: "get" requests to request information, "set" requests that modify the configuration of a remote device, and "trap" messages that provide a monitoring function. SNMP requests and traps are transported over User Datagram Protocol (UDP) and are received at the assigned destination port numbers 161 and 162, respectively.

SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network. **RFC2574** defines the use of HMAC-MD5-96 and HMAC-SHA-96 as the possible authentication protocols for SNMPv3.

Vulnerabilities have been identified in the authentication code of multiple SNMPv3 implementations. This advisory identifies two vulnerabilities that are almost identical. Both are specifically related to malformed SNMPv3 packets that manipulate the Hash Message Authentication Code (HMAC). The two vulnerabilities may impact both Secure Hashing Algorithm-1 (SHA-1) and Message-Digest Algorithm 5 (MD5). The vulnerabilities described in this document can be successfully exploited using spoofed SNMPv3 packets.

**Applicable Platforms**
Cisco IOS Devices.

**Impact**
Successful exploitation of these vulnerabilities could result in the disclosure of sensitive information on a device or allow an attacker to make configuration changes to a vulnerable device that is based on the SNMP configuration.

**Suggested Fix**
**Infrastructure Access Control Lists**
Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure Access Control Lists (iACLs) are a network security best practice and should be
considered as a long-term addition to good network security as well as a workaround for these specific vulnerabilities. The iACL example below should be included as part of the deployed infrastructure access-list which will protect all devices with IP addresses in the infrastructure IP address range:

**Note:** UDP port 161 is applicable for all versions of SNMP.

```plaintext
--- Permit SNMP UDP 161 packets from trusted hosts destined to infrastructure addresses.

access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK eq 161

--- Deny SNMP UDP 161 packets from all other sources destined to infrastructure addresses.

access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 161

--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance with existing security policies and configurations

access-list 150 permit ip any any interface serial 2/0 ip access-group 150 in

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:


**Control Plane Policing**

Control Plane Policing (CoPP) can be used to block untrusted SNMP access to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The following example, which uses 192.168.100.1 to represent a trusted host, can be adapted to your network.

```plaintext
--- Deny SNMP UDP traffic from trusted hosts to all IP addresses

access-list 111 deny udp host 192.168.100.1 any eq 161

--- configured on all interfaces of the affected device so that it will be allowed by the CoPP feature

access-list 111 deny udp host 192.168.100.1 any eq 161

--- Permit all other SNMP UDP traffic sent to all IP addresses

--- configured on all interfaces of the affected device so that it will be policed and dropped by the CoPP feature
```
access-list 111 permit udp any any eq 161

!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!--- traffic in accordance with existing security policies and
!--- configurations for traffic that is authorized to be sent
!--- to infrastructure devices

!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all drop-snmpv3-class
match access-group 111

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-snmpv3-traffic
class drop-snmpv3-class
drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

class-map match-all drop-snmpv3-class
match access-group 111

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function.
Please note that the policy-map syntax is different in the 12.2S and 12.0S Cisco IOS trains:

```
policy-map drop-snmpv3-traffic
class drop-snmpv3-class
policy 32000 1500 1500 conform-action drop exceed-action drop
```

Additional information on the configuration and use of the CoPP feature is available at the following links:


### Transit Access Control Lists

Filters that deny SNMP packets using UDP port 161 should be deployed throughout the network as part of a Transit Access Control List (tACL) policy for protection of traffic that enters the network at ingress access points. This policy should be configured to protect the network device where the filter is applied and other devices behind it. Filters for SNMP packets that use UDP port 161 should also be deployed in front of vulnerable network devices so that traffic is only allowed from trusted clients.

Additional information about tACLs is available in "Transit Access Control Lists: Filtering at Your Edge:"


### Hardening Guide Statement

Customers are advised to review the "Fortifying the Simple Network Management Protocol" section of the "Cisco Guide to Harden Cisco IOS Devices" for information on configuring an IOS device for SNMPv3 authentication and privacy:


### Cisco IOS authPriv Configuration

Enabling the SNMPv3 privacy subsystem (if it is not already in use) is a short-term workaround for users who are unable to upgrade in a timely fashion. This subsystem is used to encrypt SNMPv3 traffic using a shared secret.

In Cisco IOS, administrators can enable this workaround by using the `authPriv` SNMPv3 feature. Only Cisco IOS crypto images can run the authPriv feature.

**Note:** Ensure that the management application supports SNMPv3 `authPriv` before implementing this feature.

### SSH Can Cause a Crash -24862 [IOS]

#### Description

While fixing vulnerabilities mentioned in the Cisco Security Advisory: Multiple SSH Vulnerabilities we inadvertently introduced an instability in some products. When an attacker tries to exploit the vulnerability VU#945216 (described in the CERT/CC Vulnerability Note at http://www.kb.cert.org/vuls/id/945216) the SSH module will consume too much of the processor's time, effectively causing a DoS. In some cases the device will reboot. In order to be exposed SSH must be enabled on the device.. See "Scanning for SSH Can Cause a Crash." at Cisco Security Advisories website

#### Applicable Platforms

Cisco IOS Devices
References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 24862: Verfiy Scanning for SSH Can Cause a Crash Vulnerability [IOS]
Description
While fixing the vulnerabilities (Cisco Security Advisory: Multiple SSH Vulnerabilities) an instability is introduced in some products. When exposed to an overly large packet, the SSH process will consume a large portion of the processor's instruction cycles, effectively causing a DoS. The capability to create such a packet is available in publicly available exploit code. In some cases this availability attack may result in a reboot of the device. In order to be exposed SSH must be enabled on the device. The vulnerability in question is named CRC-32. It is also marked as VU#945216 and described in the CERT/CC Vulnerability Note.

Applicable Platforms
Cisco IOS Devices.

Impact
By repeatedly exploiting this vulnerability an attacker can cause a denial of service, though Cisco products remain unaffected to the exploits that are trying to exploit vulnerabilities.

Suggested Fix
It is possible to mitigate this vulnerability in two ways:

• Block all SSH connections on the border on your network, or
• On each individual device allow SSH connections only from the required IP addresses and block all others.

Blocking all SSH connections, and all other protocols that are not supposed to come from the outside, on the network edge should be an integral part of the network security best practice.

SSH Malformed Packet -29581 [IOS]

Description
Certain Cisco products containing support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS® is disabled by default.

See "SSH Malformed Packet Vulnerabilities" at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices
References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 29581: Verify SSH Malformed Packet Vulnerabilities [IOS]

Description
Certain Cisco products containing support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS® is disabled by default.

See "SSH Malformed Packet Vulnerabilities" at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices.

Impact
The vulnerability can be exploited to make an affected product unavailable for several minutes while the device reloads. Once it has resumed normal processing, the device is still vulnerable and can be forced to reload repeatedly.

Suggested Fix
Workarounds consist of disabling the SSH server, removing SSH as a remote access method, permitting only trusted hosts to connect to the server, and blocking SSH traffic to the device completely via external mechanisms.

SSH TACACS+ Authentication -64439 [IOS]

Description
Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on IOS devices, may contain two vulnerabilities that can potentially cause IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with other authentication methods like Remote Authentication Dial In User Service (RADIUS) and the local user database may also be affected. "Vulnerabilities in SSH Server using TACACS+ authentication." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Rule 1

**Rule**
PSIRT - 64439: Vulnerabilities in SSH Server using TACACS+ authentication [IOS]

**Description**
Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on IOS devices, may contain two vulnerabilities that can potentially cause IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with other authentication methods like Remote Authentication Dial In User Service (RADIUS) and the local user database may also be affected. "Vulnerabilities in SSH Server using TACACS+ authentication." at Cisco Security Advisories website

**Applicable Platforms**
Cisco IOS Devices.

**Impact**
Successful exploitation of the vulnerability may result in a reload of the device or resource depletion. Repeated exploitation could result in a sustained denial of service condition.

**Suggested Fix**
It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted hosts to connect to the device via SSH.

**SSL -91888 [IOS]**

**Description**
Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker to decrypt any previously encrypted information.

**Applicable Platforms**
Cisco IOS Devices
References

Security Advisories: For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices: For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 91888: Verify For Vulnerabilities While Processing SSL Packets [IOS]

Description
SSL is a protocol designed to provide a secure connection between two hosts. The SSL Protocol is described in RFC4346. While not necessary for the understanding of this advisory, users are encouraged to consult the section “7.3 handshake Protocol Overview” in RFC4346 as well as Figure 1 in the same section. The text of the RFC4346 is available at the following link: http://tools.ietf.org/html/rfc4346#section-7.3.

An attacker can trigger these vulnerabilities after establishing a TCP connection, but prior to the exchange of authentication credentials, such as username/password or certificate. The requirement of the complete TCP 3-way handshake reduces the probability that these vulnerabilities will be exploited through the use of spoofed IP addresses.

An attacker intercepting traffic between two affected devices cannot exploit these vulnerabilities if the SSL session is already established because SSL protects against such injection. However, such an attack could abnormally terminate an existing session, via a TCP RST, for example. The attacker could then wait for a new SSL session to be established and inject malicious packets at the beginning of the new SSL session, thus triggering the vulnerability.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of any vulnerability listed in this advisory may result in the crash of the affected device. Repeated exploitation can result in a sustained DoS condition.

Suggested Fix
The only way to prevent a device from being susceptible to the listed vulnerabilities is to disable the affected service(s). However, if regular maintenance and operation of the device relies on these services, there is no workaround.

It is possible to mitigate these vulnerabilities by preventing unauthorized hosts from accessing affected devices. Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document for this advisory.
SSL Packet Processing Vulnerability - 107631 [IOS]

Description
A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

Cisco has released free software updates that address this vulnerability. Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 107631: Verify SSL Packet Processing Vulnerability[IOS]

Description
This vulnerability is triggered during the termination of an SSL session. Possession of valid credentials such as a username, password or a certificate is not required. SSL protocol uses TCP as a transport protocol. The requirement of the complete TCP 3-way handshake reduces the probability that this vulnerability will be exploited through the use of spoofed IP addresses.

A device running vulnerable Cisco IOS Software with SSL-based service configured will crash while terminating an SSL session.

Applicable Platforms
Cisco IOS Devices.

Impact
A successful exploit of this vulnerability may cause a crash of the affected device. Repeated exploitation may result in a sustained denial of service condition.

Suggested Fix
To prevent an exploit of a vulnerable device, SSL-based services need to be disabled. However, if regular maintenance and operation of the device relies on this service, there is no workaround.

The following command will disable the vulnerable HTTPS service:
Router(config)#no ip http secure-server

The following command will disable the vulnerable SSL VPN service:
Router(config)#no webvpn enable

The following command will disable the vulnerable OSP service:
Router(config)#no settlement <n>
Another option is to revert to HTTP protocol instead using HTTPS. The downside of this workaround is that the settlement information will be sent over the network unprotected.

It is possible to mitigate this vulnerability by preventing unauthorized hosts from accessing affected devices.

**Control Plane Policing (CoPP)**

Cisco IOS software versions that support Control Plane Policing (CoPP) can be configured to help protect the device from attacks that target the management and control planes. CoPP is available in Cisco IOS release trains 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T.

In the following CoPP example, the ACL entries that match the exploit packets with the permit action will be discarded by the **policy-map drop** function, whereas packets that match a **deny** action (not shown) are not affected by the policy-map drop function:

```plaintext
! -- Include deny statements up front for any protocols/ports/IP addresses that
! -- should not be impacted by CoPP
! -- Include permit statements for the protocols/ports that will be
! -- governed by CoPP
access-list 100 permit tcp any any eq 443

! -- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
! -- traffic in accordance with existing security policies and
! -- configurations for traffic that is authorized to be sent
! -- to infrastructure devices.
!
! -- Create a Class-Map for traffic to be policed by
! -- the CoPP feature.
!
class-map match-all drop-SSL-class match access-group 100
!
! -- Create a Policy-Map that will be applied to the
! -- Control-Plane of the device.
!
policy-map drop-SSL-policy class drop-SSL-class drop

! -- Apply the Policy-Map to the Control-Plane of the
! -- device.
!
control-plane service-policy input drop-SSL-policy

Note: In the preceding CoPP example, the ACL entries with the **permit** action that match the exploit packets will result in the discarding of those packets by the **policy-map drop** function, whereas packets that match the deny action are not affected by the **policy-map drop** function.

Access Control List (ACL)
An Access Control List (ACL) can be used to help mitigate attacks that target this vulnerability. ACLs can specify that only packets from legitimate sources are permitted to reach a device, and all others are to be dropped. The following example shows how to allow legitimate SSL sessions from trusted sources and deny all other SSL sessions:

```
access-list 101 permit tcp host <legitimate_host_IP_address> host <router_IP_address> eq 443
access-list 101 deny tcp any any eq 443
```

**SSL VPN Vulnerability - 112029 [IOS]**

**Description**
Cisco IOS Software contains a vulnerability when the Cisco IOS SSL VPN feature is configured with an HTTP redirect. Exploitation could allow a remote, unauthenticated user to cause a memory leak on the affected devices, that could result in a memory exhaustion condition that may cause device reloads, the inability to service new TCP connections, and other denial of service (DoS) conditions.

**Applicable Platforms**
Cisco IOS Devices

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT - 112029: Verify Cisco IOS Software SSL VPN Vulnerability[IOS]
Description

Devices running affected versions of Cisco IOS Software are vulnerable if configured with SSL VPN and HTTP port redirection.

The following methods may be used to confirm if the device is configured for Cisco IOS SSL VPNs and is vulnerable:

If the output from `show running-config | include webvpn` contains "webvpn gateway <word>" then the device is supporting the Cisco IOS SSL VPN feature. A device is vulnerable if it has the `inservice` command in at least one of the "webvpn gateway" sections and is configured for HTTP port redirection. The following example shows a vulnerable device configured with Cisco IOS SSL VPN:

```
Router#show running | section webvpn
webvpn gateway Gateway
  ip address 10.1.1.1 port 443
  http-redirect port 80
  ssl trustpoint Gateway-TP
  inservice
!
Router#
```

A device that supports the Cisco IOS SSL VPN is not vulnerable if "webvpn gateway" is not configured.

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the `show version` command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the `show version` command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.4(20)T with an installed image name of C2800NM-ADVSECURITYK9-M:

```
Router#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVSECURITYK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 22:00 by prod_rel_team
!
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide"

Applicable Platforms
Cisco IOS Devices.
Impact
Successful exploitation of the vulnerability may result in a lack of available memory resources on the affected device, which could affect new connections to the device such as SSH and Telnet connections. Depletion of memory resources may also result in failing of routing protocols and other services.

Suggested Fix
Disabling HTTP redirection for SSL VPN connections can be used as a workaround for this vulnerability. HTTP redirection for SSL VPN connections is disabled by executing the command `no http-redirect port in webvpn` gateway configuration mode.

In addition, manually clearing the hung TCBs with the command `clear tcp tcb *` will transition the TCBs into a CLOSED state. After a time they will clear the CLOSED state and the memory will be released.

Note: Clearing the TCB will clear both legitimate and hung connections, including remote connections to the device such as Telnet and SSH connections.

The Cisco Applied Mitigation Bulletin (AMB) "Identifying and Mitigating Exploitation of the TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products", contains two mitigations (EEM scripts and SNMP) that can be used to detect and clear hung TCP connections.

Embedded Event Manager (EEM)
A Cisco IOS Embedded Event Manager (EEM) policy that is based on Tool Command Language (Tcl) can be used on vulnerable Cisco IOS devices to identify and detect a hung, extended, or indefinite TCP connection that is caused by this vulnerability. The policy allows administrators to monitor TCP connections on a Cisco IOS device. When Cisco IOS EEM detects potential exploitation of this vulnerability, the policy can trigger a response by sending a syslog message or a Simple Network Management Protocol (SNMP) trap to clear the TCP connection. The example policy provided in this document is based on a Tcl script that monitors and parses the output from two commands at defined intervals, produces a syslog message when the monitor threshold reaches its configured value, and can reset the TCP connection.

The Tcl script is available for download at the "Cisco Beyond: Embedded Event Manager (EEM) Scripting Community" at the following link:

A sample device configuration is provided below.

```plaintext
!
!-- Location where the Tcl script will be stored
!

event manager directory user policy disk0:/eem

!
!-- Define variable and set the monitoring interval

!-- as an integer (expressed in seconds)
!
```
event manager environment EEM_MONITOR_INTERVAL 60

!
!-- Define variable and set the threshold value as
!-- an integer for the number of retransmissions
!-- that determine if the TCP connection is hung
!-- (a recommended value to use is 15)
!

event manager environment EEM_MONITOR_THRESHOLD 15

!
!-- Define variable and set the value to "yes" to
!-- enable the clearing of hung TCP connections
!

event manager environment EEM_MONITOR_CLEAR yes

!
!-- Define variable and set to the TCP connection
!-- state or states that script will monitor, which
!-- can be a single state or a space-separated list
!-- of states
!

event manager environment EEM_MONITOR_STATES CLOSEWAIT

!
!-- Register the script as a Cisco EEM policy
!

event manager policy monitor-sockets.tcl

!
Secure Copy Authorization Bypass Vulnerability - 97261 [IOS]

Description
The server side of the Secure Copy (SCP) implementation in Cisco Internetwork Operating System (IOS) contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

The IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS Secure Copy Server service are not affected by this vulnerability.

This vulnerability does not apply to the IOS Secure Copy Client feature.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 97261: Verify Secure Copy Authorization Bypass Vulnerability[IOS]
Description

Secure Copy (SCP) is a protocol similar to the Remote Copy (RCP) protocol, which allows for the transfer of files between systems. The main difference between SCP and RCP is that in SCP, all aspects of the file transfer session, including authentication, occur in encrypted form, which makes SCP a more secure alternative than RCP. SCP relies on the Secure Shell (SSH) protocol, which uses TCP port 22 by default.

The server side of the Secure Copy implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

This vulnerability does not allow for authentication bypass; login credentials are verified and access is only granted if a valid username and password is provided. This vulnerability may cause authorization to be bypassed.

A device with the Secure Copy server enabled is vulnerable regardless of whether Authentication, Authorization, and Accounting (AAA) is enabled. If access control is enabled on the Virtual Terminal (vty) via the login command, which allows logins via Virtual Terminals, then the device is affected.

Applicable Platforms
Cisco IOS Devices.

Impact

Successful exploitation of the vulnerability described in this advisory may allow valid but unauthorized users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

Suggested Fix

If the IOS Secure Copy Server functionality is not needed then the vulnerability described in this document can be mitigated by disabling the Secure Copy server. The Secure Copy server can be disabled by executing the following command in global configuration mode:

```bash
no ip scp server enable
```

If the Secure Copy server cannot be disabled due to operational concerns, then no workarounds exist.

Secure Copy Privilege Escalation Vulnerability - 109323 [IOS]

Description

The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.
The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS SCP client feature.

Cisco has released free software updates that address this vulnerability.

There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

**Applicable Platforms**
Cisco IOS Devices

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT - 109323: Verify Secure Copy Privilege Escalation Vulnerability [IOS]

**Description**
SCP is a protocol similar to the Remote Copy (RCP) protocol, which allows the transfer of files between systems. The main difference between SCP and RCP is that in SCP, all aspects of the file transfer session, including authentication, occur in encrypted form, which makes SCP a more secure alternative than RCP. SCP relies on the Secure Shell (SSH) protocol, which uses TCP port 22 by default.

The Role-Based CLI Access feature allows the network administrator to define "views". Views are sets of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS software EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. For more information about the Role-Based CLI Access feature, reference


The server side of the SCP implementation in Cisco IOS software contains a vulnerability that allows authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be a SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow authenticated users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files. This configuration file may include passwords or other sensitive information.

Users confined to a CLI view can elevate their privileges by using SCP to write to the device's configuration. Note that a view can be attached to a user when defining the user in the local database (via the username <user name> view ... command), or by passing the attribute cli-view-name from an AAA server.

This vulnerability does not allow for authentication bypass; login credentials are verified and access is only granted if a valid username and password is provided. This vulnerability may cause authorization to be bypassed.
Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of the vulnerability described in this advisory may allow valid but unauthorized users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files. This configuration file may include passwords or other sensitive information.

Suggested Fix
If the Cisco IOS SCP server functionality is not needed then the vulnerability described in this document can be mitigated by disabling the SCP server or the CLI view feature. The SCP server can be disabled by executing the following command in global configuration mode:

no ip scp server enable

If the SCP server cannot be disabled due to operational concerns, then no workarounds exist. The risk posed by this vulnerability can be mitigated by following the best practices detailed in "Cisco Guide to Harden Cisco IOS Devices" at http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml. Please refer to the Obtaining Fixed Software section of this advisory for appropriate solutions to resolve this vulnerability.

Due to the nature of this vulnerability, networking best practices like access control lists (ACLs) and Control Plane Policing (CoPP) that restrict access to a device to certain IP addresses or subnetworks may not be effective. If access is already granted to a specific IP address or subnetwork, a user with low privileges will be able to establish an SCP session with the device, which would allow the user to exploit this vulnerability.

Secure Shell Denial of Services Vulnerabilities -99725 [IOS]

Description
The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device. The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 99725: Verify Secure Shell Denial of Services Vulnerabilities [IOS]
Description
Secure shell (SSH) was developed as a secure replacement for the telnet, ftp, rlogin, rsh, and rcp protocols, which allow for the remote access of devices. The main difference between SSH and older protocols is that SSH provides strong authentication, guarantees confidentiality, and uses encrypted transactions. The server side of the SSH implementation in Cisco IOS contains multiple vulnerabilities that allow an unauthenticated user to generate a spurious memory access or, in certain cases, reload the device. If the attacker is able to reload the device, these vulnerabilities could be repeatedly exploited to cause an extended Denial of Service (DoS) condition. A device with the SSH server enabled is vulnerable.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of these vulnerabilities may result in a spurious memory access or, in certain cases, reload the device potentially resulting in a DoS condition.

Suggested Fix
If disabling the IOS SSH Server is not feasible, the following workarounds may be useful to some customers in their environments.

Telnet
Telnet is not vulnerable to the issue described in this advisory and may be used as an insecure alternative to SSH. Telnet does not encrypt the authentication information or data; therefore, it should only be enabled for trusted local networks.

VTY Access Class
It is possible to limit the exposure of the Cisco device by applying a VTY access class to allow only known, trusted hosts to connect to the device via SSH.

The following example permits access to VTYs from the 192.168.1.0/24 netblock and the single IP address 172.16.1.2 while denying access from anywhere else:
```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 1 permit host 172.16.1.2
Router(config)# line vty 0 4
Router(config-line)# access-class 1 in
```
Different Cisco platforms support different numbers of terminal lines. Check your device’s configuration to determine the correct number of terminal lines for your platform.
Infrastructure ACLs (iACL)

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The ACL example shown below should be included as part of the deployed infrastructure access-list, which will protect all devices with IP addresses in the infrastructure IP address range.

A sample access list for devices running Cisco IOS is below:

```plaintext
!--- Permit SSH services from trusted hosts destined
!--- to infrastructure addresses.

access-list 150 permit tcp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK eq 22

!--- Deny SSH packets from all other sources destined to infrastructure addresses.

access-list 150 deny tcp any INFRASTRUCTURE_ADDRESSES MASK eq 22

!--- Permit all other traffic to transit the device.

access-list 150 permit IP any any
```

interface serial 2/0
  ip access-group 150 in

The white paper titled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained here:


Control Plane Policing (CoPP)

The Control Plane Policing (CoPP) feature may be used to mitigate these vulnerabilities. In the following example, only SSH traffic from trusted hosts and with 'receive' destination IP addresses is permitted to reach the route processor (RP).

Note: Dropping traffic from unknown or untrusted IP addresses may affect hosts with dynamically assigned IP addresses from connecting to the Cisco IOS device.

```plaintext
access-list 152 deny tcp TRUSTED_ADDRESSES MASK any eq 22
  access-list 152 permit tcp any any eq 22

!--- Permit all other traffic to transit the device.

access-list 150 permit IP any any
```

interface serial 2/0
  ip access-group 150 in
match access-group 152
!
!
policy-map COPP-INPUT-POLICY
class COPP-KNOWN-UNDESIRABLE
drop
!
control-plane
	service-policy input COPP-INPUT-POLICY

In the above CoPP example, the ACL entries that match the exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action are not affected by the policy-map drop function.

CoPP is available in Cisco IOS release trains 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T.

Additional information on the configuration and use of the CoPP feature can be found at the following URL:

Session Initiation Protocol Denial of Services Vulnerability -111448 [IOS]

Description
Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS® that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled. Remote code execution may also be possible.

Cisco has released free software updates that address these vulnerabilities. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerabilities.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 111448: Verify Session Initiation Protocol Denial of Services Vulnerability [IOS]
Description

SIP is a popular signaling protocol that is used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination. Voice and video are the most popular types of sessions that SIP handles, but the protocol has the flexibility to accommodate other applications that require call setup and termination. SIP call signaling can use UDP (port 5060), TCP (port 5060), or TLS (TCP port 5061) as the underlying transport protocol.

Three vulnerabilities exist in the SIP implementation in Cisco IOS Software that may allow a remote attacker to cause a device reload, or execute arbitrary code. These vulnerabilities are triggered when the device running Cisco IOS Software processes malformed SIP messages.

In cases where SIP is running over TCP transport, a TCP three-way handshake is necessary to exploit these vulnerabilities.

Applicable Platforms

Cisco IOS Devices.

Impact

Successful exploitation of the vulnerabilities in this advisory may result in a reload of the device. Repeated exploitation could result in a sustained denial of service condition. There is a potential to execute arbitrary code. In the event of successful remote code execution, device integrity could be completely compromised.

Suggested Fix

If the affected Cisco IOS device requires SIP for VoIP services, SIP cannot be disabled, and no workarounds are available. Users are advised to apply mitigation techniques to help limit exposure to the vulnerabilities. Mitigation consists of allowing only legitimate devices to connect to affected devices. To increase effectiveness, the mitigation must be coupled with anti-spoofing measures on the network edge. This action is required because SIP can use UDP as the transport protocol.

Additional mitigations that can be deployed on Cisco devices within the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager Express and Cisco IOS Software H.323 and Session Initiation Protocol Denial of Service Vulnerabilities".

Disable SIP Listening Ports

For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. Some versions of Cisco IOS Software allow administrators to disable SIP with the following commands:

- sip-ua
- no transport udp
- no transport tcp
- no transport tcp tls

Warning: When applying this workaround to devices that are processing Media Gateway Control Protocol (MGCP) or H.323 calls, the device will not stop SIP processing while active calls are being processed. Under these circumstances, this workaround should be implemented during a maintenance window when active calls can be briefly stopped.

The show udp connections, show tcp brief all, and show processes | include SIP commands can be used to confirm that the SIP UDP and TCP ports are closed after applying this workaround.
Depending on the Cisco IOS Software version in use, the output from the show ip sockets command may still show the SIP ports open, but sending traffic to them will cause the SIP process to emit the following message:

*Feb 2 11:36:47.691: sip_udp_sock_process_read: SIP UDP Listener is DISABLED

**Control Plane Policing**

For devices that need to offer SIP services it is possible to use Control Plane Policing (CoPP) to block SIP traffic to the device from untrusted sources. Cisco IOS Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to specific network configurations:

```
!-- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.

!-- Everything else is not trusted. The following access list is used

!-- to determine what traffic needs to be dropped by a control plane

!-- policy (the CoPP feature.) If the access list matches (permit)

!-- then traffic will be dropped and if the access list does not

!-- match (deny) then traffic will be processed by the router.

access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060

access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5060

access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5061

access-list 100 deny udp host 172.16.1.1 any eq 5060

access-list 100 deny tcp host 172.16.1.1 any eq 5060

access-list 100 deny tcp host 172.16.1.1 any eq 5061

access-list 100 permit udp any any eq 5060

access-list 100 permit tcp any any eq 5060

access-list 100 permit tcp any any eq 5061

access-list 100 permit udp any any eq 5060

access-list 100 permit tcp any any eq 5060

access-list 100 permit tcp any any eq 5061

!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
```
Understanding Compliance and Audit Manager (CAAM) Policies

!-- traffic in accordance with existing security policies and

!-- configurations for traffic that is authorized to be sent

!-- to infrastructure devices.

!-- Create a Class-Map for traffic to be policed by

!-- the CoPP feature.

   class-map match-all drop-sip-class

match access-group 100

!-- Create a Policy-Map that will be applied to the

!-- Control-Plane of the device.

   policy-map control-plane-policy

   class drop-sip-class

   drop

!-- Apply the Policy-Map to the Control-Plane of the

!-- device.

   control-plane

service-policy input control-plane-policy

**Warning:** Because SIP can use UDP as a transport protocol, it is possible to easily spoof the IP address of the sender, which may defeat access control lists that permit communication to these ports from trusted IP addresses.

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Additional information on the configuration and use of the CoPP feature can be found at http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html and http://www.cisco.com/en/US/docs/ios/redirect/eol.html.
Syslog Crash -13660 [IOS]

Description
Certain versions of Cisco IOS software may crash or hang when they receive invalid user datagram protocol (UDP) packets sent to their "syslog" ports (port 514). At least one commonly-used Internet scanning tool generates packets which can cause such crashes and hangs. This fact has been announced on public Internet mailing lists which are widely read both by security professionals and by security "crackers", and should be considered public information.

See "Cisco IOS Syslog Crash." at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability. Rule 1

Rule
PSIRT - 111448: Verify Session Initiation Protocol Denial of Services Vulnerability [IOS]

Description
Certain versions of Cisco IOS software may crash or hang when they receive invalid user datagram protocol (UDP) packets sent to their "syslog" ports (port 514). At least one commonly-used Internet scanning tool generates packets which can cause such crashes and hangs. This fact has been announced on public Internet mailing lists which are widely read both by security professionals and by security "crackers", and should be considered public information. See "Cisco IOS Syslog Crash." at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices.

Impact
Attackers can cause Cisco IOS devices to crash and reload. Furthermore, an attacker can repeat the process at will. By striking continuously, an attacker might be able to completely disable a Cisco IOS device until that device was reconfigured by its administrator.

Some Cisco IOS devices have been observed to hang instead of crashing when attacked. These devices do not recover until manually restarted by reset or power cycle. This means that it might be necessary for an administrator to physically visit an attacked device in order to recover from the attack, even if the attacker is no longer actively sending any traffic.

Some devices have crashed without providing stack traces; devices crashed using this vulnerability may indicate that they were "restarted by power-on", even when that is not actually the case.

Suggested Fix
You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to its port 514. This can be done either using packet filtering on surrounding devices, or by using input access list filtering on the affected IOS device itself.
TCP -72318 [IOS]

Description
The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition. This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 72318: Verify Crafted TCP Packet Can Cause Denial of Service [IOS]

Description
TCP is the transport layer protocol designed to provide connection-oriented, reliable delivery of a data stream. To accomplish this, TCP uses a mixture of flags to indicate state and sequence numbers to identify the order in which the packets are to be reassembled. TCP also provides a number, called an acknowledgement number, that is used to indicate the sequence number of the next packet expected. The full specification of the TCP protocol can be found at http://www.ietf.org/rfc/rfc0793.txt.

Cisco IOS devices that are configured to receive TCP packets are exposed to this issue. This Advisory does not apply to traffic that is transiting the device.

Certain crafted packets destined to an IPv4 address assigned to a physical or virtual interface on a Cisco IOS device may cause the device to leak a small amount of memory. Over time, such a memory leak may lead to memory exhaustion and potentially degraded service.

Although this is an issue with TCP, it is not required to complete the TCP 3-way handshake in order for the memory leak to be triggered. Therefore, TCP packets with a spoofed source address may trigger the leak.

The following document contains additional information on how to identify if your router is suffering from a memory leak in Processor memory:

Applicable Platforms
Cisco IOS Devices

Impact
Successful exploitation of the vulnerability may result in a small amount of processor memory to leak, which may lead to degraded service. This issue will not resolve over time, and will require a device reset to recover the leaked memory.
This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the device will not trigger this issue.

**Suggested Fix**

ACLs can be used as an effective mitigation technique for the Crafted TCP transit enforcement points.

Anti-spoof protection in the form of unicast Reverse Path Forwarding (uRPF) can provide limited mitigation if properly configured.

Anti-Spoofing and Embryonic Connection Limiting with TCP-Intercept can also be used mitigating this vulnerability.

### TCP Conn Reset -50960 [IOS]

**Description**

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain a TCP stack are susceptible to this vulnerability.

This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer), and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router).

See “TCP Vulnerabilities in Multiple IOS-Based Cisco Products” at Cisco Security Advisories website.

**Applicable Platforms**

Cisco IOS Devices

**References**

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**

PSIRT - 50960: TCP connection reset vulnerabilities [IOS]

**Description**

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application,
the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain a TCP stack are susceptible to this vulnerability.

This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer), and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router).

See "TCP Vulnerabilities in Multiple IOS-Based Cisco Products" at Cisco Security Advisories website

**Applicable Platforms**
Cisco IOS Devices.

**Impact**
The impact will be different for each specific protocol. While in the majority of cases a TCP connection will be automatically re-established, in some specific protocols a second order of consequences may have a larger impact than tearing down the connection itself.

**Suggested Fix**
The workaround for BGP is to configure MD5 secret for each session between peers. There are no workarounds available to mitigate the effects of this vulnerability on Cisco IOS Firewall.

**TCP Denial of Service Service Vulnerability -112099 [IOS]**

**Description**
Cisco IOS Software Release, 15.1(2)T is affected by a denial of service (DoS) vulnerability during the TCP establishment phase. The vulnerability could cause embryonic TCP connections to remain in a SYNRCVD or SYNSENT state. Enough embryonic TCP connections in these states could consume system resources and prevent an affected device from accepting or initiating new TCP connections, including any TCP-based remote management access to the device.

No authentication is required to exploit this vulnerability. An attacker does not need to complete a three-way handshake to trigger this vulnerability; therefore, this vulnerability can be exploited using spoofed packets. This vulnerability may be triggered by normal network traffic.

Cisco has released Cisco IOS Software Release 15.1(2)T0a to address this vulnerability.

**Applicable Platforms**
Cisco IOS Devices

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Rule 1

Rule
PSIRT - 112099: Verify TCP DoS vulnerability [IOS]

Description
TCP provides reliable data transmission services in packet-switched network environments. TCP corresponds to the transport layer (Layer 4) of the OSI reference model. Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.

When TCP connections are terminated in Cisco IOS Software, they are allocated a transmission control block (TCB). All allocated TCBs, associated TCP port numbers, and the TCP state are displayed in the output of the `show tcp brief all` command-line interface (CLI) command.

Cisco IOS Software version 15.1(2)T contains a vulnerability that could cause an embryonic TCP connection to remain in SYNRCVD or SYSENTER state without a further TCP state transition. Examining the output of the `show tcp brief all` command multiple times will indicate if TCP sessions remain in one of these states.

This vulnerability is triggered only by TCP traffic that is terminated by or originated from the device. Transit traffic will not trigger this vulnerability.

Both connections to and from the router could trigger this vulnerability. An example of a connection to the router is that you may still be able to ping the device, but fail to establish a TELNET or SSH connection to the device. For example, an administrator may still be able to ping the device but fail to establish a Telnet or SSH connection to the device. Administrators who attempt a Telnet or a SSH connection to a remote device from the CLI prompt will encounter a hung session and the “Trying <ip address|hostname> ...” prompt. The connection that is initiated or terminated by the router can be removed from the socket table by clearing the associated TCB with the `clear tcp tcb 0x<address>` command.

Devices could be vulnerable if examining the output of the CLI command `debug ip tcp transactions`, displays the error messages connection queue limit reached: port <port number> or No wild listener: port <port number>.

Devices could also be vulnerable if output from repetitive `show tcp brief all` CLI commands indicates many TCBs in the state SYNRCVD or SYSENTER.

The following example shows a device that has several HTTP, SSH, and Telnet sessions in the TCP SYNRCVD state:

Example#show tcp brief all

<table>
<thead>
<tr>
<th>TCB</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>(state)</th>
</tr>
</thead>
<tbody>
<tr>
<td>07C2D6C8</td>
<td>192.168.0.2.443</td>
<td>192.168.0.5.11660</td>
<td>SYNRCVD</td>
</tr>
<tr>
<td>07C38128</td>
<td>192.168.0.2.23</td>
<td>192.168.0.5.35018</td>
<td>SYNRCVD</td>
</tr>
<tr>
<td>07C2DD60</td>
<td>192.168.0.2.443</td>
<td>192.168.0.5.19316</td>
<td>SYNRCVD</td>
</tr>
<tr>
<td>07C2A8A0</td>
<td>192.168.0.2.80</td>
<td>192.168.0.5.13818</td>
<td>SYNRCVD</td>
</tr>
</tbody>
</table>

Any TCP sessions can be cleared by clearing the associated TCB with `clear tcp tcb 0x<address>`.

Alternatively, administrators can clear all TCBs at once by issuing `clear tcp tcb *`.

Note: This will clear all active and hung TCP connections.

Some TCP application specific information is provided in the following sections:

Telnet and SSH
Telnet can not be explicitly disabled on a Cisco IOS device. Configuring transport input none on the vty lines of a vulnerable device will prevent it from being exploited on TCP port 23. However, if the Cisco IOS SSH server feature is configured on the device, transport input none will not prevent the device from being exploited on TCP port 22.

Configuration of vty access control lists can partially mitigate this vulnerability because the vulnerability can be exploited using spoofed IP source addresses.

**Border Gateway Protocol**

Routers that are configured with Border Gateway Protocol (BGP) can be protected further by using the Generalized Time to Live (TTL) Security Mechanism (GTSM) feature. GTSM allows users to configure the expected TTL of a packet between a source and destination address. Packets that fail the GTSM check will be dropped before TCP processing occurs, which prevents an attacker from exploiting this vulnerability through BGP. GTSM is implemented with the command ttl-security hops.

Further information on protecting BGP can be found in Protecting Border Gateway Protocol for the Enterprise.

TCP MD5 Authentication for BGP does not prevent this vulnerability from being exploited.

**Applicable Platforms**

Cisco IOS Devices.

**Impact**

Successful exploitation of this vulnerability may prevent some TCP applications on Cisco IOS Software from accepting any new connections. Exploitation could also prevent remote access to the affected system via the vtyts. Remote access to the affected device via out-of-band connectivity to the console port should still be available.

**Suggested Fix**

The only complete workaround to mitigate this vulnerability is to disable the specific features that make a device vulnerable, if this action is feasible.

Allowing only legitimate devices to connect to affected devices will help limit exposure to this vulnerability. Refer to the following Control Plane Policing and Configuring Infrastructure Access Lists subsections for further details. Because a TCP three-way handshake is not required, the mitigation must be combined with anti-spoofing measures on the network edge to increase effectiveness.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.

**Cisco Guide to Harden Cisco IOS Devices**

The Cisco Guide to Harden Cisco IOS Devices provides examples of many useful techniques to mitigate TCP state manipulation vulnerabilities. These include:

- Infrastructure Access Control Lists (iACL)
- Receive Access Control Lists (rACL)
- Transit Access Control Lists (tACL)
- vty Access Control Lists
- Control Plane Policing (CoPP)
- Control Plane Protection (CPPr)

For more information on these topics, consult Cisco Guide to Harden Cisco IOS Devices.

**CoPP**
For devices that need to offer TCP services, administrators can use CoPP to block TCP traffic from untrusted sources that is destined to the affected device. Cisco IOS Software Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to specific network configurations:

```cisco
!!-- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.
!-- Everything else is not trusted. The following access list is used
!-- to determine what traffic needs to be dropped by a control plane
!-- policy (the CoPP feature.) If the access list matches (permit),
!-- then traffic will be dropped. If the access list does not
!-- match (deny), then traffic will be processed by the router.
!-- Note that TCP ports 22 and 23 are examples; this
!-- configuration needs to be expanded to include all used
!-- TCP ports.
!
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 23
access-list 100 deny tcp host 172.16.1.1 any eq 22
access-list 100 deny tcp host 172.16.1.1 any eq 23
access-list 100 permit tcp any any
!
!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices.
!-- Create a class map for traffic that will be policed by
!-- the CoPP feature.
!
class-map match-all drop-tcp-class
  match access-group 100
!
!-- Create a policy map that will be applied to the
!-- Control Plane of the device, and add the "drop-tcp-traffic"
!-- class map.
!
policy-map control-plane-policy
```
Understanding Compliance and Audit Manager (CAAM) Policies

class drop-tcp-class
  drop
!
!-- Apply the policy map to the control plane of the
device.
!
control-plane
  service-policy input control-plane-policy

Because a TCP three-way handshake is not required to exploit this vulnerability, it is possible to spoof the IP address of the sender, which could defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses.

In the preceding CoPP example, the access control entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Additional information on the configuration and use of the CoPP feature can be found at Control Plane Policing Implementation Best Practices and Control Plane Policing.

Configuring iACLs

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper Protecting Your Core: Infrastructure Protection Access Control Lists presents guidelines and recommended deployment techniques for infrastructure protection ACLs.

BGP Considerations

GTSM can help prevent exploitation of this vulnerability by means of the BGP port because packets that originate from devices that do not pass the TTL check configured by GTSM are dropped before any TCP processing occurs. For information on GTSM refer to BGP Support for TTL Security Check and BGP Time To Live Security Check.

Embedded Event Manager (EEM)

A Cisco IOS Embedded Event Manager (EEM) policy that is based on Tool Command Language (Tcl) can be used on vulnerable Cisco IOS devices to identify and detect a hung, extended, or indefinite TCP connection that is caused by this vulnerability. The policy allows administrators to monitor TCP connections on a Cisco IOS device. When Cisco IOS EEM detects potential exploitation of this vulnerability, the policy can trigger a response by sending a syslog message or a Simple Network Management Protocol (SNMP) trap to clear the TCP connection. The example policy provided in this document is based on a Tcl script that monitors and parses the output from two commands at defined intervals, produces a syslog message when the monitor threshold reaches its configured value, and can reset the TCP connection.

The Tcl script is available for download at the Embedded Event Manager (EEM) Scripting Community at the following link

https://supportforums.cisco.com/community/netpro/network-infrastructure/eem, and the device sample configuration is provided below.

!  !-- Location where the Tcl script will be stored
event manager directory user policy disk0:/eem

!  

!-- Define variable and set the monitoring interval
!-- as an integer (expressed in seconds)
!

event manager environment EEM_MONITOR_INTERVAL 60

!

!-- Define variable and set the threshold value as
!-- an integer for the number of retransmissions
!-- that determine if the TCP connection is hung
!-- (a recommended value to use is 15)
!

event manager environment EEM_MONITOR_THRESHOLD 15

!

!-- Define variable and set the value to "yes" to
!-- enable the clearing of hung TCP connections
!

event manager environment EEM_MONITOR_CLEAR yes

!

!-- Define variable and set to the TCP connection
!-- state or states that script will monitor, which
!-- can be a single state or a space-separated list
!-- of states
!

event manager environment EEM_MONITOR_STATES SYNRCVD SYNSENT

!
!-- Register the script as a Cisco EEM policy
!

event manager policy monitor-sockets.tcl

TCP ISN -13631 [IOS]

Description
Cisco IOS Software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.

This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.

See "Cisco IOS Software TCP Initial Sequence Number Randomization Improvements." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 13631: Verify TCP Initial Sequence Number Randomization Vulnerability [IOS]

Description
To provide reliable delivery in the Internet, the Transmission Control Protocol (TCP) makes use of a sequence number in each packet to provide orderly reassembly of data after arrival, and to notify the sending host of the successful arrival of the data in each packet.

TCP sequence numbers are 32-bit integers in the circular range of 0 to 4,294,967,295. The host devices at both ends of a TCP connection exchange an Initial Sequence Number (ISN) selected at random from that range as part of the setup of a new TCP connection. After the session is established and data transfer begins, the sequence number is regularly augmented by the number of octets transferred, and transmitted to the other host. To prevent the receipt and reassembly of duplicate or late packets in a TCP stream, each host maintains a "window", a range of values close to the expected sequence number, in which the sequence number in an arriving packet must fall if it is to be accepted. Assuming a packet arrives with the correct source and destination IP addresses, source and destination port numbers, and a sequence number within the allowable window, the receiving host will accept the packet as genuine.

This method provides reasonably good protection against accidental receipt of unintended data. However, to guard against malicious use, it should not be possible for an attacker to infer a particular number in the sequence. If the initial sequence number is not chosen randomly or if it is incremented in a non-random manner between the initialization of subsequent TCP sessions, then it is possible, with varying degrees of
success, to forge one half of a TCP connection with another host in order to gain access to that host, or hijack an existing connection between two hosts in order to compromise the contents of the TCP connection. To guard against such compromises, ISNs should be generated as randomly as possible.

**Applicable Platforms**
Cisco IOS Devices.

**Impact**
Forged packets can be injected into a network from a location outside its boundary so that they are trusted as authentic by the receiving host, thus resulting in a failure of integrity. Such packets could be crafted to gain access or make some other modification to the receiving system in order to attain some goal, such as gaining unauthorized interactive access to a system or compromising stored data.

From a position within the network where it is possible to receive the return traffic (but not necessarily in a position that is directly in the traffic path), a greater range of violations is possible. For example, the contents of a message could be diverted, modified, and then returned to the traffic flow again, causing a failure of integrity and a possible failure of confidentiality.

**Note:** Any compromise using this vulnerability is only possible for TCP sessions that originate or terminate on the affected Cisco device itself. It does not apply to TCP traffic that is merely forwarded through the device.

**Suggested Fix**
There is no specific configurable workaround to directly address the possibility of predicting a TCP Initial Sequence Number. To prevent malicious use of this vulnerability from inside the network, ensure that transport that makes interception and modification detectable, if not altogether preventable, is in use as appropriate. Examples include using IPSEC or SSH to the Cisco device for interactive session, MD5 authentication to protect BGP sessions, strong authentication for access control, and so on.

**TCP State Manipulation DoS Vulnerability -109444 [IOS]**

**Description**
Multiple Cisco products are affected by denial of service (DoS) vulnerability that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

**Applicable Platforms**
Cisco IOS Devices

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.
Rule 1

Rule
PSIRT - 109444: Verify TCP State Manipulation DoS Vulnerability [IOS]

Description
Multiple Cisco products are affected by DoS vulnerabilities in the TCP protocol. By manipulating the state of TCP connections, an attacker could force a system that is under attack to maintain TCP connections for long periods of time, or indefinitely in some cases. With a sufficient number of open TCP connections, the attacker may be able to cause a system to consume internal buffer and memory resources, resulting in new TCP connections being denied access to a targeted port or an entire system. A system reboot may be required to restore full system functionality. A full TCP three-way handshake is required to exploit these vulnerabilities.

Network devices are not directly impacted by TCP state manipulation DoS attacks transiting a device; however, network devices that maintain the state of TCP connections may be impacted. If the attacker can establish enough TCP connections through a transit device that maintains TCP state, device resources may be exhausted and prevent the device from processing new TCP connections, resulting in a DoS condition. If an affected device that forwards traffic (that is, routes) in a network is the target of a TCP state manipulation attack, the attacker could cause a network-impacting DoS condition.

Cisco IOS Software
All Cisco IOS Software versions are affected by this vulnerability. A device running Cisco IOS Software that is under attack will have numerous hung TCP connections in the FINWAIT1 state. The show tcp brief command can be used to display the hung TCP connections. The following is example output showing an attack in progress.

Router#show tcp brief | include FIN

<table>
<thead>
<tr>
<th>LOCAL ADDRESS</th>
<th>REMOTE ADDRESS</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>63D697C4</td>
<td>192.168.1.10.80</td>
<td>FINWAIT1</td>
</tr>
<tr>
<td>63032A28</td>
<td>192.168.1.10.80</td>
<td>FINWAIT1</td>
</tr>
<tr>
<td>645F8068</td>
<td>192.168.1.10.80</td>
<td>FINWAIT1</td>
</tr>
<tr>
<td>630323F4</td>
<td>192.168.1.10.80</td>
<td>FINWAIT1</td>
</tr>
<tr>
<td>63D69190</td>
<td>192.168.1.10.80</td>
<td>FINWAIT1</td>
</tr>
</tbody>
</table>

This method provides reasonably good protection against accidental receipt of unintended data. However, to guard against malicious use, it should not be possible for an attacker to infer a particular number in the sequence. If the initial sequence number is not chosen randomly or if it is incremented in a non-random manner between the initialization of subsequent TCP sessions, then it is possible, with varying degrees of success, to forge one half of a TCP connection with another host in order to gain access to that host, or hijack an existing connection between two hosts in order to compromise the contents of the TCP connection. To guard against such compromises, ISNs should be generated as randomly as possible.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of the TCP state manipulation vulnerabilities may result in a DoS condition where new TCP connections are not accepted on an affected system. Repeated exploitation may result in a sustained DoS condition. A reboot may be required to recover affected systems.
Suggested Fix
The Cisco Guide to Harden Cisco IOS Devices provides examples of many useful techniques to mitigate against the TCP state manipulation vulnerabilities. These include:

- Infrastructure Access Control Lists (iACL)
- Receive Access Control Lists (rACL)
- Transit Access Control Lists (tACL)
- VTY Access Control Lists
- Control Plane Policing (CoPP)
- Control Plane Protection (CPPr)
- Management Plane Policing (MPP)

For more information on the topics listed above, consult the Cisco Guide to Harden Cisco IOS Devices at the following link:


Telnet DoS -61671 [IOS]

Description
A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Data Link Switching (DLSw) and protocol translation connections may also be affected. Telnet, reverse telnet, RSH, SSH, DLSw and protocol translation sessions established prior to exploitation are not affected.

All other device services will operate normally. Services such as packet forwarding (excluding DLSw and protocol translation per above), routing protocols and all other communication to and through the device are not affected.

See "Cisco Telnet Denial of Service Vulnerability." at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 61671: Verify Telnet DoS Vulnerability [IOS]

Description
A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access
to the Cisco device. Data Link Switching (DLSw) and protocol translation connections may also be affected. Telnet, reverse telnet, RSH, SSH, DLSw and protocol translation sessions established prior to exploitation are not affected.

All other device services will operate normally. Services such as packet forwarding (excluding DLSw and protocol translation per above), routing protocols and all other communication to and through the device are not affected.

See "Cisco Telnet Denial of Service Vulnerability." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices.

Impact
Exploitation of this vulnerability may result in the denial of new telnet, reverse telnet, RSH, SSH, SCP, DLSw, protocol translation and HTTP connections to a device running IOS. Other access to the device via the console or SNMP is not affected. The device will remain in this state until the problematic TCP connection is cleared, or the device is reloaded (which will clear the problematic session). If no other access methods are available, exploitation of this vulnerability could deny remote access to the device.

Suggested Fix
Enable SSH and disable Telnet access to the device.

Telnet Option-10939 [IOS]

Description
A defect in multiple Cisco IOS software versions will cause a Cisco router to reload unexpectedly when the router is tested for security vulnerabilities by security scanning software programs. The defect can be exploited repeatedly to produce a consistent denial of service (DoS) attack. See "Cisco IOS Software TELNET Option Handling Vulnerability." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 10939: Verify TELNET Option Handling Vulnerability [IOS]

Description
Software packages are available from various commercial and free sites that perform automated remote tests for computer security vulnerabilities by scanning computers on a network for known security flaws. Two security vulnerabilities associated with several UNIX-based platforms are the subject of two specific tests that have the same effect on vulnerable Cisco routers. The scanning program is asserting the Telnet ENVIRON option, #36, before the router indicates that it is willing to accept it, and this causes the router to reload unexpectedly.
Applicable Platforms
Cisco IOS Devices.

Impact
Can be used to mount a consistent and repeatable denial of service (DoS) attack on any vulnerable Cisco product, which may result in violations of the availability aspects of a customer's security policy. This defect by itself does not cause the disclosure of confidential information nor allow unauthorized access.

Suggested Fix
Disable Telnet and use SSH to access the device.

Timers Heap Overflow -68064 [IOS]

Description
The Cisco Internetwork Operating System (IOS) may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

(See "IOS Heap-based Overflow Vulnerability in System Timers" at Cisco Security Advisories website for more information.)

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 68064: Verify IOS Heap-based Overflow Vulnerability in System Timers [IOS]

Description
The Cisco Internetwork Operating System (IOS) may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitations of heap-based buffer overflow vulnerabilities in Cisco IOS software often result in a Denial of Service because the exploit causes the router to crash and reload due to inconsistencies in running memory. In some cases it is possible to overwrite areas of system memory and execute arbitrary code from those locations. In the event of successful remote code execution, device integrity will have been completely compromised.
Suggested Fix

There are no workarounds or configuration changes that will implement counter-measures equivalent to the increased integrity checks on system timers that have been introduced. In order to reduce the potential for system timer-related arbitrary code execution, an IOS upgrade is necessary.
Tunnels DoS Vulnerability -109482 [IOS]

Description
Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.
Cisco has released free software updates that address this vulnerability.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 109482: Verify Tunnels DoS Vulnerability [IOS]

Description
A tunnel protocol encapsulates a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link between internetworking devices over an IP network.
Cisco Express Forwarding is a Layer 3 IP switching technology. It improves network performance and scalability for networks with high and dynamic traffic patterns.
Devices that are running Cisco IOS Software and configured for GRE, IPinIP, Generic Packet Tunneling in IPv6 or IPv6 over IP tunnels tunnels and Cisco Express Forwarding may reload upon switching a specially crafted malformed packets. Please note that using PPTP creates GRE tunnels that are transparent to the end user so devices configured for PPTP are vulnerable if they are configured on an affected software version. Using MVPN also creates GRE tunnels that are transparent to the end user. However MVPN configurations are not vulnerable.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of the vulnerability may result in the reload of an affected system, causing a DoS condition.

Suggested Fix
Disabling Cisco Express Forwarding will mitigate this vulnerability. It can be disabled in two ways:

Disabling Cisco Express Forwarding Globally
Cisco Express Forwarding can be globally disabled by using the no ip cef and no ipv6 cef global configuration command.

Disabling Cisco Express Forwarding on Tunnel Interfaces
Cisco Express Forwarding can also be disabled on individual tunnel interfaces. To be effective, it must be disabled on all tunnel interfaces configured on an affected device. Cisco Express Forwarding can be disabled on individual interfaces as shown in the following example:
interface Tunnel [interface-ID]
   no ip route-cache cef
   no ipv6 cef

Note: Disabling Cisco Express Forwarding may have significant performance impact and is not recommended.

Additional mitigations that can be deployed on Cisco devices in the network are available in the Cisco Applied Mitigation Bulletin companion document.

Unified Communications Manager Express Vulnerability -110451

Description
Cisco IOS devices that are configured for Cisco Unified Communications Manager Express (CME) and the Extension Mobility feature are vulnerable to a buffer overflow vulnerability. Successful exploitation of this vulnerability may result in the execution of arbitrary code or a Denial of Service (DoS) condition on an affected device.

Cisco has released free software updates that address this vulnerability.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 110451: Verify Unified Communications Manager Express Vulnerability [IOS]

Description
Cisco Unified CME is the call processing component of an enhanced IP telephony solution that is integrated into Cisco IOS.
The Extension Mobility feature in Cisco Unified CME provides the benefit of phone mobility for end users. A user login service allows phone users to temporarily access a physical phone other than their own phone and utilize their personal settings, such as directory number, speed-dial lists, and services, that is assigned to their own desk phone. The phone user can make and receive calls on that phone using the same personal directory number as is on their own desk phone. More information on Extension Mobility feature is available at the following URL:


A vulnerability in the login section of the Extension Mobility feature may allow an unauthenticated attacker to execute arbitrary code or cause a Denial of Service (DoS) condition. Such packets can only come from registered phone IP addresses in the form of HTTP requests. If the auto-registration feature is enabled, an attacker can register its IP address and subsequently send a crafted payload to exploit this vulnerability. The auto-registration feature is enabled by default. More information on auto-registration can be found at the following link:


Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of this vulnerability may result in the execution of arbitrary code or a Denial of Service (DoS) condition on an affected device.

Suggested Fix
There are no workarounds to mitigate this vulnerability, other than disabling Extension Mobility. However, auto-registration can be disabled to make exploitation more difficult. Auto-registration can be disabled by the following command:

telephony-service
  no auto-reg-ephone

Before disabling auto-registration, all phone MAC addresses need to be explicitly defined on the Cisco Unified CME. Otherwise phones will not be able to register. More information on auto-registration can be found at the following link:


Additional mitigations that can be deployed on Cisco devices in the network are available in the Cisco Applied Mitigation Bulletin companion document.

User Datagram protocol delivery issue -100638 [IOS]

Description
A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.
(See "IOS User Datagram Protocol Delivery Issue For IPv4/IPv6 Dual-stack Routers" at Cisco Security Advisories website for more information.)

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule

Description
A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected. Only Cisco IOS software releases that have IPv6 enabled are affected by this vulnerability. In order to be vulnerable both support for IPv6 protocol and IPv4 UDP-based services must be enabled on the device. The IPv6 is not enabled by default in Cisco IOS software.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of the vulnerability can result in one of the following two conditions:

1. The device will crash if RSVP service is configured on the interface.
2. Any other affected IPv4 UDP-based service will prevent the interface from receiving additional traffic. Only the interface on which the vulnerability is exploited will be affected.

Suggested Fix
A blocked interface can be unblocked by disabling the UDP service whose packets are blocking the interface. This procedure can restore normal operation of the interface without rebooting the device. The procedure for disabling vulnerable services are described in the "If IPv4 UDP-based Services Are Not Required" section.

The following workarounds are options that may be available depending on the Cisco IOS software running on the device and the operating environment. The workarounds depend on whether IPv6 or any of the affected UDP services are required for the normal operation.

If IPv6 Protocol Is Not Required
Disable IPv6. To disable IPv6 use the following commands:
Router(config)#interface FastEthernet0/0
Router(config-if)#no ipv6 address

or

Router(config)#interface FastEthernet0/0
Router(config-if)#no ipv6 enable

If RSVP is the only affected service that is configured it is sufficient to disable IPv6 only on the interface where RSVP is configured. If any other affected UDP service is present on the device then IPv6 would have to be disabled from all interfaces.

**If IPv4 UDP-based Services Are Not Required**
Disable all affected IPv4 UDP-based services.

**Virtual Private Dial-up Network DoS Vulnerability -97278 [IOS]**

**Description**
Two vulnerabilities exist in the virtual private dial-up network (VPDN) solution when Point-to-Point Tunneling Protocol (PPTP) is used in certain Cisco IOS releases prior to 12.3. PPTP is only one of the supported tunneling protocols used to tunnel PPP frames within the VPDN solution.

The first vulnerability is a memory leak that occurs as a result of PPTP session termination. The second vulnerability may consume all interface descriptor blocks on the affected device because those devices will not reuse virtual access interfaces. If these vulnerabilities are repeatedly exploited, the memory and/or interface resources of the attacked device may be depleted. (See for more information.)

**Applicable Platforms**
Cisco IOS Devices

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT - 97278: Verify Virtual Private Dial-up Network DoS Vulnerability [IOS]
Description

Two vulnerabilities exist in the virtual private dial-up network (VPDN) solution when Point-to-Point Tunneling Protocol (PPTP) is used in certain Cisco IOS releases prior to 12.3. PPTP is only one of the supported tunneling protocols used to tunnel PPP frames within the VPDN solution.

The first vulnerability is a memory leak that occurs as a result of PPTP session termination. The second vulnerability may consume all interface descriptor blocks on the affected device because those devices will not reuse virtual access interfaces. If these vulnerabilities are repeatedly exploited, the memory and/or interface resources of the attacked device may be depleted.

Cisco has made free software available to address these vulnerabilities for affected customers.

There are no workarounds available to mitigate the effects of these vulnerabilities.

Applicable Platforms

Cisco IOS Devices.

Impact

Successful exploitation of the vulnerability may result in a memory leak of processor memory or consumption of all available IDBs on the device. With continued exploitation, the device will deplete its processor memory or reach an IDB limit. Both impacts would result in a denial of service condition for the device.

Suggested Fix

There are no workarounds for these vulnerabilities. Cisco recommends upgrading to the fixed version of Cisco IOS.
Vulnerabilities Found by PROTOS IPSec Test Suite -68158 [IOS]

Description
Multiple Cisco products contain vulnerabilities in the processing of IPSec IKE (Internet Key Exchange) messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for IPSec and can be repeatedly exploited to produce a denial of service. See "Multiple Vulnerabilities Found by PROTOS IPSec Test Suite" at Cisco Security Advisories website.

Applicable Platforms
Cisco IOS Devices

References
For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 68158: Verify Multiple Vulnerabilities Found by PROTOS IPSec Test Suite [IOS]

Description
IP Security, or IPSec, is a set of protocols standardized by the IETF to support encrypted and/or authenticated transmission of IP packets. IPSec is a protocol commonly used in Virtual Private Networks (VPNs).

The Internet Key Exchange (IKE) protocol is used to negotiate keying material for IPSec Security Associations (SAs) and provides authentication of peers.

When IKE is used for establishing VPN connections, receiving certain malformed packets can cause Cisco devices to reset.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of the vulnerabilities may result in the restart of the device. The device will return to normal operation without any intervention required.

Suggested Fix
For customers that use IPSec, but do not require IKE for connection establishment, IPSec connection information may be entered manually, and IKE can be disabled, eliminating the exposure.

It is possible to mitigate the effects of this vulnerability by restricting the devices that can send IKE traffic to your IPSec devices. Due to the potential for IKE traffic to come from a spoofed source address, a combination of Access Control Lists (ACLs) and anti-spoofing mechanisms will be most effective.

The Unicast Reverse Path Forwarding (Unicast RPF) feature helps to mitigate problems that are caused by spoofed IP source addresses.
Vulnerability in IOS Firewall Feature Set -9360 [IOS]

Description
The IOS Firewall Feature set, also known as Cisco Secure Integrated Software, also known as Context Based Access Control (CBAC), and introduced in IOS version 11.2P, has a vulnerability that permits traffic normally expected to be denied by the dynamic access control lists. See "A Vulnerability in IOS Firewall Feature Set." at Cisco Security Advisories website

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 9360: Verify IOS Firewall Feature Set Vulnerability [IOS]

Description
The IOS Firewall Feature set, also known as Cisco Secure Integrated Software, also known as Context Based Access Control (CBAC), and introduced in IOS version 11.2P, has a vulnerability that permits traffic normally expected to be denied by the dynamic access control lists.

Applicable Platforms
Cisco IOS Devices.

Impact
The device will permit traffic normally expected to be denied by the dynamic access control lists.

Suggested Fix
There is no workaround
WeBVPN and SSLVPN Vulnerabilities -107397 [IOS]

Description
Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

1. Crafted HTTPS packet will crash device.
2. SSLVPN sessions cause a memory leak in the device.

Cisco has released free software updates that address these vulnerabilities.

There are no workarounds that mitigate these vulnerabilities.

Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 107397: Verify WeBVPN and SSLVPN Vulnerabilities [IOS]

Description
The Cisco SSLVPN feature provides remote access to enterprise sites by users from anywhere on the Internet. The SSLVPN provides users with secure access to specific enterprise applications, such as e-mail and web browsing, without requiring them to have VPN client software installed on their end-user devices.

The WebVPN Enhancements feature (Cisco IOS SSLVPN), released in Cisco IOS Release 12.4(6)T, obsoletes the commands and configurations originally put forward in Cisco IOS WebVPN.

Further information about Cisco IOS WebVPN is available in the "Cisco IOS Software Release 12.3T WebVPN feature guide” at the following link:

Further information about Cisco IOS SSLVPN is available in the "Cisco IOS Software Release 12.4T SSLVPN feature guide” at the following link:

Details regarding these two vulnerabilities in Cisco IOS devices that are running affected versions of system software are:

Crafted HTTPS packet will crash device
A device configured for SSLVPN may reload or hang when it receives a specially crafted HTTPS packet. Completion of the 3-way handshake to the associated TCP port number of the SSLVPN feature is required in order for the vulnerability to be successfully exploited, however authentication is "not" required. The default TCP port number for SSLVPN is 443.

SSLVPN sessions cause a memory leak in the device
A device configured for SSLVPN may leak transmission control blocks (TCBs) when processing an abnormally disconnected SSL session. Continued exploitation may result in the device depleting its memory resources and result in a crash of the device. Authentication is "not" required to exploit this vulnerability.

The memory leak can be detected by running the command "show tcp brief", like in the following example:

```
Router#show tcp brief
TCB    Local Address    Foreign Address (state)
468BBDC0 192.168.0.22.443   192.168.0.33.19794   CLOSEWAIT
482D4730 192.168.0.22.443   192.168.0.33.22092   CLOSEWAIT
482779A4 192.168.0.22.443   192.168.0.33.16978   CLOSEWAIT
4693DEBC 192.168.0.22.443   192.168.0.33.21580   CLOSEWAIT
482D3418 192.168.0.22.443   192.168.0.33.17244   CLOSEWAIT
4828ACC 192.168.0.22.443   192.168.0.33.16564   CLOSEWAIT
46954EB0 192.168.0.22.443   192.168.0.33.19532   CLOSEWAIT
4689BA98 192.168.0.22.443   192.168.0.33.15781   CLOSEWAIT
482908C4 192.168.0.22.443   192.168.0.33.19275   CLOSEWAIT
4829D66C 192.168.0.22.443   192.168.0.33.19314   CLOSEWAIT
4682D94 192.168.0.22.443   192.168.0.33.14736   CLOSEWAIT
4686F590 192.168.0.22.443   192.168.0.33.18786   CLOSEWAIT
4693CBA4 192.168.0.22.443   192.168.0.33.12176   CLOSEWAIT
4829ABC4 192.168.0.22.443   192.168.0.33.39629   CLOSEWAIT
4691206C 192.168.0.22.443   192.168.0.33.17818   CLOSEWAIT
4828224 192.168.0.22.443   192.168.0.33.16774   CLOSEWAIT
4832BFAC 192.168.0.22.443   192.168.0.33.39883   CLOSEWAIT
482D10CC 192.168.0.22.443   192.168.0.33.13936   CLOSEWAIT
4829B120 192.168.0.22.443   192.168.0.33.20870   CLOSEWAIT
482862FC 192.168.0.22.443   192.168.0.33.17035   CLOSEWAIT
482EC13C 192.168.0.22.443   192.168.0.33.16053   CLOSEWAIT
482901D8 192.168.0.22.443   192.168.0.33.16200   CLOSEWAIT
```

In the output above, those Transmission Control Blocks (TCBs) in the state CLOSEWAIT will not go away and represent memory leaks. Please note that only TCP connections with a local TCP port of 443 (the well-known port for HTTPS) are relevant.

**Applicable Platforms**

Cisco IOS Devices.

**Impact**

Successful exploitation of any of the two vulnerabilities may result in the device crashing, not accepting any new SSLVPN sessions or a memory leak. Repeated exploitation may result in an extended denial of service (DoS) condition.
Suggested Fix
There are no workarounds for the vulnerabilities described in this advisory.

Zone-Based Policy Firewall Vulnerability -110410 [IOS]

Description
Cisco IOS devices that are configured with Cisco IOS Zone-Based Policy Firewall Session Initiation Protocol (SIP) inspection are vulnerable to denial of service (DoS) attacks when processing a specific SIP transit packet. Exploitation of the vulnerability could result in a reload of the affected device.
Cisco has released free software updates that address this vulnerability.
Workarounds that mitigate this vulnerability are available.

. Applicable Platforms
Cisco IOS Devices

References
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 110410: Verify Zone-Based Policy Firewall Vulnerability [IOS]
Description

Firewalls are networking devices that control access to the network assets of an organization. Firewalls are often positioned at the entrance points into networks. Cisco IOS software provides a set of security features that enable you to configure a simple or elaborate firewall policy, according to your particular requirements.

SIP inspection in the Cisco IOS Firewall provides basic SIP inspect functionality (SIP packet inspection and pinhole opening) as well as protocol conformance and application security.

Cisco IOS Software that is configured with Cisco IOS Zone-Based Policy Firewall SIP inspection are vulnerable to a DoS attack when processing a specific SIP transit packet. Exploitation of this vulnerability will result in a reload of the affected device.

Cisco IOS Zone-Based Policy Firewall SIP inspection was first introduced in Cisco IOS Software versions 12.4(15)XZ and 12.4(20)T.

Cisco IOS Firewall CBAC support for SIP inspection by way of the ip inspect name [inspection_name] sip is not vulnerable. Additional information regarding Cisco IOS Firewall CBAC support for SIP inspection is available in the document "Firewall Support for SIP" at the following link: http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_fwall_sip_supp.html:

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of the vulnerability may result in a reload of the affected device. Repeated exploit attempts may result in a sustained DoS attack.

Suggested Fix
The only workaround for this vulnerability is to disable Cisco IOS zone-based policy firewall SIP inspection in the affected device's configuration. Disabling SIP inspection will allow the rest of the firewall features to continue to function until a software upgrade can be implemented. All other firewall features will continue to perform normally. Disabling SIP Inspection will vary depending on the implementation of the SIP inspection firewall.

**cTCP Denial of Service Vulnerability -109314 [IOS]**

Description
A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

Applicable Platforms
Cisco IOS Devices
References

Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

Rule 1

Rule
PSIRT - 109314: Verify IOS cTCP Denial of Service Vulnerability [IOS]

Description
The Cisco Tunneling Control Protocol (cTCP) feature is used by Easy VPN remote device operating in an environment in which standard IPSec does not function transparently without modification to existing firewall rules. The cTCP traffic is actually TCP traffic. Cisco IOS cTCP packets are Internet Key Exchange (IKE) or Encapsulating Security Payload (ESP) packets that are being transmitted over TCP.

A vulnerability exists where a series of TCP packets may cause a Cisco IOS device that is configured as an Easy VPN server with the cTCP encapsulation feature to run out of memory.

Applicable Platforms
Cisco IOS Devices.

Impact
Successful exploitation of this vulnerability may cause the affected device to run out of memory. Repeated exploitation will result in a denial of service (DoS) condition.

Suggested Fix
No workarounds are available.

As an alternative, the IPSec NAT traversal (NAT-T) feature can be used. The IPSec NAT-T feature introduces support for IP Security (IPSec) traffic to travel through Network Address Translation (NAT) or Port Address Translation (PAT) points in the network by addressing many known incompatibilities between NAT and IPSec.

Note: The NAT-T feature was introduced in Cisco IOS version 12.2(13)T.

NAT Traversal is a feature that is auto detected by VPN devices. There are no configuration steps for a router running Cisco IOS Release 12.2(13)T and later. If both VPN devices are NAT-T capable, NAT Traversal is auto-detected and auto-negotiated.

Note: When you enable NAT-T, the Cisco IOS device automatically opens UDP port 4500 on all IPSec enabled interfaces.

Caution: Be aware that you may need to enable IPSec over UDP on Cisco VPN software clients to support NAT-T. Additionally, you may need to change firewall rules to allow UDP port 500 for Internet Key Exchange (IKE) and UDP port 4500 for NAT-T.

For more information about NAT-T, refer to the white paper at:

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document.
uBR10012 Series Devices SNMP Vulnerability -107696 [IOS]

**Description**
Cisco uBR10012 series devices automatically enable Simple Network Management Protocol (SNMP) read/write access to the device if configured for linecard redundancy. This can be exploited by an attacker to gain complete control of the device. Only Cisco uBR10012 series devices that are configured for linecard redundancy are affected.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

**Applicable Platforms**
Cisco IOS Devices

**References**
Security Advisories For security issues that directly impact Cisco products and action is necessary to repair the Cisco product. Security Notices For issues that require a response to information posted to a public forum, or recommendations to mitigate general problems affecting network stability.

**Rule 1**

**Rule**
PSIRT - 109314: Verify Cisco uBR10012 Series Devices SNMP Vulnerability [IOS]

**Description**
Cisco uBR10012 series devices need to communicate with an RF Switch when configured for linecard redundancy. This communication is based on SNMP (Simple Network Management Protocol). When linecard redundancy is enabled on a Cisco uBR10012 series device, SNMP is also automatically enabled with a default community string of private that has read/write privileges. Since there are no access restrictions on this community string, it may be exploited by an attacker to gain complete control of the device.

Changing the default community string, adding access restrictions on SNMP or doing both will mitigate this vulnerability. The recommended mitigation is to do both.

**Applicable Platforms**
Cisco IOS Devices.

**Impact**
Successful exploitation of the vulnerability may allow an attacker to gain complete control of the device.

**Suggested Fix**

**Changing SNMP community string and restricting access**
By default, Cisco uBR10012 series devices that are configured for linecard redundancy use a community string of *private*. This community string can be changed in Cisco IOS versions 12.3(13)BC and later. It is recommended to change the community string and apply access control restrictions that only permit authorized devices SNMP access to the device.

The following configuration example provides operators with information on changing the community string and adding SNMP access control restrictions using an access control list (ACL).

access-list 90 permit host <RF-Switch-IP-1>
access-list 90 permit host <RF-Switch-IP-2>
access-list 90 permit host <up-converter-IP-if-exists>
access-list 90 deny any
redundancy
  linecard-group 1 cable
    rf-switch snmp-community <RF-Switch-SNMP-community>
snmp-server community <RF-Switch-SNMP-community> rw 90
When the SNMP community is changed on a Cisco uBR10012 device, it must also be changed on the RF Switch. It can be changed by the following command:
set SNMP COMMUNITY <RF-Switch-SNMP-community>
If there is an up-converter in the network, the SNMP community used by the up-converter must also be changed after changing the community string on the Cisco uBR10012 device. Information on changing the community string used by the up-converter can be found at the following link:
If the Cisco IOS version does not support changing the community string, access control restrictions can be applied to the default community string. The following configuration example provides operators with information on applying access control restrictions to the default community string.
access-list 90 permit host <RF-Switch-IP-1>
access-list 90 permit host <RF-Switch-IP-2>
access-list 90 permit host <up-converter-IP-if-exists>
access-list 90 deny any
snmp-server community private rw 90

**Land Attack**

**Description**
This policy checks to make sure that the network can not be used by a malicious attacker to install Distributed Denial Of Service (DDOS) scripts on any of the machines inside the network. DDOS attacks use a number of compromised sites to flood a target site with sufficient traffic or service requests to render it useless to legitimate users.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**References**
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.3.3 Page 90 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
Rule 1

Rule
Check for Land attack vulnerability [IOS, PIX, ASA]

Description
This check will make sure that given interfaces are protected against a possible Land attack. It will check that the interfaces have access lists installed to prevent IP traffic that has both source and destination address same AND is one of the router's IP addresses. This makes sure that ALL given interfaces have ACLs installed that would block incoming traffic with source IP and destination IP fields same AND is one of the router's active IP addresses. The Land Attack involves sending a packet to the router with the same IP address in the source and destination address fields and with the same port number in the source port and destination port fields. This attack may cause denial of service or degrade the performance of the router.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
This device may be vulnerable for Land attack.

Suggested Fix
Add the following ACL entries to the interface access list, one entry for each of the router's IP address and apply it to all the required interfaces using the commands:

\[
\text{deny ip host <router interface's IP address > host <router interface's IP address >}
\]

Risky Traffic

Description
Risky traffic (protocols and services) that needs to be blocked at the routers. It is not always possible to follow the strict security guidelines. In that case, fall back to prohibiting services that are commonly not needed, or are known to be popular vehicles for security compromise. These policies check for common services to restrict because they can be used to gather information about the protected network or they have weaknesses that can be exploited against the protected network. Some these services should be completely blocked by a typical border router. Unless there is a specific operational need to support, these services and protocols should not be allowed across the router in either direction.


Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

References
National Security Agency (NSA) Cisco Router Configuration Guide (Section 3.2.2 page 38 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Payment Card Industry Data Security Standard (PCI) (1.2 of Version 1.1, September, 2006)
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

Rule 1

Rule
List of interfaces to check the rules [IOS, PIX, ASA].

Description
This check makes sure configuration on given ports is not allowing any risky traffic.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
None

Suggested Fix
None

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Interfaces To Check | Group of interfaces to make sure unused port configuration is enforced. Example valid Values: 'Any', 'AnyEthernet', 'FastEthernet', 'GigabitEthernet', 'FastEthernet0/1', 'FastEthernet0/2', and so on. | Required: true
Required: true
Default: [Firewall External] |
Note
Using the Interfaces To Check Editor option, you can add, or remove the interface details. You can also change the order of the interface details.

Rule 2

Rule
Check if TCPMUX traffic is allowed [IOS, PIX, ASA].

Description
Make sure TCPMUX traffic (Port 1 in TCP and UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
TCPMUX (Port 1 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

```
deny tcp any eq 1 any
deny udp any eq 1 any
```

Rule 3

Rule
Check if ECHO traffic is allowed [IOS, PIX, ASA].

Description
Make sure ECHO traffic (Port 7 in TCP and UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
ECHO (Port 7 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

```
deny tcp any eq 7 any
deny udp any eq 7 any
```
Rule 4

Rule
Check if DISCARD traffic is allowed [IOS, PIX, ASA].

Description
Make sure DISCARD traffic (Port 9 in TCP and UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
DISCARD (Port 9 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

```
deny tcp any eq 9 any
deny udp any eq 9 any
```

Rule 5

Rule
Check if SYSTAT traffic is allowed [IOS, PIX, ASA].

Description
Make sure SYSTAT traffic (Port 11 in TCP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
SYSTAT (Port 11 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

```
deny tcp any eq 11 any
```

Rule 6

Rule
Check if DAYTIME traffic is allowed [IOS, PIX, ASA].

Description
Make sure DAYTIME traffic (Port 13 in TCP and UDP) is blocked if it is not required.
Understanding Compliance and Audit Manager (CAAM) Policies

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
DAYTIME (Port 13 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[
\text{deny tcp any eq 13 any} \\
\text{deny udp any eq 13 any}
\]

Rule 7

Rule
Check if NETSTAT traffic is allowed [IOS, PIX, ASA].

Description
Make sure NETSTAT traffic (Port 15 in TCP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
NETSTAT (Port 15 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[
\text{deny tcp any eq 15 any}
\]

Rule 8

Rule
Check if CHARGEN traffic is allowed [IOS, PIX, ASA].

Description
Make sure CHARGEN traffic (Port 19 in TCP and UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
CHARGEN (Port 19 in TCP and UDP) traffic can enter the router through given interface.
Suggested Fix
Add the following ACL entries to the interface access list.

\[
\text{deny tcp any eq 19 any} \\
\text{deny udp any eq 19 any}
\]

Rule 9

Rule
Check if TIME traffic is allowed [IOS, PIX, ASA].

Description
Make sure TIME traffic (Port 37 in TCP and UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
TIME (Port 37 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[
\text{deny tcp any eq 37 any} \\
\text{deny udp any eq 37 any}
\]

Rule 10

Rule
Check if WHOIS traffic is allowed [IOS, PIX, ASA].

Description
Make sure WHOIS traffic (Port 43 in TCP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
WHOIS (Port 43 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[
\text{deny tcp any eq 43 any}
\]
Rule 11

Rule
Check if BOOTP traffic is allowed [IOS, PIX, ASA].

Description
Make sure BOOTP traffic (Port 67 in UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
BOOTP (Port 67 in UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[\text{deny udp any eq 67 any}\]

Rule 12

Rule
Check if TFTP traffic is allowed [IOS, PIX, ASA].

Description
Make sure TFTP traffic (Port 69 in UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
TFTP (Port 69 in UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[\text{deny udp any eq 69 any}\]

Rule 13

Rule
Check if SUPDUP traffic is allowed [IOS, PIX, ASA].

Description
Make sure SUPDUP traffic (Port 95 in TCP and UDP) is blocked if it is not required.
Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
SUPDUP (Port 95 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.
\[
\text{deny tcp any eq 95 any} \\
\text{deny udp any eq 95 any}
\]

Rule 14

Rule
Check if SUNRPC traffic is allowed [IOS, PIX, ASA].

Description
Make sure SUNRPC traffic (Port 111 in TCP and UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
SUNRPC (Port 111 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.
\[
\text{deny tcp any eq 111 any} \\
\text{deny udp any eq 111 any}
\]

Rule 15

Rule
Check if LOCSRV traffic is allowed [IOS, PIX, ASA].

Description
Make sure LOCSRV traffic (Port 135 in TCP and UDP) is blocked if it is not required.
Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
LOCSRV (Port 135 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.
\[\text{deny} \ tcp \ any \ eq \ 135 \ any\]
\[\text{deny} \ udp \ any \ eq \ 135 \ any\]

Rule 16

Rule
Check if NETBIOS_NS traffic is allowed [IOS, PIX, ASA].

Description
Make sure NETBIOS_NS traffic (Port 137 in TCP and UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
NETBIOS_NS (Port 137 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.
\[\text{deny} \ tcp \ any \ eq \ 137 \ any\]
\[\text{deny} \ udp \ any \ eq \ 137 \ any\]

Rule 17

Rule
Check if NETBIOS_DGM traffic is allowed [IOS, PIX, ASA].

Description
Make sure NETBIOS_DGM traffic (Port 138 in TCP and UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
NETBIOS_DGM (Port 138 in TCP and UDP) traffic can enter the router through given interface.
**Suggested Fix**
Add the following ACL entries to the interface access list.

```plaintext
deny tcp any eq 138 any
deny udp any eq 138 any
```

**Rule 18**

**Rule**
Check if NETBIOS_SSN traffic is allowed [IOS, PIX, ASA].

**Description**
Make sure NETBIOS_SSN traffic (Port 139 in TCP and UDP) is blocked if it is not required.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
NETBIOS_SSN (Port 139 in TCP and UDP) traffic can enter the router through given interface.

**Suggested Fix**
Add the following ACL entries to the interface access list.

```plaintext
deny tcp any eq 139 any
deny udp any eq 139 any
```

**Rule 19**

**Rule**
Check if XDMCP traffic is allowed [IOS, PIX, ASA].

**Description**
Make sure XDMCP traffic (Port 177 in UDP) is blocked if it is not required.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
XDMCP (Port 177 in UDP) traffic can enter the router through given interface.

**Suggested Fix**
Add the following ACL entries to the interface access list.

```plaintext
deny udp any eq 177 any
```
Rule 20

Rule
Check if NETBIOS_DS traffic is allowed [IOS, PIX, ASA].

Description
Make sure NETBIOS_DS traffic (Port 445 in TCP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
NETBIOS_DS (Port 445 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.
\[deny tcp any eq 445 any\]

Rule 21

Rule
Check if REXEC traffic is allowed [IOS, PIX, ASA].

Description
Make sure REXEC (Remote Exec) traffic (Port 512 in TCP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
REXEC (Remote Exec) (Port 512 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.
\[deny tcp any eq 512 any\]

Rule 22

Rule
Check if LPR traffic is allowed [IOS, PIX, ASA].

Description
Make sure LPR traffic (Port 515 in TCP) is blocked if it is not required.
Applied Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
LPR (Port 515 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[\text{deny tcp any eq 515 any}\]

Rule 23

Rule
Check if TALK traffic is allowed [IOS, PIX, ASA].

Description
Make sure TALK traffic (Port 517 in UDP) is blocked if it is not required.

Applied Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
TALK (Port 517 in UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[\text{deny udp any eq 517 any}\]

Rule 24

Rule
Check if NTALK traffic is allowed [IOS, PIX, ASA].

Description
Make sure NTALK traffic (Port 518 in UDP) is blocked if it is not required.

Applied Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
NTALK (Port 518 in UDP) traffic can enter the router through given interface.
Understanding Compliance and Audit Manager (CAAM) Policies

Chapter 4 Using Compliance and Audit Manager Feature

Rule 25

Suggested Fix
Add the following ACL entries to the interface access list.

\texttt{deny udp any eq 518 any}

Rule
Check if UUCP traffic is allowed [IOS, PIX, ASA].

Description
Make sure UUCP traffic (Port 540 in TCP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
UUCP (Port 540 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\texttt{deny tcp any eq 540 any}

Rule 26

Rule
Check if Microsoft SQL Server traffic is allowed [IOS, PIX, ASA].

Description
Make sure Microsoft SQL SERVER traffic (Port 1434 in UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
Microsoft SQL SERVER (Port 1434 in UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\texttt{deny udp any eq 1434 any}

Rule 27

Rule
Check if Microsoft UPnP SSDP traffic is allowed [IOS, PIX, ASA].
**Description**
Make sure Microsoft UPnP SSDP traffic (Port 1900, 5000 in TCP and UDP) is blocked if it is not required.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
Microsoft UPnP SSDP (Port 1900, 5000 in TCP and UDP) traffic can enter the router through given interface.

**Suggested Fix**
Add the following ACL entries to the interface access list.

```
deny tcp any eq 1900 any
deny tcp any eq 5000 any
deny udp any eq 1900 any
deny udp any eq 5000 any
```

**Rule 28**

**Rule**
Check if NFS traffic is allowed [IOS, PIX, ASA].

**Description**
Make sure NFS traffic (Port 2049 in UDP) is blocked if it is not required.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
NFS (Port 2049 in UDP) traffic can enter the router through given interface.

**Suggested Fix**
Add the following ACL entries to the interface access list.

```
deny udp any eq 2049 any
```

**Rule 29**

**Rule**
Check if X WINDOW System traffic is allowed [IOS, PIX, ASA].

**Description**
Make sure X WINDOW System traffic (Port 6000-6063 in TCP) is blocked if it is not required.
Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
X WINDOW System (Port 6000-6063 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.
\[
\text{deny tcp any range 6000 6063 any}
\]

Rule 30

Rule
Check if IRC traffic is allowed [IOS, PIX, ASA].

Description
Make sure IRC traffic (Port 6667 in TCP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices Cisco PIX Devices Running >= 7.x and ASA devices

Impact
IRC (Port 6667 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.
\[
\text{deny tcp any eq 6667 any}
\]

Rule 31

Rule
Check if NetBus traffic is allowed [IOS, PIX, ASA].

Description
Make sure NetBus traffic (Port 12345-12346 in TCP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
NetBus (Port 12345-12346 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.
\[
\text{deny tcp any range 12345 12346 any}
\]
Rule 32

Rule
Check if BackOrifice traffic is allowed [IOS, PIX, ASA].

Description
Make sure Back Orifice traffic (Port 31337 in TCP and UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
Back Orifice (Port 31337 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[
\text{deny tcp any eq 31337 any} \\
\text{deny udp any eq 31337 any}
\]

Rule 33

Rule
Check if FINGER traffic is allowed [IOS, PIX, ASA].

Description
Make sure FINGER traffic (Port 79 in TCP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
FINGER (Port 79 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[
\text{deny tcp any eq 79 any}
\]

Rule 34

Rule
Check if SNMP traffic is allowed [IOS, PIX, ASA].

Description
Make sure SNMP traffic (Port 161 in TCP and UDP) is blocked if it is not required.
Understanding Compliance and Audit Manager (CAAM) Policies

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
SNMP (Port 161 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[
\text{deny udp any eq 161 any} \\
\text{deny tcp any eq 161 any}
\]

Rule 35

Rule
Check if SNMP_TRAP traffic is allowed [IOS, PIX, ASA].

Description
Make sure SNMP TRAP traffic (Port 162 in TCP and UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
SNMP TRAP (Port 162 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[
\text{deny udp any eq 162 any} \\
\text{deny tcp any eq 162 any}
\]

Rule 36

Rule
Check if RLOGIN traffic is allowed [IOS, PIX, ASA].

Description
Make sure RLOGIN traffic (Port 513 in TCP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
RLOGIN (Port 513 in TCP) traffic can enter the router through given interface.
Suggested Fix
Add the following ACL entries to the interface access list.

\[ \text{deny tcp any eq 513 any} \]

Rule 37

Rule
Check if WHO traffic is allowed [IOS, PIX, ASA].

Description
Make sure WHO traffic (Port 513 in UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
WHO (Port 513 in UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[ \text{deny udp any eq 513 any} \]

Rule 38

Rule
Check if RSH_RCP traffic is allowed [IOS, PIX, ASA].

Description
Make sure RSH, RCP, RDIST and RDUMP traffic (Port 514 in TCP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
RSH, RCP, RDIST and RDUMP (Port 514 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[ \text{deny tcp any eq 514 any} \]

Rule 39

Rule
Check if SYSLOG traffic is allowed [IOS, PIX, ASA].
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Description
Make sure SYSLOG traffic (Port 514 in UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
SYSLOG (Port 514 in UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

deny udp any eq 514 any

Rule 40

Rule
Check if NEW_WHO traffic is allowed [IOS, PIX, ASA].

Description
Make sure NEW WHO traffic (Port 550 in TCP and UDP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

Impact
NEW WHO (Port 550 in TCP and UDP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

deny udp any eq 550 any
deny tcp any eq 550 any

Rule 41

Rule
Check if T0rn rootkit traffic is allowed [IOS, PIX, ASA].

Description
Make sure T0rn rootkit traffic (Port 47017 in TCP) is blocked if it is not required.

Applicable Platforms
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices
Impact
Turn rootkit traffic (Port 47017 in TCP) traffic can enter the router through given interface.

Suggested Fix
Add the following ACL entries to the interface access list.

\[deny tcp any eq 47017 an\]

Loopback Interfaces

Description
Policies to enforce different protocols to use loopback interface as their source interface.

Applicable Platforms
Cisco IOS Devices
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability
Cisco IOS Devices With NetFlow Capability

References
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.1.4 Page 58, Section 4.1.6 Page 66, Section 4.1.8, Page 68, Section 4.5.2 Page 145, Section 4.6.4 Page 193 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
Cisco SAFE Compliance(1.1b)
SAFE: A Security Blueprint for Enterprise Networks
Center for Internet Security, Benchmark for Cisco IOS.(Section 2.2.1, Page: 39 of Version 2.2, Nov 2007)
CIS benchmark Cisco IOS, recommends the prudent level of minimum due care for operating system security. CIS benchmark IOS, contains some security configuration recommendations that affect functionality, and are therefore of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the functions and applications running in their particular environments. All IOS devices should implement these settings.

Rule 1

Rule
At least one loopback interface should be configured [IOS]

Description
Check that at least one loopback interface is configured
Understanding Compliance and Audit Manager (CAAM) Policies

Applicable Platforms
Cisco IOS Devices
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability
Cisco IOS Devices With NetFlow Capability

Impact
It is considered best practice, in configuring Cisco routers, to define one loopback interface, and designate it as the source interface for most traffic generated by the router itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. When a router is configured to use the loopback interface for services, it is possible to configure the security of other devices in the network more tightly. (When a service is configured to use the loopback interface as its source, we say that the service is bound to that interface. It means that IP packets generated by the router will have the loopback interface's address as their source address. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of your network from potential attackers is usually good practice.

Suggested Fix
Create a loopback interface and assign it an IP address. For a border router, the loopback's address should be in the range of the internal or DMZ network, not the external network. Note that the loopback address cannot be the same as the address of any other interface, nor can it be part of the same network as any other interface. Configure loopback interface using the command:

```
interface <loopback interface name> loopback
```

Rule 2

Rule
Check FTP uses Loopback interface [IOS]

Description
If FTP service is configured on the device, check that it uses loopback interface as its source interface

Applicable Platforms
Cisco IOS Devices
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability
Cisco IOS Devices With NetFlow Capability

Impact
It is considered best practice, in configuring Cisco routers, to define one loopback interface, and designate it as the source interface for most traffic generated by the router itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. When a router is configured to use the loopback interface for services, it is possible to configure the security of other devices in the network more tightly. (When a service is configured to use the loopback interface as its source, we say that the service is bound to that interface. It means that IP packets generated by the router will have the loopback interface's address as their source address. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of your network from potential attackers is usually good practice.
Suggested Fix
Configure a loopback interface name as the source interface for FTP service using the command:

\textit{ip ftp source-interface loopback}

\section*{Rule 3}
\textbf{Rule}
Check Remote Command uses Loopback interface [IOS]

\textbf{Description}
Check if Remote Commands use loopback interface as their source interface. If RCP or RSH is not enabled, no check will be done.

\textbf{Applicable Platforms}
Cisco IOS Devices
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability
Cisco IOS Devices With NetFlow Capability

\textbf{Impact}
It is considered best practice, in configuring Cisco routers, to define one loopback interface, and designate it as the source interface for most traffic generated by the router itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. When a router is configured to use the loopback interface for services, it is possible to configure the security of other devices in the network more tightly. (When a service is configured to use the loopback interface as its source, we say that the service is bound to that interface. It means that IP packets generated by the router will have the loopback interface's address as their source address. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of your network from potential attackers is usually good practice.

\textbf{Suggested Fix}
Configure a loopback interface name as the source interface for Remote Command service using the command:

\textit{ip rcmd source-interface loopback}

\section*{Rule 4}
\textbf{Rule}
Check Syslog uses Loopback interface [IOS]

\textbf{Description}
Check if syslog protocol use loopback interface as their source interface. No check will be done if Syslog logging is disabled on the device.
Applicable Platforms
Cisco IOS Devices
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability
Cisco IOS Devices With NetFlow Capability

Impact
It is considered best practice, in configuring Cisco routers, to define one loopback interface, and designate it as the source interface for most traffic generated by the router itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. When a router is configured to use the loopback interface for services, it is possible to configure the security of other devices in the network more tightly. (When a service is configured to use the loopback interface as its source, we say that the service is bound to that interface. It means that IP packets generated by the router will have the loopback interface's address as their source address. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of your network from potential attackers is usually good practice.

Suggested Fix
Configure a loopback interface name as the source interface for Syslog service using the command:

logging source-interface loopback

Rule 5

Rule
Check NTP uses Loopback interface [IOS]

Description
Check if NTP protocol use loopback interface as their source interface. No check is done if NTP is not configured on the device.

Applicable Platforms
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability

Impact
It is considered best practice, in configuring Cisco routers, to define one loopback interface, and designate it as the source interface for most traffic generated by the router itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. When a router is configured to use the loopback interface for services, it is possible to configure the security of other devices in the network more tightly. (When a service is configured to use the loopback interface as its source, we say that the service is bound to that interface. It means that IP packets generated by the router will have the loopback interface's address as their source address. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of your network from potential attackers is usually good practice.

Suggested Fix
Configure a loopback interface name as the source interface for NTP services using the command:

ntp source loopback
Rule 6

Rule
Check RADIUS uses Loopback interface [IOS]

Description
Check if RADIUS protocol use loopback interface as their source interface

Applicable Platforms
Cisco IOS Devices
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability
Cisco IOS Devices With NetFlow Capability

Impact
It is considered best practice, in configuring Cisco routers, to define one loopback interface, and designate it as the source interface for most traffic generated by the router itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. When a router is configured to use the loopback interface for services, it is possible to configure the security of other devices in the network more tightly. (When a service is configured to use the loopback interface as its source, we say that the service is bound to that interface. It means that IP packets generated by the router will have the loopback interface's address as their source address. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of your network from potential attackers is usually good practice.

Suggested Fix
Configure a loopback interface name as the source interface for RADIUS service using the command:

ip radius source-interface loopback

Rule 7

Rule
Check TACACS uses Loopback interface [IOS]

Description
Check if TACACS protocol use loopback interface as their source interface

Applicable Platforms
Cisco IOS Devices
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability
Cisco IOS Devices With NetFlow Capability
Impact
It is considered best practice, in configuring Cisco routers, to define one loopback interface, and designate it as the source interface for most traffic generated by the router itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. When a router is configured to use the loopback interface for services, it is possible to configure the security of other devices in the network more tightly. (When a service is configured to use the loopback interface as its source, we say that the service is bound to that interface. It means that IP packets generated by the router will have the loopback interface's address as their source address. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of your network from potential attackers is usually good practice.

Suggested Fix
Configure a loopback interface name as the source interface for TACACS service using the command:

```
ip tacacs source-interface loopback
```

Rule 8

Rule
Check SNMP Trap service uses Loopback interface [IOS]

Description
Check if SNMP Trap service uses loopback interface as its source interface. No check is done if SNMP Traps are not configured.

Applicable Platforms

Impact
It is considered best practice, in configuring Cisco routers, to define one loopback interface, and designate it as the source interface for most traffic generated by the router itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. When a router is configured to use the loopback interface for services, it is possible to configure the security of other devices in the network more tightly. (When a service is configured to use the loopback interface as its source, we say that the service is bound to that interface. It means that IP packets generated by the router will have the loopback interface's address as their source address. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of your network from potential attackers is usually good practice.

Suggested Fix
Configure a loopback interface name as the source interface for SNMP service using the command:

```
ssnmp-server trap-source loopback
```

Rule 9

Rule
Check Telnet service uses Loopback interface [IOS]
Chapter 4  Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

Description
Check if Telnet service uses loopback interface as its source interface

Applicable Platforms
Cisco IOS Devices
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability
Cisco IOS Devices With NetFlow Capability

Impact
It is considered best practice, in configuring Cisco routers, to define one loopback interface, and designate it as the source interface for most traffic generated by the router itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. When a router is configured to use the loopback interface for services, it is possible to configure the security of other devices in the network more tightly. (When a service is configured to use the loopback interface as its source, we say that the service is bound to that interface. It means that IP packets generated by the router will have the loopback interface's address as their source address. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of your network from potential attackers is usually good practice.

Suggested Fix
Configure a loopback interface name as the source interface for Telnet service using the command:

```
ip telnet source-interface loopback
```

Rule 10

Rule
Check TFTP service uses Loopback interface [IOS]

Description
Check if TFTP service uses loopback interface as its source interface

Applicable Platforms
Cisco IOS Devices
Cisco IOS Devices With NTP_CLIENT Capability
Cisco IOS Devices With NTP_SERVER Capability
Cisco IOS Devices With NetFlow Capability

Impact
It is considered best practice, in configuring Cisco routers, to define one loopback interface, and designate it as the source interface for most traffic generated by the router itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. When a router is configured to use the loopback interface for services, it is possible to configure the security of other devices in the network more tightly. (When a service is configured to use the loopback interface as its source, we say that the service is bound to that interface. It means that IP packets generated by the router will have the loopback interface's address as their source address. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of your network from potential attackers is usually good practice.
Suggested Fix
Configure a loopback interface name as the source interface for TFTP service using the command:

\textit{ip tftp source-interface loopback}

\section*{Rule 11}

\textbf{Rule}
Check if NetFlow service uses loopback interface

\textbf{Description}
Check if NetFlow service uses loopback interface as its source interface

\textbf{Applicable Platforms}
Cisco IOS Devices With NetFlow Capability

\textbf{Impact}
It is considered best practice, in configuring Cisco routers, to define one loopback interface, and designate it as the source interface for most traffic generated by the router itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. When a router is configured to use the loopback interface for services, it is possible to configure the security of other devices in the network more tightly. (When a service is configured to use the loopback interface as its source, we say that the service is bound to that interface. It means that IP packets generated by the router will have the loopback interface's address as their source address. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of your network from potential attackers is usually good practice.

\textbf{Suggested Fix}
Configure a loopback interface name as the source interface for NetFlow service using the command:

\textit{ip flow-export source loopback}

\section*{Distributed DoS Attacks}

\textbf{Description}
This policy checks to make sure that the network can not be used by a malicious attacker to install Distributed Denial Of Service (DDOS) scripts on any of the machines inside the network. DDOS attacks use a number of compromised sites to flood a target site with sufficient traffic or service requests to render it useless to legitimate users.

\textbf{Applicable Platforms}
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

\textbf{References}
National Security Agency (NSA) Cisco Router Configuration Guide(Section 4.3.3 Page 92 of Version 1.1c)
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Information Technology - Code of practice for information security management.

**Rule 1**

**Rule**

List of interfaces to check the rules [IOS, PIX, ASA]

**Description**

This check makes sure configuration on given ports is not allowing any DDoS traffic patterns.

**Applicable Platforms**

Cisco IOS Devices

Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**

none

**Suggested Fix**

none

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces to Check</td>
<td>Group of interfaces to make sure unused port configuration is enforced. Example valid Values: 'Any', 'AnyEthernet', 'FastEthernet', 'GigabitEthernet', 'FastEthernet0/1', 'FastEthernet0/.*' etc. Using Interfaces to Check Editor option, you can add, or remove Interface details. You can also change the order of the Interface details.</td>
<td>Required: true Default: [Firewall External]</td>
</tr>
</tbody>
</table>

**Rule 2**

**Rule**

Check for TRINOO DDoS attack vulnerability [IOS, PIX, ASA]

**Description**

This check will make sure that a malicious attacker can not install TRIN00 DDOS scripts on any of the machines inside the network. TRIN00 DDOS scripts that are installed on the devices will cause a DDOS attack to be generated from this network.

**Applicable Platforms**

Cisco IOS Devices

Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
Network is vulnerable to be installed with DDOS scripts, which can be used by an attacker to launch an attack originating from this network. This check will make sure the network does not allow any traffic with destination ports 27665(tcp), 31335(udp), 27444(udp) to enter and leave this network.

**Suggested Fix**
Add the following ACL entries to the interface access list.

- `deny tcp any any eq 27665`
- `deny udp any any eq 31335`
- `deny udp any any eq 27444`

**Rule 3**

**Rule**
Check for Stacheldraht DDoS attack vulnerability [IOS, PIX, ASA]

**Description**
This check will make sure that a malicious attacker can not install Stacheldraht DDOS scripts on any of the machines inside the network. Stacheldraht DDOS scripts that are installed on the devices will cause a DDoS attack to be generated from this network. This check will make sure the network does not allow any traffic with destination ports (16660(tcp), 65500(tcp)) to enter and leave this network.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
Network is vulnerable to be installed with DDOS scripts, which can be used by an attacker to launch an attack originating from this network.

**Suggested Fix**
Add the following ACL entries to the interface access list.

- `deny tcp any any eq 16660`
- `deny tcp any any eq 65000`

**Rule 4**

**Rule**
Check for TriniyV3 DDoS attack vulnerability [IOS, PIX, ASA]

**Description**
This check will make sure that a malicious attacker can not install TrinityV3 DDOS scripts on any of the machines inside the network. TrinityV3 DDOS scripts that are installed on the devices will cause a DDoS attack to be generated from this network. This check will make sure the network does not allow any traffic with destination ports (33260(tcp), 39168(tcp)) to enter and leave this network.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
Network is vulnerable to be installed with DDOS scripts, which can be used by an attacker to launch an attack originating from this network.

**Suggested Fix**
Add the following ACL entries to the interface access list.

```
deny tcp any any eq 33270
deny tcp any any eq 39168
```

**Rule 5**

**Rule**
Check for Subseven DDoS attack vulnerability [IOS, PIX, ASA]

**Description**
This check will make sure that a malicious attacker can not install Subseven DDOS scripts on any of the machines inside the network. Subseven DDOS scripts that are installed on the devices will cause a DDOS attack to be generated from this network. This check will make sure the network does not allow any traffic with destination ports (6711, 6712, 6776, 6669, 2222 and 7000) to enter and leave this network.

**Applicable Platforms**
Cisco IOS Devices
Cisco PIX Devices Running >= 7.x and ASA devices

**Impact**
Network is vulnerable to be installed with DDOS scripts, which can be used by an attacker to launch an attack originating from this network.

**Suggested Fix**
Add the following ACL entries to the interface access list.

```
deny tcp any any range 6711 6712
deny tcp any any eq 6776
deny tcp any any eq 6669
deny tcp any any eq 2222
deny tcp any any eq 7000
```

**Web Mode Status**

**Description**
HTTP Server allows web based remote administration of the device. It is useful primarily when intervening device prevent use of Telnet for that purpose. However, it is important to note that both Telnet and web-based remote administration reveal critical passwords in clear text. Further, web-based administration imposes the requirement that users log in at full (level 15) privilege. Therefore, web-based remote administration should be avoided.
References
Payment Card Industry Data Security Standard (PCI).

The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

National Security Agency (NSA) Cisco Router Configuration Guide Section 4.2.1 Page 71
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Rule

Rule
Web mode should be disabled.

Description
HTTP Server allows web based remote administration of the device. It is useful primarily when intervening device prevent use of Telnet for that purpose. However, it is important to note that both Telnet and web-based remote administration reveal critical passwords in clear text. Further, web-based administration imposes the requirement that users log in at full (level 15) privilege. Therefore, web-based remote administration should be avoided

Impact
Can be exploited to access the device

Suggested Fix
HTTP can be disable using config network webmode disable.

SNMP Status

Description
The Simple Network Management Protocol (SNMP) is the standard Internet protocol for automated remote monitoring and administration. There are several different versions of SNMP, with different security properties. If a network has a deployed SNMP infrastructure in place for administration, then all routers on that network should be configured to securely participate in it. In the absence of a deployed SNMP scheme, all SNMP facilities on all routers should be disabled. While SNMP is helpful because it allows an administrator to remotely configure the router, it also offers a potentially dangerous conduit into a network.
References
Payment Card Industry Data Security Standard (PCI).

The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

National Security Agency (NSA) Cisco Router Configuration Guide Section 4.2.1 Page 70
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Rule

Rule
SNMPV1 Should be disabled

Description
SNMP V1 Should be disabled

Impact
The Simple Network Management Protocol (SNMP) is the standard Internet protocol for automated remote monitoring and administration. There are several different versions of SNMP, with different security properties. If a network has a deployed SNMP infrastructure in place for administration, then all routers on that network should be configured to securely participate in it. In the absence of a deployed SNMP scheme, all SNMP facilities on all routers should be disabled. While SNMP is helpful because it allows an administrator to remotely configure the router, it also offers a potentially dangerous conduit into a network.

Suggested Fix
The safest way to ensure that SNMP is really unavailable to an attacker, and will remain so, is to list the established SNMP community strings and explicitly unset all of them. It is also recommended to disable [SNMP trap] and [system shutdown] features and finally disabling SNMP Server on the device using the command:

  config snmp version v1 Disable

Rule 2

Rule
SNMP V2 Status should be disabled

Description
SNMPv2 should be disabled
Impact
The Simple Network Management Protocol (SNMP) is the standard Internet protocol for automated remote monitoring and administration. There are several different versions of SNMP, with different security properties. If a network has a deployed SNMP infrastructure in place for administration, then all routers on that network should be configured to securely participate in it. In the absence of a deployed SNMP scheme, all SNMP facilities on all routers should be disabled. While SNMP is helpful because it allows an administrator to remotely configure the router, it also offers a potentially dangerous conduit into a network.

Suggested Fix
The safest way to ensure that SNMP is really unavailable to an attacker, and will remain so, is to list the established SNMP community strings and explicitly unset all of them. It is also recommended to disable [SNMP trap] and [system shutdown features] and finally disabling SNMP Server on the device using the command:

```
cfg snmp version v2c disable
```
Impact
While SNMP is helpful because it allows an administrator to remotely configure the router, it also offers a potentially dangerous conduit into a network. Care should be taken while configuring SNMP community strings with write access since an attacker can change the system state.

Suggested Fix
`config snmp community accessmode ro [community string name]`

Rule 5

Rule
Traps should be disabled

Description
SNMP Trap messages are generated by the device for configuration event notifications or security alerts.

Impact
SNMP traps carry information in clear text. This information can be easily captured to retrieve sensitive information.

Suggested Fix
`config snmp trapreceiver mode disable [snmp community name]`

WLAN Security Status

Description
Default ssid, ssid broadcast and pre shared keys should be disabled

References
Payment Card Industry Data Security Standard (PCI).
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

National Security Agency (NSA) Cisco Router Configuration Guide Section 2.1
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Rule 1

Rule
Check statis WEP key should be disabled
Understanding Compliance and Audit Manager (CAAM) Policies

Rule 1

Description
static wep keys should be Disabled

Impact
Enable wepkeys may vulnerable device

Suggested Fix
wepkey can disabled using command config wlan security static-wep-key disable [wlan id]

Rule 2

Rule
Check SSID broadcast on WLAN should be disabled

Description
Broadcast SSID should be Disabled

Impact
enable ssid broadcast may cause device vulnerable

Suggested Fix
ssid broadcast can be disabled using command:
config wlan broadcast-ssid disable [wlan id]

Rule 3

Rule
Default SSID Should not be configured

Description
Default ssid should not be configured

Impact
Device may vulnerable

Suggested Fix
SSID can be configured using config wlan create [wlan id] [profilename]

CDP Status

Description
Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches
References
National Security Agency (NSA) Cisco Router Configuration Guide Section 4.2.1 Page 70
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Rule 1

**Rule**

CDP Status

**Description**
The Cisco Discovery Protocol is a proprietary protocol that Cisco devices use to identify each other on a LAN segment. It is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

**Impact**
CDP is useful only in specialized situations, and is considered deleterious to security.

**Suggested Fix**
To turn off CDP entirely, use the global configuration command config cdp disable.

Syslog Status

**Description**
Logging level and state should be carefully chosen so that important information is logged but at the same time, the logging server is not flooded with too many log messages from the devices. Also, the device should be configured to send log messages to a designated host on the protected network

References
Payment Card Industry Data Security Standard (PCI).
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

National Security Agency (NSA) Cisco Router Configuration Guide Section 4.5.2 Page 139
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
Rule 1

Rule
Check Syslog host should configured

Description
Logging level and state should be carefully chosen so that important information is logged but at the same time, the logging server is not flooded with too many log messages from the devices. Also, the device should be configured to send log messages to a designated host on the protected network

Impact
If the logging level and host(s) are not configured according to the policy, it may make it harder to troubleshoot problems

Suggested Fix
Logging host can configure using command:
config logging syslog host [ip address]/config syslog [ip address]

Telnet Status

Description
Make sure that all the terminal lines are configured to block incoming connections using un-authorized protocols

References
Payment Card Industry Data Security Standard(PCI).
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

National Security Agency (NSA) Cisco Router Configuration Guide Section 4.1.5 Page 58
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Rule 1

Rule
Telnet should be disabled

Description
Make sure that all the terminal lines are configured to block incoming connections using un-authorized protocols
Chapter 4      Using Compliance and Audit Manager Feature

Understanding Compliance and Audit Manager (CAAM) Policies

**Rule 1**

**Rule**
Check NTP client should configured

**Rule 2**

**Rule**
line time out should not be more than 5 min

**Description**
Make sure that all the lines should configured less than 5 min timeout

**Impact**
An unauthorized user may connect to the device using any undesired protocols violating the set policy

**Suggested Fix**
Line time can configure using command config sessions timeout [in minutes]

**NTP Server should be Configured**

**Description**
The Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP is designed to make time synchronization automatic and efficient across all devices in the network. Having accurate time is important for security, especially for intrusion and forensic analysis.

**References**
Payment Card Industry Data Security Standard (PCI).
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

National Security Agency (NSA) Cisco Router Configuration Guide Section 4.5.2 Page 149
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.
Understanding Compliance and Audit Manager (CAAM) Policies

Description
All devices in the network should be configured to synchronize their times with an authoritative NTP Server. It is recommended that the border router be configured to synchronize time from at least two reliable NTP servers and all the devices in the protected network can be configured as clients to this border router

Impact
Unless all the devices are properly configured to synchronize the time, the event logs coming from different devices would have different time stamps. This makes it very hard to analyze the logs in terms of intrusion detection and forensics

Suggested Fix
Configure ntp client using the commands:
config time ntp server 1 1.5.2.6

Check IDS Status

Description
Cisco IDS introduces the ability to configure deny actions when policy violations (signatures) are detected. Based on user configuration at the IDS/IPS system, a shun request can be sent to a WLC in order to block the packets from a particular IP address.

References
Payment Card Industry Data Security Standard (PCI).

The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

National Security Agency (NSA) Cisco Router Configuration Guide Section 3.3
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Rule 1

Rule
IDS Should be configured on WLC

Description
Cisco IDS introduces the ability to configure deny actions when policy violations (signatures) are detected. Based on user configuration at the IDS/IPS system, a shun request can be sent to a WLC in order to block the packets from a particular IP address.

Impact
Device may be vulnerable
Suggested Fix
IDS can be configured using command:

```
config wps cids-sensor add [index] [server ip address] [username] [password]
```

Check Authentication Servers

Description
By using AAA along with security server, you can control access to Device and other network services from a centralized location. This allows for easier management of user accounts and privileges and provides additional capabilities for auditing of network service usage

References
Payment Card Industry Data Security Standard (PCI)
The Payment Card Industry (PCI) Data Security Standard resulted from a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. PCI Data Security requirements apply to all members, merchants and service providers that store, process or transmit cardholder data.

National Security Agency (NSA) Cisco Router Configuration Guide Section 4.6.2 Page 182
The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network components, and help protect the integrity and confidentiality of network traffic.

Rule 1

Rule
Check at least one TACACS server should configured

Description
By using AAA along with security server, you can control access to device and other network services from a centralized location. This allows for easier management of user accounts and privileges and provides additional capabilities for auditing of network service usage

Impact
No known impact

Suggested Fix
Configure required TACACS servers using the command:

```
config tacacs auth add [index] [IP addr] [port] [ascii/hex] [secret]
```

Rule 2

Rule
Local authentication should configured last
Data Synchronization between LMS and CAAM

CAAM database should always be in sync with LMS database. When a new device is added to LMS or an unmanaged device is managed, and if the CAAMSерver process is down, the device will not be added to CAAM database. When the CAAMSерver process comes up, the device will be added to CAAM database but the device details such as Inventory, Config, and Show Commands will not be updated in CAAM database. You have to manually perform Inventory, Config, and Show Commands collection to update the CAAM database.

To perform Inventory collection, select **Inventory > Job Browsers > Inventory Collection**

To perform Config collection, select **Configuration > Configuration Archive > Synchronization**

To perform Show Commands collection, select **Admin > Collection Settings > Compliance Data Collection**

Compliance Management License

From LMS 4.2.1, LMS-COMP Evaluation Management License will be renamed as “Compliance Management License” (PI CM), which is a 60-day evaluation license.
The following Compliance and Audit Reports require Compliance Management License from LMS 4.2.1:

- HIPAA Compliance Reports
- SOX (COBIT) Compliance Reports
- ISO/IEC 27002 Compliance Reports
- NSA Compliance Reports
- PCI DSS Compliance Reports
- DHS Checklist Reports
- DISA Checklists Report
- CIS Benchmarks
Netconfig is one of the Configuration Management applications that provides you with easy access to the configuration files of all supported devices. It allows you to change the configuration of network devices, provided the configurations are archived. Netconfig automatically updates the archive when it changes the configuration.

The advantages of using Netconfig instead of CLI configuration commands include but are not limited to:

- Scheduling jobs
- Using jobs to run multiple commands on multiple devices
- Using tasks to carry out easy and reliable configuration changes
- Mandating approval before running a job
- Rolling back configuration changes when a job fails

This chapter contains:

- NetConfig Tasks
- Preparing to Use NetConfig
- Rolling Back Configuration Changes
- Understanding NetConfig User Permissions
- Using NetConfig
- Starting a New NetConfig Job
- Browsing and Editing Jobs Using the NetConfig Job Browser
- Assigning Tasks to Users
- Using System-defined Tasks
- Creating and Editing User-defined Tasks
- Handling Interactive Commands
- Handling Multi-line Commands
- cwcli netconfig
NetConfig Tasks

As a NetConfig user, you can:

- Define and schedule NetConfig jobs
  Use the configuration tasks (system-defined or user-defined) to create the configuration commands that you want to apply to devices.

- Browse and edit NetConfig jobs
  Browse all NetConfig jobs on your system and edit, copy, stop, retry or delete them. For information about a particular job, click the hyperlink of the Job ID in the NetConfig Job Browser.

- Use the command line interface for NetConfig jobs
  Use the cwcli command line interface to create and schedule NetConfig jobs from the command line.

As a NetConfig administrator, you can:

- Create User-defined tasks
  Create your own user-defined tasks containing configuration or rollback commands, and download them to a set of selected devices. You can enter the configuration commands by typing them or by importing them from a file.
  User-defined tasks can be parameterized, that is, they can contain variables that take values from a specified file that resides on the LMS server.

- Assign tasks
  Provide selected network operators the rights to execute configuration tasks. You can assign more than one task to one or more users. By default, only network administrators can use configuration tasks.

- Specify the order of the protocol to deploy the configuration and fetch operations
  Specify the protocol order separately for configuration download and update operations of NetConfig jobs. This enables you to use preferred protocols for downloading and fetching configurations.
  For example, you can use Telnet to download configuration to the device, and TFTP to fetch the configuration, thus improving the overall performance of NetConfig.

- Set default NetConfig job policies
  Each NetConfig job has job properties (including enabling job password) that defines how the job will be executed. You can configure defaults for these properties that will be applied to all future jobs. For each property, you can specify if users can change the default when creating a job.

See Understanding NetConfig User Permissions.

Note
You can select the log level settings for the NetConfig application at Admin > System > Debug Settings > Log Level Settings.
Preparing to Use NetConfig

This section details the following pre-requisites for using NetConfig:

- Verifying Device Credentials
- Modifying Device Security
- Verifying Device Prompts
- Configuring Default Job Policies (Optional)
- Assigning Task Access Privileges to Users (Optional)
- Enabling Job Approval (Optional)

Verifying Device Credentials

NetConfig needs access to device credentials to make device configuration changes. The device credentials are available in the Device and Credential repository. Use Inventory > Device Administration > Add / Import / Manage Devices to verify if the devices that you want to configure are having the correct credentials.

Modifying Device Security

To configure devices, you must disable security that prohibits NetConfig job from running the commands on the devices. For the list of commands, see Administration of Cisco Prime LAN Management Solution 4.2.
Chapter 5  Making and Deploying Configuration Changes Using NetConfig

Preparing to Use NetConfig

Verifying Device Prompts

Table 5-1 describes the CLI prompt formats for NetConfig.

Table 5-1  NetConfig CLI Prompt Formats

<table>
<thead>
<tr>
<th>Transport Mechanism</th>
<th>Format</th>
</tr>
</thead>
</table>
| Telnet              | • For IOS-based devices, Content Engine devices, and Content Service Switch devices  
|                     | – The login prompt must end with a greater-than symbol (>).  
|                     | – The enable prompt must end with a pound sign (#).  
|                     | • For Catalyst devices  
|                     | – The login prompt must end with a greater-than symbol (>).  
|                     | – The enable prompt must end with the text (enable).  
| SSH                 | • For IOS-based devices, Content Engine devices, and Content Service Switch devices  
|                     | – The login prompt may end with (>), (#), (:), (%).  
|                     | – The enable prompt must end with a pound sign (#).  
|                     | • For Catalyst devices  
|                     | – The login prompt may end with (>), (#), (:), (%).  
|                     | – The enable prompt must end with the text (enable).  

Default prompts use these formats. If the defaults formats have been changed, ensure that the prompts meet these requirements.

Configuring Default Job Policies (Optional)

NetConfig jobs have properties that determine how they run. You can configure the default job policies (Admin > Network > Configuration Job Settings > Config Job Policies) that apply to all NetConfig jobs.

Assigning Task Access Privileges to Users (Optional)

You can assign task access privileges that determine the configuration tasks each user can use to create NetConfig jobs. See Understanding NetConfig User Permissions.

Enabling Job Approval (Optional)

Netconfig jobs require approval before they can run. See the section “Setting Up Job Approval” in Administration of Cisco Prime LAN Management Solution 4.2.
Rolling Back Configuration Changes

NetConfig lets you roll back (undo) the configuration changes made to network devices if a job does not get completed. Rollback commands (the configuration commands that are used to roll back the configuration changes) are created based on how the job was created.

You must configure a NetConfig job to automatically roll back configuration changes, if the job fails to complete.

NetConfig can roll back configurations only if the device configurations are archived in Configuration Archive. See Archiving Configurations andManaging them using Configuration Archive.

This section contains:
- Creating Rollback Commands
- Configuring a Job to Roll Back on Failure

Creating Rollback Commands

For system-defined tasks, the rollback commands are automatically created by the task. For user-defined tasks, you can enter the rollback commands while creating the task.

Configuring a Job to Roll Back on Failure

You can define a job failure policy so that it automatically rolls back configuration changes, if the job fails to run. You can select one of the three rollback options:
- Rollback device and stop—Rolls back the changes on the failed device and stops the job.
- Rollback device and continue—Rolls back the changes on the failed device and continues the job.
- Rollback job on failure—Rolls back the changes on all devices and stops the job.

Understanding NetConfig User Permissions

Access to NetConfig functionality is controlled by permissions. Users having only Help Desk permissions cannot access NetConfig. Other users can access NetConfig, but their access to functionality is controlled.

In the Permission Report (Reports > System > Users > Permission) check if you have the required privileges to perform the required NetConfig task.

This section details:
- Job Approval Permissions
- User-defined Tasks Permissions
- Administrator Task Permissions
- Job Editing Permissions
Job Approval Permissions

Users with Approver permissions can approve NetConfig jobs. Jobs must be approved before they are scheduled to run if Job Approval is enabled on the system. See the section “Setting Up Job Approval” in Administration of Cisco Prime LAN Management Solution 4.2.

User-defined Tasks Permissions

By default, only users with Network Administrator permissions can create user-defined configuration tasks. For more information, see Creating and Editing User-defined Tasks. A Network Administrator can give other users the required permissions on a task-by-task basis.

Administrator Task Permissions

Network Administrators can perform the tasks listed in the Admin menu. Administrator tasks are:

- Assigning tasks to users
- Configuring default job properties
- Creating and editing user-defined tasks

For user permissions, see Understanding NetConfig User Permissions.

Job Editing Permissions

After a NetConfig job is created, the owner, or a user with the owner privileges, or a network administrator can:

- Copy a job
- Edit a job
- Retry a job
- Delete a job
- Stop a job while it is running

Using NetConfig

NetConfig allows you to do the following tasks:

- Create and manage NetConfig jobs using the NetConfig job browser. See:
  - Starting a New NetConfig Job
  - Browsing and Editing Jobs Using the NetConfig Job Browser
- Create your own NetConfig tasks and run them on a selected set of devices. See Creating and Editing User-defined Tasks.
- Assign tasks to users. You can assign one or more tasks to one or more users. See Assigning Tasks to Users.
Starting a New NetConfig Job

You can create and schedule:

- Device-based jobs
- Module-based jobs
- Port-based jobs

This section tells you how to:

- Create a NetConfig Job based on Device
- Create a NetConfig Job based on Module or Port

To manage Netconfig jobs using NetConfig job browser, see Browsing and Editing Jobs Using the NetConfig Job Browser.

Ensure that you have set the:

- Transport protocol order for your job using Admin > Collection Settings > Config > Config Transport Settings. See Administration of Cisco Prime LAN Management Solution 4.2.
- Job and password policy for your job using Admin > Network > Configuration Job Settings before starting a new NetConfig job. See Administration of Cisco Prime LAN Management Solution 4.2.

Note: View the Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

Create a NetConfig Job based on Device

To create a new NetConfig job based on Device:

Step 1
Select either:

- Configuration > Tools > NetConfig > Deploy
- Configuration > Job Browsers > NetConfig

The NetConfig Job Browser appears.

Step 2
Click Create.

The Netconfig Job Type page appears, displaying the following job types:

- Device Based
- Module Based
- Port Based

Step 3
Select Device Based and click Go.
Chapter 5      Making and Deploying Configuration Changes Using NetConfig

Starting a New NetConfig Job

The Devices and Tasks dialog box appears, with these panes:

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Selector</td>
<td>Select devices on which the NetConfig job has to run. You can select multiple device categories. For cable devices, you should select only one device for which you are creating the job.</td>
</tr>
<tr>
<td>Task Selector</td>
<td>Select the System-defined tasks or User-defined tasks that you want to run on the selected devices. All System-defined and User-defined tasks are categorized into various task groups. To select the tasks, expand the corresponding Task Group node. You can also search for a task or a group of tasks in the Task Selector by entering the Search expressions in the Search field. You can use the wildcard character “*” along with the Search expression. When you click the Search icon, the results are displayed in the Search Results tab. For descriptions of System-defined tasks and the device categories they support, see Using System-defined Tasks. For creating and using User-defined tasks, see Creating and Editing User-defined Tasks.</td>
</tr>
</tbody>
</table>

Step 4  Select the devices from the Device Selector pane. See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to use the Device Selector.

Step 5  Select the tasks from the Task Selector.

You can select one or more tasks at a time. Your selection will appear in the Selection pane.

Step 6  Click Next.

The Add Tasks dialog box appears with these panes:

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable Tasks</td>
<td>Allows you to add a task. The tasks that you had selected using the Task Selector appear here. Note Of the tasks selected, only tasks that apply to the devices selected appear here. Select a task and click Add to create an instance for the task (see Step 7).</td>
</tr>
<tr>
<td>Added Instances</td>
<td>Allows you to edit the task instance you have added, view its CLI, or delete it. Select the instance of the task and click the required button (see Table 5-2).</td>
</tr>
</tbody>
</table>

The buttons available in this page are:

<table>
<thead>
<tr>
<th>Table 5-2</th>
<th>Tasks Performed by Buttons in the Added Instances Pane</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buttons</td>
<td>Description</td>
</tr>
<tr>
<td>Edit</td>
<td>Task pop-up opens with previously assigned values. You can modify these values and click Save.</td>
</tr>
</tbody>
</table>
Starting a New NetConfig Job

**Step 7** Select an applicable task and click **Add**.

The pop-up for the selected task appears.

**Step 8** Set the parameters in the task dialog box and click **Save**.

(To reset the values that you have selected click **Reset**. Click **Cancel** to return to the previous dialog box, without saving your changes.)

You will see the instance of the task in the Added Tasks pane. The instance appears in the format: **Taskname_n**, where **Taskname** is the name of the task you have added, and **n** is the number of the instance. For example, the first instance of a Banner task is **Banner_1**.

You can add as many instances as required, for a task.

**Step 9** Click **Next**.

The Job Schedule and Options dialog box appears.

**Step 10** Set the schedule for the job, in the Scheduling pane:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Type</td>
<td>Select the run type or frequency of the job—Immediate, Once, Daily, Weekly, Monthly, or Last Day of Month. If Job Approval is enabled, the Immediate option is not available.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the start date for the job.</td>
</tr>
<tr>
<td>At</td>
<td>Select the start time for the job from the hour and minute drop-down lists.</td>
</tr>
</tbody>
</table>
### Starting a New NetConfig Job

**Step 11** Set the job options, in the Job Options pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job Info</strong></td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter the Job Description. This is mandatory. Make each description unique so you can easily identify jobs.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter the e-mail addresses to which the status notices of the job will be sent. Separate multiple addresses with commas or semicolons. You must configure the SMTP server to send e-mails (<a href="#">Admin &gt; System &gt; System Preferences</a>). Notification e-mails include a URL that displays the job details (<a href="#">Viewing Job Details</a> for more information on the details displayed). You need to be logged in to view the job details.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter your comments for the job. Comments appear in the job work order and are stored in the configuration archive.</td>
</tr>
<tr>
<td>Approver Comments</td>
<td>Enter comments for the job approver. This field is displayed only if you have enabled job approval for NetConfig. See <a href="#">Administration of Cisco Prime LAN Management Solution 4.2</a> for more information.</td>
</tr>
<tr>
<td>Maker E-mail</td>
<td>Enter the E-mail ID of the job creator. This field is displayed only if you have enabled job approval for NetConfig. This is a mandatory field. See <a href="#">Administration of Cisco Prime LAN Management Solution 4.2</a> for more information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail on Mismatch of Config Versions</td>
<td>Select to consider the job to be a failure when the most recent configuration version in the configuration archive is not identical to the most recent configuration version that was in the configuration archive when you created the job.</td>
</tr>
<tr>
<td>Sync Archive before Job Execution</td>
<td>Directs LMS archive running configuration before applying configuration changes.</td>
</tr>
<tr>
<td>Copy Running Config to Startup</td>
<td>Directs LMS to write the running configuration to the startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.</td>
</tr>
</tbody>
</table>

**Enable Job Password**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Username</td>
<td>Enter the Login Username. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This option overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of LMS.</td>
</tr>
<tr>
<td>Login Password</td>
<td>Enter the job password. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This option overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of LMS.</td>
</tr>
</tbody>
</table>
### Chapter 5      Making and Deploying Configuration Changes Using NetConfig

#### Starting a New NetConfig Job

**Step 12**  Click **Device Order** to view the order of the device.

The Set Device Order pop-up appears. You can reset the order in which the job should be executed on the devices using the Up and Down arrows.

When you are done, click **Done**. The pop-up closes.

**Step 13**  Click **Next**.

The Job Work Order dialog box appears with the general information about the job, the job policies, the job approval details (if you have enabled job approval), the device details, the task, and the CLI commands that will be executed on the selected devices as part of this job.

**Step 14**  Click **Finish** after you review the details of your job in the Job Work Order dialog box.

A notification message appears along with the Job ID. The newly created job appears in the NetConfig Job Browser.

### Enable Password

Enter the Enable password. This option is available to you if you have set the appropriate job password policy in the Configuration Management module.

This option overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of LMS.

### Failure Policy

Select one of these options to specify what the job should do if it fails to run on a device.

- **Stop on failure**—If the job fails to execute on a device, the job is stopped. The database is updated only for the devices on which the job was executed successfully.
- **Ignore failure and continue**—If the job fails on a device, the job skips the device and continues with the remaining devices. The database is updated only for the devices on which the job was executed successfully.
- **rollback device and stop**—Rolls back the changes on the failed device and stops the job.
- **rollback device and continue**—Rolls back the changes on the failed device and continues the job.
- **rollback job on failure**—Rolls back the changes on all devices and stops the job. See **Configuring a Job to Roll Back on Failure**.

### Execution

Specify the order in which the job should run on the devices.

- **Parallel**—Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time.
- **Sequential**—Allows the job to run on only one device at a time. If you select sequential execution, you can click **Set Device Order** to set the order of the devices.

In the Device Ordering dialog box:

a. Select a device name

b. Click **Move Up** or **Move Down** to change its place in the order.

c. Click **OK** to save the current order and close the dialog box

or

Click **Cancel** to close the dialog box without making any changes.

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Password</td>
<td>Enter the Enable password. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This option overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of LMS.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Policy</td>
<td>Select one of these options to specify what the job should do if it fails to run on a device.</td>
</tr>
<tr>
<td></td>
<td>• Stop on failure—If the job fails to execute on a device, the job is stopped. The database is updated only for the devices on which the job was executed successfully.</td>
</tr>
<tr>
<td></td>
<td>• Ignore failure and continue—If the job fails on a device, the job skips the device and continues with the remaining devices. The database is updated only for the devices on which the job was executed successfully.</td>
</tr>
<tr>
<td></td>
<td>• Rollback device and stop—Rolls back the changes on the failed device and stops the job.</td>
</tr>
<tr>
<td></td>
<td>• Rollback device and continue—Rolls back the changes on the failed device and continues the job.</td>
</tr>
<tr>
<td></td>
<td>• Rollback job on failure—Rolls back the changes on all devices and stops the job. See <strong>Configuring a Job to Roll Back on Failure</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution</td>
<td>Specify the order in which the job should run on the devices.</td>
</tr>
<tr>
<td></td>
<td>• Parallel—Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time.</td>
</tr>
<tr>
<td></td>
<td>• Sequential—Allows the job to run on only one device at a time. If you select sequential execution, you can click <strong>Set Device Order</strong> to set the order of the devices. In the Device Ordering dialog box:</td>
</tr>
<tr>
<td></td>
<td>a. Select a device name</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Move Up</strong> or <strong>Move Down</strong> to change its place in the order.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>OK</strong> to save the current order and close the dialog box or</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Cancel</strong> to close the dialog box without making any changes.</td>
</tr>
</tbody>
</table>
Create a NetConfig Job based on Module or Port

You can create a NetConfig job for ports or modules by selecting a port or module group from the Group Selector page in the NetConfig job flow.

You can create a NetConfig job for all devices in the port or module group, which is the default, or for a few devices in the port or module group. If devices are not available in the port or module groups, then Netconfig job will not be created and displays the following message: No devices in selected group.

To run the job for a few select devices, you need to select the devices from the Devices and Groups page and the port or module from the Group Selector page. The job will run for the selected devices provided the devices are available in the port or module selected. If there are no devices in Devices and Groups page, then the Netconfig job will be created only for the devices that are part of port or module groups.

To start a new NetConfig job based on Modules or Ports:

---

Step 1  Select either:

- Configuration > Tools > NetConfig > Deploy
  Or
- Configuration > Job Browsers > NetConfig

The NetConfig Job Browser appears.

Step 2  Click Create.

The Netconfig Job Type page appears, displaying the following job flows:

- Device Based
- Module Based
- Port Based

Step 3  Either select:

- Module Based—To create a NetConfig job based on modules.
  Or
- Port Based—To create a NetConfig job based on ports.

Step 4  Click Go.

The Device and Group Selector dialog box appears, with these options:

**Options** | Description
--- | ---
Device Selector | Allows you to select the devices on which the NetConfig job has to run. You can select multiple devices.
Group Selector | Allows you to select the device groups on which the NetConfig job has to run. You can select multiple device groups.

**Step 5**  Either:

- Select the devices using the Device Selector option.
  Or
- Select the device groups using the Group Selector option.

You can also skip this page by clicking Next and directly go to Group Selector page.
Step 6  Click Next.

The Group Selector page appears displaying the Port or Module Groups dialog box with these options:

<table>
<thead>
<tr>
<th>Options</th>
<th>Field/Button</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Custom Group</td>
<td></td>
<td>Select the group on which the NetConfig job has to run. You can select multiple groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Module groups are displayed for a Module based NetConfig job.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Port groups are displayed for a Port based NetConfig job.</td>
</tr>
<tr>
<td>Define an Adhoc Rule</td>
<td></td>
<td>Allows you to define Adhoc rules for a specific NetConfig job.</td>
</tr>
<tr>
<td>Object Type</td>
<td>Select the Object Type to form a group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Module—This Object Type is listed only if you are creating a NetConfig job for modules.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Port—This Object Type is listed only if you are creating a NetConfig job for ports.</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Object type attributes, based on which you can define the group.</td>
<td></td>
</tr>
<tr>
<td>Operator</td>
<td>Operator to be used in the rule. The list of possible operators changes based on the Variable selected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When using the <em>equals</em> operator the rule is case-sensitive.</td>
<td></td>
</tr>
<tr>
<td>Value</td>
<td>Value of the rule expression. The possible values depend upon the variable and operator that you have selected. The value may be free-form text or a list of values. Wildcard characters are not supported.</td>
<td></td>
</tr>
<tr>
<td>Add Rule Expression (Button)</td>
<td>Used to add the rule expression to the group rules.</td>
<td></td>
</tr>
<tr>
<td>Rule Text</td>
<td>Displays the rule.</td>
<td></td>
</tr>
<tr>
<td>Check Syntax (Button)</td>
<td>Verifies that the rule syntax is correct.</td>
<td></td>
</tr>
<tr>
<td>Include (Button)</td>
<td>Lists all the modules or ports from the selected devices that are not matching the rule. You can later choose to include the modules or ports for group creation. Click <strong>Include</strong> to launch the Include List window.</td>
<td></td>
</tr>
<tr>
<td>Exclude (Button)</td>
<td>Lists all the modules or ports from the selected devices that are matching the rule. You can later choose to exclude those modules or ports for group creation. Click <strong>Exclude</strong> to launch the Exclude List window.</td>
<td></td>
</tr>
</tbody>
</table>

Step 7  Click Next.

The Port or Module Tasks page appears.

Step 8  Select the following task using the Task Selector:
Starting a New NetConfig Job

Your selection appears in the Selection pane.

Step 9  Click Next.

The Add Tasks dialog box appears with these panes:

<table>
<thead>
<tr>
<th>Port/Module Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOLD Health Monitoring Test Task</td>
<td>Configure GOLD Health Monitoring tests on modules.</td>
</tr>
<tr>
<td>Adhoc Task</td>
<td>Configures user-defined commands on selected interfaces within a port group.</td>
</tr>
<tr>
<td>Manage Auto Smartports</td>
<td>Enables or disables Auto Smartports macros at port level.</td>
</tr>
<tr>
<td>Smartports</td>
<td>Applies Smartports macros at port level.</td>
</tr>
<tr>
<td>Catalyst Integrated Security Features</td>
<td>Configures port security features.</td>
</tr>
<tr>
<td>PoE Task</td>
<td>Configures power policies in ports.</td>
</tr>
<tr>
<td>EnergyWise Parameters Task</td>
<td>Configures EnergyWise in ports.</td>
</tr>
<tr>
<td>EnergyWise Events Task</td>
<td>Configures EnergyWise events in ports.</td>
</tr>
</tbody>
</table>
| SRE Operation Task | Configures the following operations on Services Ready Engine (SRE) supported devices at port level:
  • Install—Install application in service modules.
  • Uninstall—Uninstall application from service modules.
  • Status—Displays the following:
    – Status of the service module
    – The applicable running on the module
    – Status of the installation and uninstallation being performed in the service module
  • Abort—Stop installation on a set of service modules in a SRE device.
  • Shutdown—Shutdown the set of service modules in a SRE device.
  • Reset—Reset service modules in a SRE device. |

Your selection appears in the Selection pane.

Pane | Description
--- | ---
Applicable Tasks | Allows you to add a task. The task that you selected using the Task Selector, appears here. From your selection, only the tasks that are applicable to at least one device that you have selected, appear here. Select a task and click Add Instance to create an instance for the task (see Step 10). |
Added Instances | Allows you to edit the task instance you have added, view its CLI, or delete it. Select the instance of the task, and click the required button (see Table 5-3). |
The buttons available in this page are:

<table>
<thead>
<tr>
<th>Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Task pop-up opens with previously assigned values. You can modify the values.</td>
</tr>
<tr>
<td>View CLI</td>
<td>Device Commands pop-up opens with the list of applicable devices and their corresponding CLI commands. Devices in your selection for which the commands are not applicable, are also displayed as Non-Applicable Devices.</td>
</tr>
<tr>
<td>View Ports</td>
<td>Port Details pop-up opens showing the list of devices, their corresponding ports and the port group rule. For example, Port Group: 100 Mbps Ethernet Ports Port Group Rule: Port.Speed = &quot;100000000&quot; AND Port.Type = &quot;6&quot; IN Port.GROUP_ID = &quot;/RME@rme-ch-dev-sf4/All Devices&quot; Ports matching the port group rule: 4/1 4/2 4/3 4/4 4/5 4/6 4/7</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected task instance.</td>
</tr>
</tbody>
</table>

**Step 10** Select the applicable task and click **Add**. The pop-up for the selected task appears.

**Step 11** Set the parameters in the Task dialog box and click **Save**. You will see the instance of the task in the Added Tasks pane of the Add Tasks dialog box. The instance appears in the format: Taskname_n, where Taskname is the name of the task you have added, and n is the number of the instance. For example, the first instance of a Banner task is Banner_1. You can add as many instances as required, for a task.

**Step 12** Click **Next**. The Job Schedule and Options dialog box appears.
Starting a New NetConfig Job

**Step 13** Set the schedule for the job, in the Scheduling pane:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>Select the run type or frequency for the job—Immediate, Once, Daily, Weekly, Monthly, or Last Day of Month.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the start date for the job.</td>
</tr>
<tr>
<td>at</td>
<td>Select the start time for the job from the hour and minute drop-down lists.</td>
</tr>
<tr>
<td><strong>Job Info</strong></td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter the Job Description. Make each description unique so you can easily identify jobs. This is mandatory.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job will send status notices. Separate multiple addresses with commas or semicolons. You must configure the SMTP server to send e-mails (Admin &gt; System &gt; System Preferences). Notification e-mails include a URL that displays the job details. See Viewing Job Details. If you are not logged in, you must log in using the provided login panel to view the job details.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter your comments for the job. Comments appear in job work order and are stored in configuration archive.</td>
</tr>
<tr>
<td>Approver Comments</td>
<td>Enter comments for the job approver. This field is displayed only if you have enabled job approval for NetConfig. See Administration of Cisco Prime LAN Management Solution 4.2 for more information.</td>
</tr>
<tr>
<td>Maker E-mail</td>
<td>Enter the e-mail-ID of the job creator. This field is displayed only if you have enabled job approval for NetConfig. This is a mandatory field. See Administration of Cisco Prime LAN Management Solution 4.2 for more information.</td>
</tr>
</tbody>
</table>

**Step 14** Set the job options, in the Job Options pane:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail on Mismatch of Config Versions</td>
<td>Select to cause job to be considered a failure when the most recent configuration version in the archive is not identical to the most recent configuration version that was in the archive when you created the job.</td>
</tr>
<tr>
<td>Sync Archive before Job Execution</td>
<td>Select to cause job to archive running configuration before making configuration changes.</td>
</tr>
<tr>
<td>Copy Running Config to Startup</td>
<td>Select to cause job to write the running configuration to the startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.</td>
</tr>
</tbody>
</table>

**Enable Job Password**

Login Username | Enter the Login Username. This option is available if you have set the appropriate job password policy in the Configuration Management module. This option overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of LMS.
### Starting a New NetConfig Job

**Step 15** Click **Device Order** to view the device order. The Set Device Order pop-up appears.

You can reset the order in which the job should be executed on the devices using the up and down arrows.

**Step 16** Click **Next**.

The Job Work Order dialog box appears with:

- General information about the job
- Job policies
- Job approval details (if you have enabled job approval)
- Device details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Password</td>
<td>Enter the job password. This option is available if you have set the appropriate job password policy in the Configuration Management module. This option overrides the credentials that you entered at the time of adding the device in the Device and Credentials Administration module of LMS.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the Enable password. This option is available if you have set the appropriate job password policy in the Configuration Management module. This option overrides the credentials that you entered at the time of adding the device in the Device and Credentials Administration module of LMS.</td>
</tr>
</tbody>
</table>
| Failure Policy    | Select one of these options to specify what the job should do if it fails to run on a device.  
  • Stop on failure—If the job fails to execute on a device, the job is stopped. The database is updated only for the devices on which the job was executed successfully.  
  • Ignore failure and continue—If the job fails on a device, the job skips the device and continues with the remaining devices. The database is updated only for the devices on which the job was executed successfully.  
  • Rollback device and stop—Rolls back the changes on the failed device and stops the job.  
  • Rollback device and continue—Rolls back the changes on the failed device and continues the job.  
  • Rollback job on failure—Rolls back the changes on all devices and stops the job. See Configuring a Job to Roll Back on Failure |
| Execution         | Specify the order in which the job should run on the devices.  
  • Parallel—Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time.  
  • Sequential—Allows the job to run on only one device at a time. If you select sequential execution, you can click **Set Device Order** to set the order of the devices. In the Device Ordering dialog box:  
    a. Select a device name  
    b. Click **Move Up** or **Move Down** to change its place in the order.  
    c. Click **OK** to save the current order and close the dialog box  
       or  
    Click **Cancel** to close the dialog box without making any changes. |
Step 17 Click **Finish** after you review the details of your job in the Job Work Order dialog box.

A notification message appears along with the Job ID. The newly created job appears in the NetConfig Job Browser.

---

### Browsing and Editing Jobs Using the NetConfig Job Browser

You can browse the NetConfig jobs that are registered on the system. Using the NetConfig Job Browser, you can also manage NetConfig jobs (create, edit, copy, retry, stop, or delete).

To create and start a new NetConfig job, see [Starting a New NetConfig Job](#).

**Note** View Permission Report (**Reports > System > Users > Permission**) to check whether you have the required privileges to perform this task.

To invoke the NetConfig Job browser that lists all the scheduled report jobs, select either:

- **Configuration > Tools > NetConfig > Deploy**
- **Configuration > Job Browsers > NetConfig**

The columns in the NetConfig job browser displays the following information:
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique number assigned to a job when it is created.</td>
</tr>
<tr>
<td></td>
<td>For periodic jobs such as Daily, Weekly, the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001.</td>
</tr>
<tr>
<td></td>
<td>Click on the hyperlink to view the Job details. See Viewing Job Details.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the job:</td>
</tr>
<tr>
<td></td>
<td>• Successful—When the job is successful.</td>
</tr>
<tr>
<td></td>
<td>• Failed—When the job has failed.</td>
</tr>
<tr>
<td></td>
<td>The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed.</td>
</tr>
<tr>
<td></td>
<td>For example, If the status displays Failed(5), then the count of devices that had failed amounts to 5.</td>
</tr>
<tr>
<td></td>
<td>• Cancelled—When the job has been stopped.</td>
</tr>
<tr>
<td></td>
<td>• Running—When the job is in progress.</td>
</tr>
<tr>
<td></td>
<td>• Waiting—When the job is waiting for approval (if job approval has been enabled).</td>
</tr>
<tr>
<td></td>
<td>• Rejected—When the job has been rejected (if job approval has been enabled).</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the job, entered at the time of job creation.</td>
</tr>
<tr>
<td>Owner</td>
<td>Username of the job creator.</td>
</tr>
<tr>
<td>Scheduled at</td>
<td>Date and time at which the job was scheduled.</td>
</tr>
<tr>
<td>Completed at</td>
<td>Date and time at which the job was completed.</td>
</tr>
<tr>
<td>Flow Type</td>
<td>Type of the job flow—Port, Module, Device.</td>
</tr>
<tr>
<td>Schedule Type</td>
<td>Type of job schedule—Immediate, Once, Daily, Weekly, Monthly, Last day of the month. You can specify when you want to run the NetConfig job.</td>
</tr>
<tr>
<td></td>
<td>To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs the report immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs the report once at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>• Daily—Runs daily at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly—Runs weekly on the day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Monthly—Runs monthly on the day of the month and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Last Day of the Month—Runs the job on the last day of the month, beginning with the month that you specify.</td>
</tr>
<tr>
<td></td>
<td>For periodic jobs, the subsequent instances will run only after the earlier instance of the job is complete.</td>
</tr>
<tr>
<td></td>
<td>For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the November 1 job has completed. If the 10:00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.</td>
</tr>
</tbody>
</table>
You can filter the jobs using the Filter by field in the NetConfig Job Browser using any of the following criteria:

<table>
<thead>
<tr>
<th>Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Select All to display all jobs in the job browser</td>
</tr>
<tr>
<td>Job ID</td>
<td>Select Job ID and enter the Job ID that you want to display. For non-periodic jobs, the specified Job ID appears in the browser. For periodic jobs, all the instances of the selected Job ID will also be displayed in the browser.</td>
</tr>
</tbody>
</table>
| Status          | Select Status and then select any one of these:  
|                | • Successful  
|                | • Failed  
|                | • Cancelled  
|                | • Running  
|                | • Scheduled  
|                | • Approved  
|                | • Waiting  
|                | • Rejected |
| Description     | Select Description and enter the first few letters or the complete description. |
| Owner           | Select Owner and enter the user ID or the beginning of the user ID. |
| Schedule Type   | Select the schedule type and select any one of these:  
|                | • Immediate  
|                | • Once  
|                | • Daily  
|                | • Weekly  
|                | • Monthly  
|                | • Last day of the month |
| Flow Type       | Select Flow Type and then select any one of these:  
|                | • Device  
|                | • Port  
|                | • Module |
| Refresh (Icon)  | Click this icon to refresh the NetConfig job browser. |

You can schedule a default purge job to purge the records of NetConfig jobs.
You can perform the following operations using the NetConfig job browser. (See Table 5-4):

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>
| Edit   | Edits the selected pending job.  
• For Device based jobs, the Job definition opens at the Devices and Tasks dialog box, with current information about the job.  
• For Module based jobs, the Job definition opens at the Devices and Groups dialog box, with current information about the job.  
• For Port based jobs, the Job definition opens at the Devices and Groups dialog box, with current information about the job.  
You can edit a job the same way you define and schedule a new job. See Starting a New NetConfig Job.  
The Job ID of an edited job remains unchanged. | Unless you own a job, your login ID determines whether you can use this option.  
If the job start time occurs during editing, it runs without edits. You can complete the edits and schedule the job to run again, but you cannot re-edit the job.  
To prevent the job from running without edits, either:  
• Complete your edits before the job start time.  
Or  
• Cancel the job and create a new one. |
Browsing and Editing Jobs Using the NetConfig Job Browser

---

### Table 5-4: Operations Using the NetConfig Job Browser (continued)

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>
| Copy   | Copies selected job.  
You can copy a job and give it a new schedule.  
- For Device based jobs, the Job definition opens at the Devices and Tasks dialog box, with all the selections for the job that you are copying.  
- For Module based jobs, the Job definition opens at the Devices and Groups dialog box, with all the selections for the job that you are copying.  
- For Port based jobs, the Job definition opens at the Devices and Groups dialog box, with all the selections for the job that you are copying.  
You can copy a job in the same way you define and schedule a new job.  
See Starting a New NetConfig Job.  
A new Job ID with the copied job details is created. | - |
| Retry  | Retry a failed job.  
- For Device based jobs, the Job definition opens at the Devices and Tasks dialog box.  
  You can edit the job the same way as you would define and schedule a new job. However, you cannot add new devices or change the tasks for the job that you are retrying.  
  You can select a few of the failed devices to retry the job.  
- For Module based jobs, the Job definition opens at the Devices and Groups dialog box.  
  You can edit the job the same way as you would define and schedule a new job. However, you cannot add new devices, modules or change the tasks for the job that you are retrying.  
  You can select a few of the failed devices to retry the job.  
- For Device based jobs, the Job definition opens at the Devices and Groups dialog box.  
  You can edit the job the same way as you would define and schedule a new job. However, you cannot add new devices, ports or change the tasks for the job that you are retrying.  
  You can select a few of the failed devices to retry the job.  
| Unless you own the job, your login determines whether you can use this option.  
There may be some devices whose configuration has been downloaded. However, their running configuration has not been written to the Startup configuration.  
You can perform Retry Job on these devices just as you can on a failed job. |
Browsing and Editing Jobs Using the NetConfig Job Browser

You can learn more about any job by viewing its details.

**Step 1**
Go to the NetConfig Job Browser and click the Job ID hyperlink. See Starting a New NetConfig Job to invoke the NetConfig Job Browser.

The Job Details pop-up appears, displaying the day, date and time details in the header at the top of the report. The Job ID and the Status appear in the header of the report.

The Job Details dialog box has two panes. The left pane contains a table of contents for the job results. The results appear in the right pane.

**Step 2**
Click a content in the left pane to view its corresponding report in the right pane.

**Step 3**
Click expand and collapse icons to open and close the folder tree in the left pane.

If a folder has subfolders, the next level of subfolders appears under it. Otherwise, its corresponding report appears in the right pane.

The contents of the left pane depends on the state of the job. The left pane can contain:

- Job Summary (in the Job Details folder).
- Downloaded Devices (in the Device Details folder).
- Work Order

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop</td>
<td>Stops or cancels a running job. You will be asked to confirm the cancellation of the job. However, the job will be stopped only after the devices currently being processed are successfully completed. This is to ensure that no device is left in an inconsistent state. If the job that you want to stop is a periodic job, you will also be asked whether you want to cancel all the instances of the job. Click OK to cancel all instances. If you click Cancel, only the selected instance of the job is cancelled. The next instance of the job will appear in the Job browser with the status Scheduled.</td>
<td>Unless you own the job, your login determines whether you can use this option. You cannot restart the stopped job. You can however copy the stopped job and Job ID.</td>
</tr>
</tbody>
</table>
| Delete     | Deletes the selected job from the job browser. You can select more than one job to delete. You will be asked to confirm the deletion. If the job that you have selected for deletion is a periodic job, this message appears:

If you delete periodic jobs, or instances of a periodic job, that are yet to be run, the jobs will no longer run, nor will they be scheduled to be run again. You must then recreate the deleted jobs. Do you want to continue? Click OK to confirm the deletion. The selected job will be deleted. You can delete a job that has been successful, failed, or stopped, but you cannot delete a running job. | Unless you own the job, your login determines whether you can use this option. You must stop a running job before you can delete it. |
### Browsing and Editing Jobs Using the NetConfig Job Browser

<table>
<thead>
<tr>
<th>Page/Folder</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Details</td>
<td>Job Summary</td>
<td>Click to display summary of completed job:</td>
</tr>
<tr>
<td></td>
<td>• Job Summary:</td>
<td>- Status</td>
</tr>
<tr>
<td></td>
<td>• Job Summary:</td>
<td>- Start Time</td>
</tr>
<tr>
<td></td>
<td>• Job Summary:</td>
<td>- End Time</td>
</tr>
<tr>
<td></td>
<td>• Job Messages:</td>
<td>- Pre-job Execution</td>
</tr>
<tr>
<td></td>
<td>• Job Messages:</td>
<td>- Post-job Execution</td>
</tr>
<tr>
<td></td>
<td>• Device Update:</td>
<td>- Successful</td>
</tr>
<tr>
<td></td>
<td>• Device Update:</td>
<td>- Failed</td>
</tr>
<tr>
<td></td>
<td>• Device Update:</td>
<td>- Not attempted</td>
</tr>
<tr>
<td></td>
<td>• Device Update:</td>
<td>- Pending</td>
</tr>
<tr>
<td></td>
<td>• Device Update:</td>
<td>- Devices Pending Registration for Smart Call Home (SCH)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The URL <a href="https://tools.cisco.com/sch/pendingDevices.do">https://tools.cisco.com/sch/pendingDevices.do</a> is displayed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>only for SCH NetConfig jobs. Click the URL to register the devices that</td>
</tr>
<tr>
<td></td>
<td></td>
<td>are pending to process SCH messages at Cisco.com.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information on Devices Pending Registration for SCH, see the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Smart Call Home User Guide at:</td>
</tr>
<tr>
<td>Device Details</td>
<td>Downloaded Devices</td>
<td>Contains detailed job results for each device in a table:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Device—List of devices on which the job ran.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Status—Status of job (success, failure, etc.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Message—A message about the status of a job.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- If the job failed on the device, the reason for failure is displayed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- If the job was successful on the device, the message Deploy Successful</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is displayed.</td>
</tr>
</tbody>
</table>

You can filter the devices by selecting a status and clicking **Filter**.

This page displays the number of rows you have set for display in the Rows per Page field. You can increase the rows up to 500 in each page.

You can navigate among the pages of the report using the navigation icons at the right bottom of this table.

Click on a device to view the details such as protocol, status and reason when applicable, task used and the CLI output for that device. These details appear in a pop-up window.

Double-click to display status folders that correspond to possible device status.
Creating and Editing User-defined Tasks

You can create User-defined Tasks and add one or more templates to each task.

The template, in turn, is associated with the Meta-Data Framework (MDF) categories of devices, for which these templates will be applicable.

The templates contain configuration commands and rollback commands (see Creating Rollback Commands). You can enter the configuration commands either by typing them or by importing them from a file.

You can create a new task and add one or more templates to it. You can also add templates to an existing task. Name a task when you create it and as it is saved for future use. You can copy, edit, and reuse your tasks. You can assign access privileges to tasks while or after you create them (see Assigning Tasks to Users).

You cannot add User Defined Templates to System Defined Tasks.

After you have successfully created a User-defined Task, this task will appear under the User-defined Tasks group in the Task Selector of the NetConfig Job creation wizard. You can create a NetConfig job using the User-defined task. For details on the Task Selector and job creation, see Step 2 in Starting a New NetConfig Job.
Creating and Editing User-defined Tasks

For each template, you should specify all the information including the configuration commands, rollback commands (see Rolling Back Configuration Changes), mode (Config or Enable), and the device category for which these commands will be applicable.

At the time of job creation, you should ensure that the User-defined task that you have selected is applicable to the MDF categories of the devices that you have selected.

If the task that you have selected does not apply to the categories of any of the devices that you have selected, it will not be displayed in the Applicable Tasks pane of the NetConfig job wizard, during job creation.

For example, if you have selected an CatalystOS category of device, but selected a user-defined task that is applicable to a Cable device, then the task will not appear in the Applicable Tasks pane of the job wizard and you will not be able to proceed further with the job creation. For details on the Applicable Tasks pane and job creation, see Step 6 in Starting a New NetConfig Job.

Caution

NetConfig does not validate the commands you enter in a user-defined template within a task. If you enter incorrect commands you might misconfigure or disable the devices on which the job using the template runs.

View the Permission Report (Reports > System > Users > Permission) to check whether you have the required privileges to perform this task.

Step 1

Select Configuration > Tools > NetConfig > User Defined Tasks.

The User-defined Tasks dialog box appears. If you are creating a task for the first time, the system displays a message that there are no user-defined tasks.

The User-defined Tasks dialog box has a Tasks browser in its left pane. After you create a task, the task is displayed in the Tasks browser along with its templates.

Step 2

Define or edit a User-defined task by entering the following information in the dialog box.

<table>
<thead>
<tr>
<th>Area/Field/Button</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>
| Name              | Enter name for the new task. This is a mandatory field. | To create new task from a copy of an existing task:  
1. Select the name from Templates list,  
2. Enter the new name.  
3. Save the task.  
To modify a task, select it from the tasks list but do not modify its name.  
You can modify a task by adding or deleting templates, modifying existing templates and changing other details. |
| Template Name     | Enter the template name. This is a mandatory field. | Template Name is provided for User Defined Tasks when you create a template for more than one device category which has different commands to execute. |
### Creating and Editing User-defined Tasks

<table>
<thead>
<tr>
<th>Area/Field/Button</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command Mode</strong></td>
<td>Select mode (config or enable) in which commands will run.</td>
<td>Each user-defined template can run commands in one mode only. If you select <strong>Enable</strong>, enter Rollback Commands area is disabled because only config commands can be rolled back.</td>
</tr>
<tr>
<td><strong>Parameterized</strong></td>
<td>Select Parameterized if you want to create a parameterized template.</td>
<td>The template parameters will be picked up from a file that you specify, at the time of scheduling a job using this task. See “Parameterized Templates”.</td>
</tr>
<tr>
<td><strong>Device Type</strong></td>
<td>Select device category template will configure.</td>
<td>You can associate any number of MDF categories with a template, if the command is applicable to them.</td>
</tr>
</tbody>
</table>
| **CLI Commands**  | Enter configuration commands or select the configuration commands file. The configuration commands file should reside in the default location: On Solaris and Soft Appliance: 
/var/adm/CSCOpx/files/rme/netconfig/cmdFiles/ On Windows: 
\$NMSROOT\files\rme\netconfig\cmdFiles Where, \$NMSROOT is the LMS install directory. If you want to import the configuration commands from an existing file, enter the default file location in the Import from File field. Alternatively, when you click on the Browse button, a file browser opens with the default location of the configuration commands file. You cannot change this default import directory. | To enter configuration commands, do any of the following:  
• Type in larger text box, one command in each line.  
Or  
• Enter the default file location of the configuration command files in the Import from File field.  
• Click Browse. A file browser opens with the default location of the configuration commands file. You cannot change this default import directory.  
You can also enter interactive commands and multi-line commands. See Handling Interactive Commands. |
Creating and Editing User-defined Tasks

<table>
<thead>
<tr>
<th>Area/Field/Button</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rollback Commands</td>
<td>Enter configuration commands for the template to run when the job fails and the failure policy is set to the rollback option. If you want to import the rollback commands from an existing file, enter the file location in the Import from File field. The rollback commands file should reside in the default location: On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/netconfig/cmdFiles/ On Windows: NMSROOT\files\rme\netconfig\cmdFiles Where, NMSROOT is the LMS install directory. Alternatively, when you click on the Browse button, a file browser opens with the default location of the rollback commands file. You cannot change this default import directory.</td>
<td>To enter rollback commands, do any of the following: • Type in larger text box, one command in each line. • Enter the default file location of the rollback command files in the Import from File field. • Click Browse. A file browser opens with the default location of the configuration commands file. You cannot change this default import directory.</td>
</tr>
</tbody>
</table>

- Click **Save** to save the task with the current information.
  - Or
- Click **Delete** to delete the current task from the system.

To cancel the user-defined task you are creating, select a command from the Jobs or Admin menu (or a corresponding button) and click **Yes** in the resulting dialog box.

To add a user-defined task, select **Configuration > Tools > NetConfig > User Defined Tasks**. The User-defined Tasks dialog box appears with no values.

To copy a user-defined task:

**Step 1** Select the task from the Tasks browser.
The details appear in the right pane of the User-defined Tasks dialog box.

**Step 2** Change the name of the Task and click **Save**.
To modify a user-defined task:

---

**Step 1** Select the task from the Tasks browser.
The details appear in the right pane of the User-defined Tasks dialog box.

**Step 2** Select templates associated with the task from the Task browser, and modify them
You can change details such as the command mode, parameterization option, the device type, the CLI commands or the rollback commands.

You can add a template or delete an existing one. When you click Save, a message appears that the task is modified.

This section contains:

- Parameterized Templates
- Creating a Parameters File (XML file)
- Parameters File: More Examples

### Parameterized Templates

You can include parameterized templates within User-defined tasks. A parameterized template allows the configuration commands in the templates to contain user-defined variables.

Multiline feature of parameterized templates is not supported. However, interactive command deploy is supported.

You can select the Parameterized option when you create a User-defined task (see Creating and Editing User-defined Tasks). If you select the Parameterized option, you should enter the actual values for the parameters in the template in a separate Parameters file (see Creating a Parameters File (XML file)) when you create a NetConfig job (see Creating and Editing User-defined Tasks). The Parameters file is the XML file that contains the parameter values.

The Parameters file should reside on the server at this location:

- `NMSROOT\files\rme\netconfig\cmdFiles` (On Windows)
- `/var/adm/CSCOpx/files/rme/netconfig/cmdFiles/` (On Solaris and Soft Appliance)

where `NMSROOT` is the LMS install directory.

For details see Parameters File: More Examples.

To create a Parameterized User-defined task and apply this in a NetConfig job:

---

**Step 1** Create a User defined Task with variables embedded in the command body. For details see Creating and Editing User-defined Tasks.
For example:

You can enter the command `ntp server $ntpServer` in the CLI Commands text box in the User-defined Tasks dialog box.

**Step 2** Select the Parameterized check box in the User-defined Tasks dialog box.

**Step 3** Click Save to save your User-defined Parameterized task.
Step 4  Create the Parameters file (XML file) containing the values for $ntpServer task. For details, see Creating a Parameters File (XML file).

For example:

```xml
<DEVICE NAME = 10.76.38.54>
  <CMDPARAM NAME = ntpServer>
    <value>mytimeserver</value>
  </CMDPARAM>
</DEVICE>
```

Step 5  Repeat the above step in the Parameters file, for all the devices that you plan to include in the job, if each device refers to a different $ntpServer.

Alternatively, you can have a global section if that variable does not change for each device. For details, see Creating a Parameters File (XML file).

Step 6  Store the Parameters file in:

- $NMSROOT/files/rme/netconfig/cmdFiles directory (On Windows)
- /var/adm/CSCOpx/files/rme/netconfig/cmdFiles/ (On Solaris and Soft Appliance)

where $NMSROOT is the LMS install directory.

Step 7  Create a NetConfig job and select your User-defined Parameterized task. For details see Starting a New NetConfig Job.

You are prompted to enter the filename while adding the task to the NetConfig job.

You can check the syntax of the text file that contains the parameters. To do this, select Check Syntax.

Step 8  Complete the job creation. For details, see Creating and Editing User-defined Tasks.

---

Creating a Parameters File (XML file)

A specific format is defined for embedding variables in User-defined tasks and the corresponding Parameters file that contains the values for the parameters.

The variables in the User-defined tasks, which you enter in the CLI Commands text area of the User-defined Tasks dialog box (see Creating and Editing User-defined Tasks), should be preceded by $.

For example, for an NTP server parameter, it should be: $ntpServer.

Similarly, the Parameters file also follows a specified format.
Here is the sample format and example of the Parameters file (the XML command file that contains the values for the parameters) for a parameterized template:

```xml
<GLOBAL>
  <CMDPARAM NAME = password>
    <value>abc</value>
  </CMDPARAM>
  <CMDPARAM NAME = message>
    <value>test all</value>
  </CMDPARAM>
</GLOBAL>

<DEVICE NAME = 10.76.38.54>
  <CMDPARAM NAME = ntpServer>
    <value>ServerName</value>
  </CMDPARAM>
</DEVICE>
```

You can assign the device-specific values to variables in the `<DEVICE>` area. If there are no device-specific values, the default values in the `<GLOBAL>` area are considered as actual values for these variables. You do not need to add a `<GLOBAL>` area in the Parameters file if you are referencing each device explicitly (using the `<DEVICE>` area for each device).

### Parameters File: More Examples

This section gives more examples of the format of the text to be entered in the CLI Commands body at the time of creating a User-defined Task, and the commands to be entered in the corresponding Parameters file.

For example, you can enter these parameters while creating a User-defined task, in the CLI Commands text box:

```
ntp server ntpServer
ip http port portValue
ip address ipAddress
```

In the corresponding Parameters file, which is stored under:

- `NMSROOT\files\rme\netconfig\cmdFiles` directory (On Windows)
- `/var/adm/CSCOpx/files/rme/netconfig/cmdFiles/` (On Solaris and Soft Appliance)

where `NMSROOT` is the LMS install directory, enter:

```xml
<GLOBAL>
  <CMDPARAM NAME = ntpServer>
    <value>10.10.10.10</value>
  </CMDPARAM>
  <CMDPARAM NAME = portValue>
    <value>99</value>
  </CMDPARAM>
  <CMDPARAM NAME = ipAddress>
```

Creating and Editing User-defined Tasks

When the job contains the device 10.76.38.54, the following commands are generated:

ntp server 20.20.20.20 (taken from the device-specific section of the Parameters file)

ip http port 55 (taken from the device-specific section of the Parameters file)

ip address 1.1.1.1 (taken from the global section of the Parameters file)

When the job contains the device 10.77.202.229, the following commands are generated:

ntp server 30.30.30.30 (taken from the device-specific section of the Parameters file)

ip http port 90 (taken from the global section of the Parameters file)

ip address 1.1.1.1 (taken from the global section of the Parameters file)

When the job contains other devices, all the values are taken from the global section of the XML file, and the following commands are generated:

ntp server 10.10.10.10

ip http port 90

ip address 1.1.1.1

If the value for a parameter is not found in the command file, the syntax check (in the job creation flow) displays an error.

You can enter any special character, except <, >, and $, that is accepted by the device as the value for a parameter in the command file. This is because NetConfig does not process the parameter values. NetConfig only reads the value given between <value> and </value> tags and generates the command.
Assigning Tasks to Users

You can assign access privileges to NetConfig tasks, to users with Network Operator privileges or lesser. All other users with privileges higher than Network Operator are assigned all tasks by default.

A network administrator must assign task access privileges to other users. See Understanding NetConfig User Permissions section for details.

Note View the Permission Report (Reports > System > Users > Permission) to check whether you have the required privileges to perform this task.

To assign tasks to users:

Step 1 Select Configuration > Tools > NetConfig > Assigning Tasks.

The Assign Tasks dialog box appears.

Step 2 Enter the username of the user to whom you want to assign the tasks.

This should be a valid LMS user.

Step 3 Select the task that you want to allocate to the user from the Available tasks list box and click Add. You can select more than one task, by holding down the Shift key while selecting the task.

The selected tasks appear in the Selected Tasks list box.

To remove assigned tasks, select the tasks from the Selected Tasks list box and click Remove.

Step 4 Add all the required tasks to the Selected Tasks list box.

Step 5 Click Assign to assign the task access privileges to the specified user.

For a specified user, to see the assigned tasks, enter the username in the Username field and click Show Assigned.

The tasks assigned to the user appear in the Selected Tasks list box.

Step 6 Click Report to generate the User Task Report.

The User Task Report shows the list of users and the tasks assigned for each user.

Note By default, all the tasks are assigned to admin users. Therefore, the User Task Report will not list the users with Admin privileges.

Handling Interactive Commands

An interactive command is the input you will have to enter, following the execution of a command.

For example, on a Catalyst device, a clear counters command on a Cat 5000 will give the following output:

c5000# (enable) clear counters. This command will reset all MAC and port counters reported in CLI and SNMP. Do you want to continue (y/n) [n]?

In LMS, such commands can be included in config jobs executed via NetConfig or ConfigEditor. For more details also see Editing and Deploying Configurations Using Config Editor.

You can handle interactive commands using NetConfig user-defined templates, and by using Adhoc tasks. See Using NetConfig User-defined Templates and Adhoc Tasks.

You cannot run interactive commands through NetConfig CLI.

Using NetConfig User-defined Templates and Adhoc Tasks

You can enter an interactive command in the Enter CLI Commands area, using the following syntax:

```
CLI Command <R> command response 1 <R> command response 2
```

The `<R>` tag is case-sensitive and this must be entered in uppercase only.

**Example**

For a Catalyst device, a `clear counters` command will give the following output:

```
c5000# (enable) clear counters This command will reset all MAC and port counters reported in CLI and SNMP. Do you want to continue (y/n) [n]?
```

To clear the counter, the syntax is:

```
clear counters <R>y
```

To accept the default, the syntaxes are:

```
clear counters <R>n
```

or

```
clear counters <R>
```

To accept the default value, you do not need to enter any values after the tag `<R>`.

Handling Multi-line Commands

You can enter multi-line commands as a part of User-defined and Adhoc tasks. The multi-line commands must be within the tag `<MLTCMD>` and `</MLTCMD>`.

These tags are case-sensitive and you must enter them only in uppercase. You cannot start this tag with a space.

**Example**

```
<MLTCMD> banner login "Welcome to Cisco Prime LMS Essentials - you are using Multi-line commands" </MLTCMD>
```

You can have a blank line within a multi-line command. The commands within the MLTCMD tags are considered as a single command and will be downloaded as a single command onto the device.
Using System-defined Tasks

NetConfig provides System-defined configuration tasks. You can create configuration commands by using these tasks (see Understanding the System-defined Task User Interface (Dialog Box)).

Each task supports one or more device categories (see Table 5-5). Table 5-5 displays a comprehensive list of all templates available and a brief description of each.

- For Device-based jobs, the System-defined tasks are available in the Devices and Tasks dialog box of the NetConfig job wizard.
- For Port-based jobs, the System-defined tasks are available in the Port Tasks page of the NetConfig job wizard.
- For Module-based jobs, the System-defined tasks are available in the Module Tasks page of the NetConfig job wizard.

All System-defined tasks are categorized into various task groups in the Tasks Selector. To select the tasks, you must expand the corresponding Task Group node.

After you select the devices and the tasks and click Next (see Starting a New NetConfig Job), the selected tasks appear in the Applicable Tasks pane of the Add Tasks dialog box (in the Job wizard).

When you select an applicable task and click Add Instance, a dialog box appears for the selected System-defined configuration task.

This is a dynamic user interface. The task dialog box displays parameters, based on the devices that you selected in Device Selector.

For example, if you have selected IOS devices, you can specify IOS parameters in this dialog box. If not, this section will not be available to you.

When you enter information in the fields of the task and click Save, the task appears as a numbered instance in the Added Instances pane of the Add Tasks dialog box.

For the detailed procedure and for information on how to edit the task instances, view CLI, or delete the instances, see Starting a New NetConfig Job.

You can add multiple instances of a configuration task to a job by selecting an applicable task, adding information, and saving this information. You need to do this whenever you add instances. However, you can include only one instance of a task in a job.

Each System-defined task also creates Rollback commands that you can use to roll back the changes to devices if the job fails.

- View the Permission Report (Reports > System > Users > Permission) to check whether you have the required privileges to perform this task.
- If you use TFTP protocol to deploy NetConfig templates to devices, the DCR does not reflect the updates.
### Table 5-5 NetConfig System-Defined Tasks Supported by LMS Device Categories

<table>
<thead>
<tr>
<th>Task Group</th>
<th>Task</th>
<th>Description</th>
<th>IOS</th>
<th>CatOS</th>
<th>CSS</th>
<th>CE</th>
<th>NAM</th>
<th>PIX</th>
<th>Cable</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Adhoc Task</td>
<td>Enter any configuration commands as required.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication Proxy Task</td>
<td>Configure Authentication Proxy.</td>
<td></td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Banner Task</td>
<td>Add, remove, or edit banners.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CDP Task</td>
<td>Configure Cisco Discovery Protocol (CDP).</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>DNS Task</td>
<td>Configure DNS.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>HTTP Server Task</td>
<td>Configure HTTP access on VPN devices.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>IGMP Configuration Task1</td>
<td>Configure IGMP of selected cable interfaces.</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Internet Key Exchange (IKE) Configuration Task2</td>
<td>Configure IP security (IPSec).</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface IP Address Configuration Task</td>
<td>Configure IP interface address of selected interface.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP Server Configuration Task</td>
<td>Configure Network Time Protocol (NTP).</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>RCP Configuration Task</td>
<td>Configure rcp</td>
<td></td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Reload Task</td>
<td>Reload devices</td>
<td></td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Smart Call Home Task</td>
<td>Register devices with Cisco Smart Call Home</td>
<td></td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Syslog Task</td>
<td>Configure Syslog message logging.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Transform System-Defined Task</td>
<td>Configure IPSec.</td>
<td></td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User-defined Protocol Task</td>
<td>Configure the User-defined protocol on NAM devices.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web User Task</td>
<td>Configure the web user for NAM devices</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
### Table 5-5  
**NetConfig System-Defined Tasks Supported by LMS Device Categories**

<table>
<thead>
<tr>
<th>Task Group</th>
<th>Task</th>
<th>Description</th>
<th>IOS</th>
<th>CatOS</th>
<th>CSS</th>
<th>CE</th>
<th>NAM</th>
<th>PIX</th>
<th>Cable</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cable</strong></td>
<td>Cable BPI/BPI+ Task</td>
<td>Assign self-signed certificate, configure cable interface, and set BPI/BPI+ options.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cable DHCP-GiAddr and Helper Task&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Configure DCHP-GiAddr and Helper Address of the selected cable interface.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cable Downstream Task&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Activate/Deactivate DS Ports, Interleave Depth, MPEG Framing Format, Modulations, Channel ID and Frequency of the selected cable interfaces.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cable Interface Bundling Task&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Configure Interface Bundling on selected cable interface.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cable Spectrum Management Task</td>
<td>Assign Spectrum Groups and Interfaces on a selected cable interface.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cable Trap Source Task</td>
<td>Configure SNMP Traps hosts, notification, message and notification of SNMP Traps on a cable interface.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cable Upstream Task&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Activate and configure upstream on selected cable interfaces.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Credential</strong></td>
<td>Enable Password Task</td>
<td>Configure, or change enable or secret password to enter in enable mode on devices.</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Local Username Task</td>
<td>Configure local username and password authentication on devices.</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SSH Configuration Task</td>
<td>Configure SSH.</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Telnet Password Configuration Task</td>
<td>Add, remove, and edit Telnet passwords.</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td>Certification Authority Task&lt;sup&gt;2&lt;/sup&gt;</td>
<td>Create, or modify Certification Authority. Provides manageability and scalability for IP security (IPSec) standards on VPN devices.</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Crypto Map Task&lt;sup&gt;2&lt;/sup&gt;</td>
<td>Configure IPSec.</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>EEM</strong></td>
<td>Embedded Event Manager Task</td>
<td>Configure EEM Scripts or Applets on the devices</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>EEM Environmental Variables Task</td>
<td>Configure EEM Environmental Variables on the devices</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
### Table 5-5  NetConfig System-Defined Tasks Supported by LMS Device Categories

<table>
<thead>
<tr>
<th>Task Group</th>
<th>Task</th>
<th>Description</th>
<th>IOS</th>
<th>CatO S</th>
<th>CSS</th>
<th>CE</th>
<th>NAM</th>
<th>PIX</th>
<th>Cable</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnergyWise</td>
<td>EnergyWise Configuration Task</td>
<td>Configure EnergyWise in Devices</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>GOLD</td>
<td>GOLD Boot Level Task</td>
<td>Configure Boot Level Diagnositc tests on the devices</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>GOLD Monitoring Test Task</td>
<td>Configure GOLD Monitoring tests on devices</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>SNMP</td>
<td>SNMP Community Configuration Task</td>
<td>Add, remove, and edit SNMP community strings</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SNMP Security Configuration Task</td>
<td>Configure SNMP Security feature on devices.</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SNMP Traps Configuration Task</td>
<td>Configure SNMP traps.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Port Macros</td>
<td>Auto Smartports</td>
<td>Configure Auto Smartport macros on devices.</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>TACACS</td>
<td>TACACS Configuration Task</td>
<td>Configure TACACS authentication.</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>TACACS+ Configuration Task</td>
<td>Configure TACACS+ authentication.</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>RADIUS Server Configuration Task</td>
<td>Configure RADIUS server and task.</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1. You can apply this task only to a single device, at a time because cable templates configure interfaces on devices.
2. You must follow this sequence to complete the configuration of the IPSec on devices:
   a. IKE configuration System-defined task.
   b. Transform System-defined task.
   c. Crypto Map System-defined task.
Understanding the System-defined Task User Interface (Dialog Box)

NetConfig tasks support devices in the following device categories:

- IOS
- Catalyst OS
- Content Engine
- CSS
- NAM
- PIX OS
- Cable

Each of the system-defined tasks have their own dynamic user interface, or dialog box, that displays fields for a specified category of devices only if you have selected that category of device.

The dialog boxes for system-defined tasks may have these groups, links, and buttons:

- Common Parameters—This group of fields appears at the top of the task dialog box. In the fields under this group, you can enter the parameters that are common to all the categories of devices that you have selected.
- Device Category-specific Parameters—This group of fields is specific to a device category. If, for a specified device category, only the common parameters are applicable, this message appears in the user interface:

  No Category-specific Commands

- Applicable Devices—This link is available in the device category-specific group of fields and enables you to view the devices in your selection, to which the device-specific parameters apply.
- Buttons in the system-defined tasks interface:

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves the information that you have entered in the fields in the task dialog box.</td>
</tr>
<tr>
<td>Reset</td>
<td>Clears all the fields.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels your changes, and closes the task dialog box.</td>
</tr>
</tbody>
</table>

For the cable devices, you can apply a task only to a single device at a time, because cable templates configure interfaces on devices.

Also, for the cable tasks to work correctly, you must have valid SNMP credentials in Device and Credential Repository (DCR). See Administration of Cisco Prime LAN Management Solution 4.2 for more information on setting valid SNMP credentials.

Therefore, if you have selected more than one cable device and selected tasks for them, the task may not appear in the Applicable Tasks pane of the Add Tasks dialog box. For the tasks that are applicable to cable devices, see Table 5-5.
Understanding the NetConfig Credentials Configuration Tasks

NetConfig provides for tasks to configure credentials on devices. These tasks are:

- Enable Password (See Enable Password Task.)
- Local Username (See Local Username Task.)
- Radius Server (See RADIUS Server Configuration Task.)
- TACACS TACACS Configuration Task
- TACACS+ (See TACACS+ Configuration Task.)
- SNMP Community (See SNMP Community Configuration Task.)
- SNMP Security (See SNMP Security Configuration Task.)

The credential store allows only one set of login credentials per device - Primary username and primary password, irrespective of the authentication type. Hence, this imposes certain limitations on the NetConfig templates, especially, when you are configuring/modifying the authentication method on the device.

To overcome this, an option to specifically update the credential store is provided in the credential tasks. The credential store is updated only when this option is chosen with the values specified.

The usage of NetConfig credentials tasks to configure the credentials on a device should be based on the active credentials (e.g. Telnet, TACACS, etc.) in the device. For example if the device is configured with TACACS+, you should use only TACACS+ template to configure the credentials.

Example

When you remove the TACACS+ authentication for the device, the device reverts to the authentication method that was earlier configured on it. For example, the local username.

However, LMS is unaware of the fallback authentication method, and the respective credentials. If Device and Credential Repository is not updated with the right credentials, the subsequent device operations from LMS will fail.

In this case, you should select the option to update the local credential store and specify the local username credentials. When the job runs, NetConfig updates Device and Credential Repository with this set of credentials, so that for subsequent devices, access from LMS will be successful.

Adhoc Task

You can use the Adhoc system-defined task to add configuration commands to a job, during job definition.

You cannot save an instance of an Adhoc task, for future use. If you need to reuse a template that provides capabilities unavailable from the system-defined tasks, you can create a user-defined tasks (see Creating and Editing User-defined Tasks).

Caution

NetConfig does not validate commands you enter in the Adhoc task. If you enter incorrect commands, you might misconfigure or disable devices on which jobs that use the task run.

Groups for each of the device categories that you have selected, appear in the Adhoc Configuration dialog box. To invoke the Adhoc Configuration dialog box, see Starting a New NetConfig Job.
You can enter configuration and rollback commands for these device categories:
- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- CSS
- NAM
- PIX OS

For more details, see Table 5-5.

**Note**

As Cable devices fall under the IOS category, you can enter adhoc commands in the IOS group of fields in the Adhoc Configuration dialog box.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Adhoc Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands</td>
<td>CLI Command</td>
<td>Enter configuration commands. You can also enter interactive commands (see Handling Interactive Commands) and multi-line commands see Handling Multi-line Commands).</td>
</tr>
<tr>
<td></td>
<td>Rollback</td>
<td>Enter rollback commands.</td>
</tr>
<tr>
<td>Command Mode</td>
<td>Config or</td>
<td>Select the mode (config or enable) in which the task configuration commands will run. If you have selected Catalyst OS, or NAM devices, then the enable mode is preselected, and you do not have the option to select the config mode. The Command Mode group is not available for the Adhoc Task selected in the Port Based flow of the NetConfig job.</td>
</tr>
<tr>
<td></td>
<td>Enable</td>
<td></td>
</tr>
</tbody>
</table>

If you enter any credential command in the CLI Commands or Rollback Commands fields, then those credentials will be masked in the job work order and the job results page.

For example, the command, `snmp-server community public ro` will be displayed as `snmp-server community ***** ro`.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

**Authentication Proxy Task**

The Authentication Proxy feature helps users to log into the network or access the Internet using HTTP. Their specific profiles are automatically retrieved and applied from a CiscoSecure ACS, or other RADIUS, or TACACS+ authentication server.
The Cisco Secure Integrated Software authentication proxy feature allows network administrators to apply specific security policies on a user to user basis. You can use the Authentication Proxy system-defined configuration Task on IOS devices, which have been configured for VPN functionality. The IOS category of devices (including Cable devices) are supported by this task.

For more details, see Table 5-5.

You can enter the details of this task in the Authentication Proxy Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Authentication Proxy Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Parameters</td>
<td>Authorization (AAA)</td>
<td>Action</td>
<td>Select the required option to enable, disable or make no change to the authorization configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Method 1</td>
<td>Select either TACACS+ or RADIUS as your first method of authorization.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Method 2</td>
<td>Select either TACACS+ or RADIUS as your second method of authorization, based on your selection in the first method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cache Timeout Minutes (1-2147483647)</td>
<td>Timeout value. The default timeout value can be in the range of 1 and 2,147,483,647.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set to default</td>
<td>Select this to set the default cache timeout value of 60 seconds.</td>
</tr>
<tr>
<td>Banner</td>
<td></td>
<td>Action</td>
<td>Select <strong>Enable</strong> or <strong>Disable</strong> to set or reset Banner display in the login page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If you select <strong>Enable</strong>, the router name is displayed in the login page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If you select <strong>Disable</strong>, then the router name is not displayed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If you do not want to make any changes to the banner, select <strong>No Change</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Banner Text (Optional)</td>
<td>Enter the text that you want displayed in the banner. If you enter the banner text, then this text is displayed instead of the router name in the login page. This is an optional field.</td>
</tr>
<tr>
<td>Authentication Proxy Rule</td>
<td></td>
<td>Action</td>
<td>Select <strong>Enable</strong> or <strong>Disable</strong> an authentication proxy rule.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If you select <strong>Enable</strong>, a named authentication proxy rule is created and associated with access list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If you select <strong>Disable</strong>, the associated proxy rule is removed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Select <strong>No Change</strong> if you do not want to make changes to the Authentication Proxy Rule group of fields.</td>
</tr>
</tbody>
</table>
Chapter 5  Making and Deploying Configuration Changes Using NetConfig

Using System-defined Tasks

Click on Applicable Devices to view the devices in your selection, to which this task applies.

**IOS Devices with VPN Images**

You can determine VPN images from the naming convention used for IOS images. The naming convention follows the `xxxx-yyyy-ww` format.

Where, `xxxx` represents platform, `yyyy` represents features and `ww` represents format. If the middle value (`yyyy`) contains the number `56` or `K`, where `n` is a number between 1 and 9, then this is a VPN image.

For example, `C7100-I56I-M` is a VPN image, since it contains the number `56`.

**Banner Task**

You can use the Banner system-defined, configuration task to change banners on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS

For more details, see Table 5-5.

You can enter the details of this task in the Banner Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Banner Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td>Motd Banner</td>
<td>Action</td>
<td>Select the appropriate option to add or remove a message of the day banner. Select <strong>No Change</strong>, if you are modifying an existing task, and you do not want to change the value in this field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Message</td>
<td>Enter message, if you selected <strong>Add</strong> in Action field.</td>
</tr>
</tbody>
</table>
Using System-defined Tasks

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

**CDP Task**

You can use the CDP system-defined task to configure Cisco Discovery Protocol (CDP) on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine

For more details, see Table 5-5.

You can enter the details of this task in the CDP Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the CDP Configuration dialog box are:
Using System-defined Tasks

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td>Run</td>
<td>Action</td>
<td>Select to enable, disable, or make no change to the CDP state.</td>
</tr>
<tr>
<td>Hold Time</td>
<td></td>
<td>Seconds (10-255)</td>
<td>Enter holdtime in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The CDP holdtime specifies how much time can pass between CDP messages from neighboring devices before the device is no longer considered connected and the neighboring entry is aged out. Value must be greater than value in Update Time field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set to Default</td>
<td>Select this for the default hold time of 60 seconds</td>
</tr>
<tr>
<td>Update Time</td>
<td></td>
<td>Seconds (5-254)</td>
<td>Enter time between CDP updates, in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Value must be less than value in Hold Time field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set to Default</td>
<td>Select this for the default update time of 60 seconds</td>
</tr>
<tr>
<td>CDP Version</td>
<td>Run</td>
<td></td>
<td>Select the CDP Version (CDPv1 or CDPv2. CDP version 2 is the default value. If you are modifying the CDP Task and you do not want to change this field, select No Change.</td>
</tr>
<tr>
<td>IOS Parameters</td>
<td>No category-specific commands.</td>
<td>-</td>
<td>This device category does not have any device-category-specific commands. Use the Common Parameters group to assign the values.</td>
</tr>
<tr>
<td>CatOS Parameters</td>
<td>Mod/Ports</td>
<td>Mod/Ports (Ex:2/1-12,3/5)</td>
<td>Enter modules and ports on which to enable or disable CDP. You can enter a single module and port or a range of ports, for example, 2/1-12,3/5-12.</td>
</tr>
<tr>
<td></td>
<td>All mod/ports</td>
<td></td>
<td>Select to enable or disable CDP in all ports in all modules.</td>
</tr>
<tr>
<td>CDP Format</td>
<td>Forma`t</td>
<td></td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No Change (Does not allow you to make any modifications to the specified CDP format.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• MAC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Select the required option.</td>
</tr>
<tr>
<td>CE Parameters</td>
<td>No category-specific commands.</td>
<td>-</td>
<td>This device category does not have any device-category-specific commands. Use the Common Parameters group to assign the values.</td>
</tr>
</tbody>
</table>
Certification Authority Task

You can use the Certification Authority (CA) system-defined configuration task to provide manageability and scalability for IP Security (IPSec) standards. The Certification Authority task can be used only on IOS devices configured for VPN functionality.

This task is applicable to IOS devices (including Cable devices).

For more details, see Table 5-5.

You can enter the details of this task in the Certification Authority Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For this task to work correctly, you must use a CLI-based protocol (Telnet or SSH) as the download protocol.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Certification Authority Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Parameters</td>
<td>Declare CA</td>
<td>Action</td>
<td>Select <strong>Enable</strong> or <strong>Disable</strong> to activate/deactivate Certification Authority (CA).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If you select <strong>Enable</strong> you can create or modify CA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If you select <strong>Disable</strong>, you can delete the CA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA Name</td>
<td>Enter the CA name. This name is used to identify the certification authority to be configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This name is the CA domain name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value</td>
<td>Enter the URL of the CA. The URL should include any available non-standard cgi-bin script location.</td>
</tr>
<tr>
<td>Enrollment Mode</td>
<td>Action</td>
<td>Enrollment URL</td>
<td>• Select <strong>Enable</strong> to allow router to connect to the CA, using the URL specified in the Value field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Select <strong>Disable</strong>, if you do not want to connect to the CA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Select <strong>No Change</strong> to leave the Enrollment Mode field unchanged.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LDAP Server</td>
<td>Enter the LDAP server of the CA, if your CA system provides a Registration Authority (RA).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Select <strong>Disable</strong> to disable the specified LDAP Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Select <strong>No Change</strong> to leave the Enrollment Mode field unchanged.</td>
</tr>
</tbody>
</table>
### Chapter 5      Making and Deploying Configuration Changes Using NetConfig

#### Using System-defined Tasks

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment Retry</td>
<td>Period</td>
<td>Minutes [1- 60]</td>
<td>Enter the wait period between certification request retries. The wait period is between 1 to 60.</td>
</tr>
<tr>
<td>Enrollment Retry</td>
<td></td>
<td>Set to Default</td>
<td>Select this option to set the default wait period to 1 minute.</td>
</tr>
<tr>
<td>Enrollment Retry</td>
<td>Count</td>
<td>Number [1- 100]</td>
<td>Enter the certification request retry number. The retry number must be between 1 and 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set to Default</td>
<td>Select this option to set the default retry period to 1 minute.</td>
</tr>
<tr>
<td>CRL Optional</td>
<td></td>
<td>Action</td>
<td>Select <strong>Enable</strong> to bypass the Certificate Revocation List. If you select <strong>Disable</strong>, Certificate Revocation list is checked.</td>
</tr>
<tr>
<td>Certificate Query</td>
<td></td>
<td>Action</td>
<td>Select an option to enable, disable or make no change to certificate query.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If you select <strong>Enable</strong>, certificate query will be added to all trust points on the router.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If you select <strong>Disable</strong>, the certificate will not be queried.</td>
</tr>
<tr>
<td>RSA Key pairs</td>
<td></td>
<td>Action</td>
<td>Select an option to generate, delete or make no change to the RSA key pairs. This feature allows you to configure a Cisco IOS router to have multiple key pairs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Thus, the Cisco IOS software can maintain a different key pair for each identity certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key Type</td>
<td>Specify the key type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• General Purpose—To generate a general purpose key pair that is used for both encryption and signature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Usage—To generate separate usage key pairs for encrypting and signing documents.</td>
</tr>
</tbody>
</table>

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

**IOS Devices with VPN Images**

You can determine VPN images from the naming convention used for IOS images. The naming convention follows the `xxxx-yyyy-ww` format.

Where, `xxxx` represents platform, `yyyy` represents features and `ww` represents format. If the middle value (`yyyy`) contains the number 56 or K, where `n` is a number between 1 and 9, then this is a VPN image.

For example, `C7100-IS56I-M` is a VPN image, since it contains the number 56.

**Crypto Map Task**

You can use the Crypto Map Server system-defined task to configure IPSec on devices.

**Note** You must configure the IKE configuration system-defined task (see **Internet Key Exchange (IKE) Configuration Task**) and Transform system-defined task (see **Transform System-Defined Task**) before configuring the Crypto Map system-defined task.
The following device categories are supported by this task:

- IOS (including Cable devices)
- PIX OS

For more details, see Table 5-5.

You can enter the details of this task in the Crypto Map Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Crypto Map Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Parameters</td>
<td>Configuration</td>
<td>Action</td>
<td>Select an option to add, remove, or make no change to the IOS configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Map Name</td>
<td>Enter the name for the Crypto Map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Map Number</td>
<td>Enter the number for the Crypto Map. The value must be between 1 and 65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Map Type</td>
<td>Select the map type (manual or isakmp) for the Crypto Map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Map Description</td>
<td>Enter the description for the Crypto Map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Crypto ACL</td>
<td>Enter the extended access list for Crypto Map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPSec Peer</td>
<td>Enter the IPSec peer to be associated with the Crypto Map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transform Set name</td>
<td>Enter the transform set name to be used with the Crypto Map.</td>
</tr>
<tr>
<td>PIX Parameters</td>
<td>Configuration</td>
<td>Action</td>
<td>Select an option to add, remove, or make no change to the PIX configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Map Name</td>
<td>Enter the name for the Crypto Map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Map Number</td>
<td>Enter the number for the Crypto Map. Value must be between 1 and 65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Map Type</td>
<td>Select the type (manual or isakmp) for the Crypto Map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Crypto ACL</td>
<td>Enter the extended access list for Crypto Map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPSec Peer</td>
<td>Enter the IPSec peer to be associated with the Crypto Map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transform Set name</td>
<td>Enter the transform set name to be used with the Crypto Map.</td>
</tr>
</tbody>
</table>

For each device category, click on Applicable Devices to view the devices in your selection, to which this task applies.
DNS Task

You can use the DNS system-defined task to configure DNS (Domain Name Server) on devices. The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- CSS
- NAM
- PIX OS

For more details, see Table 5-5.

You can enter the details of this task in the DNS Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the DNS Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td>DNS Server</td>
<td>Add</td>
<td>Enter the IP addresses of DNS name server(s) that you want to add. Separate multiple addresses with commas. If the device accepts only one DNS server, then the first address will be considered.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remove</td>
<td>Enter the IP addresses of DNS name server(s) that you want to remove. Separate multiple addresses with commas.</td>
</tr>
<tr>
<td></td>
<td>Domain Name</td>
<td>Name</td>
<td>Enter the domain names to complete unqualified hostnames. If a device has a domain list enabled, it will be used to complete unqualified hostnames instead of the domain name. Separate multiple addresses with commas. If the device accepts only one domain name, then the first entry will be considered.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remove</td>
<td>Select this option to remove the domain names.</td>
</tr>
<tr>
<td>IOS Parameters</td>
<td>Domain Lookup</td>
<td>Select to enable or disable IP DNS-based hostname-to-address translation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CLNS NSAP</td>
<td>Select to enable or disable or make no change to the CLNS NSAP option. If this option is enabled, any packet with the specified CLNS NSAP prefix causes CLNS (Connectionless Network Service) protocol to behave as if no route were found.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OSPF</td>
<td>Select to enable or disable or make no change to the OSPF (Open Shortest Path First) protocol option.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Domain List</td>
<td>Action</td>
<td>Select an option to add, remove, or make no change to the domain list.</td>
</tr>
</tbody>
</table>
## Using System-defined Tasks

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

### Enable Password Task

You can use the Enable Password system-defined, configuration task to change the enable and secret passwords, which allow users to enter the enable mode on devices.

When you enable or disable an enable password, the change is made on the device and in Device and Credential Repository.

**Note**

If you disable the enable password on a device, you cannot enter the enable mode on that device unless you previously enabled an alternative type of enable mode authentication.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- PIX OS

For more details, see Table 5-5.

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CatOS Parameters</td>
<td>1st Server Primary</td>
<td>Domain List</td>
<td>Enter domain names to complete unqualified hostnames, or add to the existing list. Separate multiple domain names with commas. Do not include an initial period before domain names.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Domain Lookup</td>
<td>Select an option to enable, disable, or make no change to the domain lookup.</td>
</tr>
<tr>
<td>Content Engine Parameters</td>
<td>Serial Lookup</td>
<td>Select an option to enable, disable, or make no change to the serial lookup.</td>
<td></td>
</tr>
<tr>
<td>CSS Parameters</td>
<td>Secondary DNS Server</td>
<td>Add (Hostname or IP Address)</td>
<td>Enter the hostname or an IP address of a secondary server, that you want to add. A maximum of two IP addresses are allowed. The order in which you enter them is the order in which they are used if the primary DNS server fails. Separate multiple addresses with a comma.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remove (Hostname or IP Address)</td>
<td>Enter a hostname or an IP address of a secondary server, that you want to remove. A maximum of two IP addresses are allowed. Separate multiple addresses with a comma.</td>
</tr>
<tr>
<td>NAM Parameters</td>
<td>Disable Nameservers</td>
<td>Select to disable domain name servers.</td>
<td></td>
</tr>
</tbody>
</table>
You can enter the details of this task in the Enable Password Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

---

**Note**
If you change the enable password on a Catalyst device with an RSM module using this task, the RSM enable password is also changed.
The fields in the Enable Password Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td>Setup</td>
<td>Action</td>
<td>Select an option to enable, disable or make no change to the enable password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password</td>
<td>Enter the enable password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify</td>
<td>Re-enter the password.</td>
</tr>
<tr>
<td>IOS Parameters</td>
<td>Password</td>
<td>Level (1-15)</td>
<td>Set the Enable Password level. The level can be between 1 and 15. 15 is the default level. For an IOS device, it is advisable not to disable both Enable Password and Enable Secret password. This is because the IOS device will not allow you to go into the Enable mode of the device. You can do this only if you have the console password for the device. If you have selected Enable Password as <strong>No Change</strong> in the Common Parameters pane, and selected Disable for Enable Secret in the IOS Parameters pane, then Enable Secret Password is updated in the Device and Credentials database. If you have selected Enable Password as <strong>Disable</strong> in the Common Parameters pane, and selected <strong>No Change</strong> for Enable Secret in the IOS Parameters pane, then Enable Password is updated in the Device and Credentials database.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encrypted</td>
<td>Select this option to encrypt the password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update Credentials</td>
<td>Select this to update credentials. For details see <a href="#">Understanding the NetConfig Credentials Configuration Tasks</a>.</td>
</tr>
<tr>
<td>Secret</td>
<td>Action</td>
<td>Secret</td>
<td>Select an option to enable, disable or make no change to the secret password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secret</td>
<td>Enter the secret password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify</td>
<td>Re-enter the password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Level (1-15)</td>
<td>Set the password level. The level can be between 1 and 15. 15 is the default level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encrypted</td>
<td>Select this option to encrypt the password.</td>
</tr>
<tr>
<td>CatOS Parameters</td>
<td>Password</td>
<td>Apply Command on Modules</td>
<td>Select to apply the command on the modules. If you have selected <strong>Disable</strong> as the action in the Common Parameters group, then the password will be removed.</td>
</tr>
</tbody>
</table>
For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

### HTTP Server Task

You can use HTTP Server to configure HTTP access on IOS devices, which have been configured for VPN functionality.

The following device categories are supported by this task:
- IOS (including Cable devices)
- Catalyst OS

For more details, see Table 5-5.

You can enter the details of this task in the HTTP Server Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the HTTP Server Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIX Parameters</td>
<td></td>
<td>Level(0-15)</td>
<td>Set the password level. The level can be between 0 and 15. 15 is the default level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encrypted (Password should be 16 characters)</td>
<td>Select this option if the password you are entering is already encrypted. If you select this option ensure that your password is 16 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td>Server</td>
<td>Action</td>
<td>Select an option to enable, disable or make no change to the HTTP access on the device.</td>
</tr>
<tr>
<td>Port</td>
<td></td>
<td>Number [0-65535]</td>
<td>Specify the HTTP server port number.</td>
</tr>
<tr>
<td>IOS Parameters</td>
<td>Authentication</td>
<td>Action</td>
<td>Select an option to enable, disable or make no change to the authentication method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Method</td>
<td>Select an authentication method:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- AAA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- TACACS</td>
</tr>
<tr>
<td>Access List</td>
<td>Action</td>
<td></td>
<td>Select an option to enable, disable or make no change to the access list.</td>
</tr>
</tbody>
</table>
Chapter 5  Making and Deploying Configuration Changes Using NetConfig

Using System-defined Tasks

For each device category, click on Applicable Devices to view the devices in your selection, to which this task applies.

You will lose Telnet access to the device if you configure HTTP Server. The Device may require TACACS/RADIUS/Local username and password after configuring HTTP Server. You should make sure that the device has the appropriate login configured. The username and password has to be stored in the LMS Database.

IOS Devices with VPN Images

You can determine VPN images from the naming convention used for IOS images. The naming convention follows xxxx-yyyy-ww format.

Where, xxxx represents platform, yyyy represents features and ww represents format. If the middle value (yyyy) contains, the number 56 or kn, where n is a number between 1 and 9, then this is a VPN image.

For example, C7100-IS56I-M is a VPN image, since it contains the number 56.

Local Username Task

You can use the Local Username system-defined task configure local username and password authentication on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- CSS

For more details, see Table 5-5.

You can enter the details of this task in the Local Username Task Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Local Username Task Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td>Local User Setup</td>
<td>Action</td>
<td>Select an option to add, remove or make no change to the local username setup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Username</td>
<td>Enter the local username.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password</td>
<td>Enter local username password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify</td>
<td>Re-enter the password.</td>
</tr>
</tbody>
</table>
### Using System-defined Tasks

#### IOS Parameters
**Group:** Local User Setup  
**Field:** Privilege Level [0-15]  
**Description:** Set the required privilege level.

#### Local User Setup
**Field:** Privilege Level [0-15]  
**Description:** Set the required privilege level.

**Field:** No HangUp  
**Description:** Select this option to enable No Hang Up mode.

**Field:** No Escape  
**Description:** Select this option to enable No Escape mode.

#### Local User Login Authentication
**Field:** Action  
**Description:** Select to enable, disable or make no change to the local user authentication group of fields.

#### Local Username Credentials
**Field:** Username  
**Description:** Values are entered in Device and Credential Repository only. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.

**Field:** Password  
**Description:** Values are entered in Device and Credential Repository only. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.

**Field:** Verify  
**Description:** Values are entered in Device and Credential Repository only. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.

#### CSS Parameters
**Description:** For CSS devices:
- The username length should be between 1 and 16 characters.
- The local password length should be between 6 and 16 characters.
- The DES-Encrypted password length should be between 6 and 64 characters.

#### Local User Setup
**Field:** SuperUser  
**Description:** Select this option to designate the local user as superuser.

**Field:** Password Type  
**Description:** Select the password type from these options:
- Local
- Encrypted
- DES_Encrypted

#### Directory Access
**Field:** Configure Directory Access  
**Description:** Select this option if you want to configure directory access. Defines the CSS directory access levels. By default, CSS assigns users with read and write access to the directories. Changing the access level also affects the use of the CLI commands associated with the directories.

**Field:** Directories  
**Description:** Select the required access option to the Script directory:
- No Access
- Read And Write
- Read
- Write
### Using System-defined Tasks

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Log            |           | Select the required access option to the Log directory: | • No Access  
|                |           |                | • Read And Write  
|                |           |                | • Read  
|                |           |                | • Write  |
| Root           |           | Select the required access option to the Root directory: | • No Access  
|                |           |                | • Read And Write  
|                |           |                | • Read  
|                |           |                | • Write  |
| Archive        |           | Select the required access option to the Archive directory: | • No Access  
|                |           |                | • Read And Write  
|                |           |                | • Read  
|                |           |                | • Write  |
| Release Root   |           | Select the required access option to the Release Root directory: | • No Access  
|                |           |                | • Read And Write  
|                |           |                | • Read  
|                |           |                | • Write  |
| Core           |           | Select the required access option to the Core directory: | • No Access  
|                |           |                | • Read And Write  
|                |           |                | • Read  
|                |           |                | • Write  |
| MIB            |           | Select the required access option to the MIB directory: | • No Access  
|                |           |                | • Read And Write  
|                |           |                | • Read  
|                |           |                | • Write  |
IGMP Configuration Task

You can use this task to configure the Internet Group Management Protocol (IGMP) on a cable interface.

**Note**  You can apply this task only on a single IOS device at a time. For details, see Table 5-5.

You can enter the details of this task in the IGMP Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the IGMP Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Parameters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP Configuration</td>
<td>Interface</td>
<td>Interfaces</td>
<td>Select the required option to specify the interface to be configured for IGMP, or to make no change to the existing interface selection:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Not Selected</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• FastEthernet0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• FastEthernet0/1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Cable1/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Action</td>
<td>Select the required option to enable, disable, or make no change to the Interface sub-group of fields.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PIM Mode</td>
<td>Select the required PIM mode option. Select <strong>No Change</strong> to retain any previous mode selection:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No Change</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• dense-mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• sparse-mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• sparse-dense-mode</td>
</tr>
<tr>
<td>IGMP Parameters</td>
<td>Action</td>
<td></td>
<td>Select the required option to replace the values in, or to make no change to the IGMP Parameters group of fields.</td>
</tr>
<tr>
<td></td>
<td>IGMP Version</td>
<td></td>
<td>Select the required IGMP version from the supported versions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 3</td>
</tr>
<tr>
<td></td>
<td>Last Memory Query Interval [100-25500 in msec]</td>
<td>Enter the time interval between the IGMP specific messages sent by the router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enter the last memory query interval in seconds. You can enter an interval between 100 and 25500 milliseconds. The default is 1000 milliseconds.</td>
</tr>
</tbody>
</table>
Click on Applicable Devices to view the devices in your selection, to which this task applies.

Interface IP Address Configuration Task

You can use this task to configure the IP address of a cable interface.

You can apply this task only on a single IOS device at a time. For details, see Table 5-5.

You can enter the details of this task in the Interface IP Address Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)
Using System-defined Tasks

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Interface IP Address Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cable Parameters             | Interface IP       | Cable Interface | Select the required cable interface for configuring the IP address, or select **Not Selected** to make no change to the previous selection:  
- Not Selected  
- FastEthernet0/0  
- FastEthernet0/1  
- Cable1/0 |
|                              | Configuration      | Action      | Select the following action:  
- No Change—Makes no change to the IP Addresses  
- Replace—Replaces the IP Addresses  
- Remove Primary—Removes the primary IP Address.  
- Remove Secondary—Removes the secondary IP Address.  
- Remove All—Removes both primary and secondary IP Addresses. |
|                              |                    | IPAddress   | Enter the primary IP address.                                               |
|                              |                    | Secondary   | Enter the secondary IP address.                                             |
|                              |                    | Subnet Mask | Enter the primary subnet mask.                                              |
|                              |                    | Secondary   | Enter the secondary subnet mask.                                            |

**Note**  
The values for interfaces are as returned by device.

Click on **Applicable Devices** to view the devices in your selection, to which this task applies.

**Internet Key Exchange (IKE) Configuration Task**

Use the Internet Key Exchange (IKE) Configuration System task to configure IPSec on devices.  
The following device categories are supported by this task:  
- IOS (including Cable devices)  
- PIX OS

For more details, see Table 5-5.

You can enter the details of this task in the IKE Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)
For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Parameters</td>
<td>Action</td>
<td>Select to enable, disable, or make no change to ISAKMP.</td>
<td></td>
</tr>
<tr>
<td>ISAKMP Policy</td>
<td>ISAKMP Policy Priority</td>
<td>Action</td>
<td>Select to add, remove, or make no change to ISAKMP policy priority.</td>
</tr>
<tr>
<td></td>
<td>Priority</td>
<td>Enter the policy priority number</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value must be between 1 and 10000.</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Action</td>
<td>Select to enable, disable, or make no change to encryption type.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Select the type of encryption for the policy:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3des</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• des</td>
<td></td>
</tr>
<tr>
<td>Hash</td>
<td>Action</td>
<td>Select to enable, disable, or make no change to the hash algorithm.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Algorithm</td>
<td>Select the type of hash algorithm:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sha</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• md5</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>Action</td>
<td>Select to enable, disable, or make no change to the authentication method.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Method</td>
<td>Select the type of authentication method:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• rsa-sig</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• rsa-encr</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• pre-share</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>Action</td>
<td>Select to enable, disable, or make no change to the Diffie-Hellman group identifier.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Value</td>
<td>Enter the Diffie-Hellman group identifier.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value must be 1 or 2.</td>
<td></td>
</tr>
<tr>
<td>Lifetime</td>
<td>Action</td>
<td>Select to enable, disable, or make no change to the lifetime value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Seconds</td>
<td>Enter the lifetime value in seconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value must be between 60 and 86400 seconds.</td>
<td></td>
</tr>
<tr>
<td>PIX Parameters</td>
<td>Action</td>
<td>Select to enable, disable, or make no change to ISAKMP.</td>
<td></td>
</tr>
<tr>
<td>ISAKMP Policy</td>
<td>Interface</td>
<td>Select the interface:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inside</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Outside</td>
<td></td>
</tr>
<tr>
<td>ISAKMP Policy</td>
<td>ISAKMP Policy Priority</td>
<td>Action</td>
<td>Select to add, remove, or make no change to ISAKMP policy priority.</td>
</tr>
</tbody>
</table>
For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

### NTP Server Configuration Task

You can use the NTP Server system-defined task to configure Network Time Protocol (NTP) on devices. The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- CSS
- CE

For more details, see Table 5-5.
You can enter the details of this task in the NTP Server Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td>NTP Server</td>
<td>Action</td>
<td>Select to add, remove, or make no change to Network Time Protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Host Name/IP Address</td>
<td>Enter the IP address of the NTP server to which devices will send time-of-day requests.</td>
</tr>
<tr>
<td>IOS Parameters</td>
<td>NTP Server</td>
<td>Server Type</td>
<td>Select the required server type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Version</td>
<td>Select the server version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server Key (0-4294967295)</td>
<td>Enter the NTP server Key. The value must be between 0 and 4294967295.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify Server Key</td>
<td>Re-enter the Key to confirm.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source Interface (Interface Name)</td>
<td>Enter the source interface name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Preferred</td>
<td>Select an option to specify whether the interface is a preferred interface.</td>
</tr>
<tr>
<td></td>
<td>NTP Authentication Key</td>
<td>Action</td>
<td>Select to add, remove, or make no change to the NTP authentication Key.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number [1 to 4294967295]</td>
<td>Enter the number of Key bits. The value must be between 1 and 4294967295 Key bits.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify Number</td>
<td>Re-enter the number to confirm.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MD5 Number (Max 8 chars)</td>
<td>Enter the MD5 number which can contain a maximum of 8 characters.</td>
</tr>
<tr>
<td></td>
<td>NTP Authentication</td>
<td>NTP Authentication</td>
<td>Select to enable, disable, or make no change to NTP authentication.</td>
</tr>
<tr>
<td></td>
<td>NTP Calendar</td>
<td>Action</td>
<td>Select to add, remove, or make no change to the NTP calendar.</td>
</tr>
<tr>
<td></td>
<td>NTP Access Group</td>
<td>Action</td>
<td>Select to add, remove, or make no change to the NTP access group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Type</td>
<td>Select the required action type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• QueryOnly</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ServeOnly</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Serve</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Peer</td>
</tr>
<tr>
<td></td>
<td>NTP Trusted Key</td>
<td>Action</td>
<td>Select to add, remove, or make no change to the NTP trusted Key.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACL Number [1-99]</td>
<td>Enter the ACL number which should be a value between 1 and 99.</td>
</tr>
</tbody>
</table>
RADIUS Server Configuration Task

You can use the RADIUS system-defined task to configure RADIUS on devices. The following device categories are supported by this task:

- IOS (including Cable devices)
- CSS
- CE

For more details, see Table 5-5.

You can enter the details of this task in the RADIUS Server Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).
### Using System-defined Tasks

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Configuration</td>
<td>Action</td>
<td>Select to enable, disable, or make no change to the server configuration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server Name</td>
<td>Enter the server name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Auth Port</td>
<td>Enter port used for authentication by RADIUS server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Key</td>
<td>Enter RADIUS authentication and encryption key string used by server specified in Host area.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify</td>
<td>Re-enter RADIUS key.</td>
<td></td>
</tr>
<tr>
<td>Login Authentication</td>
<td>Action</td>
<td>Select to enable, disable, or make no change to the login authentication. The Login Authentication is not applicable for CSS RADIUS Credentials</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Username</td>
<td>Enter the username. For details see Understanding the NetConfig Credentials Configuration Tasks. In case of CSS devices, this value will be used to update the Primary login details.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>Enter the password. For details see Understanding the NetConfig Credentials Configuration Tasks. In case of CSS devices, this value will be used to update the Primary login details.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify</td>
<td>Re-enter the password to verify. For details see Understanding the NetConfig Credentials Configuration Tasks. In case of CSS devices, this value will be used to update the Primary login details.</td>
<td></td>
</tr>
<tr>
<td>IOS Parameters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login Authentication</td>
<td>List</td>
<td>Enter default or named list.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set to Default</td>
<td>Select to set the default list.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Options (Drop-down list) Select the required option:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No Choice</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• radius</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• tacacs+</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• line</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• local</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• none</td>
<td></td>
</tr>
</tbody>
</table>

Similarly, select the type from the other three drop-down lists.
### Using System-defined Tasks

#### New Model

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Select to enable, disable, or make no change to new model state.</td>
</tr>
</tbody>
</table>

#### Enable mode Authentication

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Select to add, remove, or make no change to the enable mode authentication.</td>
</tr>
</tbody>
</table>

#### Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the enable username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the enable password.</td>
</tr>
<tr>
<td>Verify</td>
<td>Re-enter the enable password.</td>
</tr>
</tbody>
</table>

#### Type

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>Select the required option:</td>
</tr>
</tbody>
</table>
| (Drop-down list 1) |   - No Choice  
|              |   - radius  
|              |   - tacacs+  
|              |   - line  
|              |   - enable  
|              |   - local  
|              |   - none  

Similarly, select the type from the other three drop-down lists.

#### Content Engine Parameters

No category-specific commands.

#### CSS Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Select to enable, disable, or make no change to the host configuration.</td>
</tr>
</tbody>
</table>

#### Secondary Server Name (Host Name or IP Address)

Enter the secondary server hostname or IP address.

#### Secondary Server Key

Enter the key for the secondary server. Defines the secret string for authentication transactions between the RADIUS server and the CSS. Enter a case-sensitive string with a maximum of 16 characters.

#### Authentication Port (1-65535)

Enter custom authentication port of the RADIUS server. Value must be between 0 and 65535.

Optional field. Defines the UDP port on the secondary RADIUS server that receives authentication packets from clients. Enter a number from 0 to 65535. The default is 1645.

#### Other Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dead Time in seconds (1-255)</td>
<td>Enter the dead time in seconds. The value must be between 0 and 255.</td>
</tr>
<tr>
<td></td>
<td>Enter a number from 0 to 255. The default is 5.</td>
</tr>
<tr>
<td></td>
<td>If you enter 0, the dead time is disabled and the CSS does not send probe access-request packets to the non-responsive server. This command applies to primary and secondary servers.</td>
</tr>
</tbody>
</table>

Remove Select to remove the dead time specification. Use the no form of this command to reset the dead-time period to its default of 5 seconds.
For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

### RCP Configuration Task

You can use the RCP system-defined configuration task to configure RCP on devices.

This task supports the IOS category of devices including Cable devices.

For more details, see Table 5-5.

You can enter the details of this task in the RCP Configuration dialog box. (To invoke this dialog box, see **Starting a New NetConfig Job**.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see **Understanding the System-defined Task User Interface (Dialog Box)**

The fields in the RCP Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Parameters</td>
<td>Enable</td>
<td>Action</td>
<td>Select to enable or disable rcp state. To make rcp setup changes without enabling or disabling rcp, select <strong>No Change</strong>.</td>
</tr>
<tr>
<td>RCP User Setup</td>
<td>Action</td>
<td></td>
<td>Select the required option to add to, or to remove current user from rcp authentication list. To make rcp setup changes without enabling or disabling rcp, select <strong>No Change</strong>.</td>
</tr>
<tr>
<td>Local Username</td>
<td>Enter</td>
<td></td>
<td>Enter local name of user whose rcp access you are modifying.</td>
</tr>
<tr>
<td>Remote Host</td>
<td>Enter</td>
<td></td>
<td>Enter IP address of remote host from which local device will accept remotely executed commands.</td>
</tr>
</tbody>
</table>
For each device category, click on Applicable Devices to view the devices in your selection, to which this task applies.

### Reload Task

You can use the Reload task to schedule reload of devices. This task supports the IOS, Cat OS, SFS, NAM, CE, FastSwitch, PIX, CSS and Cable categories of devices. For more details, see Table 5-5.

You can enter the details of this task in the Reload Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box)

The fields in the Reload Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td>Reload</td>
<td>Action</td>
<td>Select either:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>Reload</strong> to enable reloading selected devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>No Change</strong> if you do not want to schedule a reload for the selected devices.</td>
</tr>
<tr>
<td>IOS Parameters</td>
<td>Do not Save config before reload</td>
<td>Action</td>
<td>You can:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Check this option if you do not want to save the configurations before reloading.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Uncheck this option if you want to save the configurations before reloading.</td>
</tr>
<tr>
<td>CatOS Parameters</td>
<td></td>
<td></td>
<td>No category-specific parameters.</td>
</tr>
<tr>
<td>CE Parameters</td>
<td>Do not Save config before reload</td>
<td>Action</td>
<td>You can:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Check this option if you do not want to save the configurations before reloading.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Uncheck this option if you want to save the configurations before reloading.</td>
</tr>
</tbody>
</table>
### Using System-defined Tasks

For each device category, click on **Applicable Devices** to view the devices in your selection, to which the reload task applies.

#### SNMP Community Configuration Task

You can use the SNMP Community Configuration system-defined task to replace, add, and remove device SNMP community strings.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- CSS
- NAM
- PIX OS

For more details, see *Table 5-5*.

You can enter the details of this task in the SNMP Community Configuration dialog box. (To invoke this dialog box, see *Starting a New NetConfig Job*.)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Do not Save config before reload</th>
<th>Action</th>
<th>You can:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAM Parameters</td>
<td>Do not Save config before reload</td>
<td>Action</td>
<td>- Check this option if you do not want to save the configurations before reloading.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Uncheck this option if you want to save the configurations before reloading.</td>
</tr>
<tr>
<td>SFS Parameters</td>
<td></td>
<td>No category-specific parameters.</td>
<td></td>
</tr>
<tr>
<td>Fast Switch parameters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIX Parameters</td>
<td>Do not Save config before reload</td>
<td>Action</td>
<td>- Check this option if you do not want to save the configurations before reloading.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Uncheck this option if you want to save the configurations before reloading.</td>
</tr>
<tr>
<td>CSS Parameters</td>
<td></td>
<td>No category-specific parameters.</td>
<td></td>
</tr>
<tr>
<td>Cable Parameters</td>
<td>Do not Save config before reload</td>
<td>Action</td>
<td>- Check this option if you do not want to save the configurations before reloading.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Uncheck this option if you want to save the configurations before reloading.</td>
</tr>
</tbody>
</table>
For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the SNMP Community Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td>Read-only</td>
<td>Action</td>
<td>Select an option to replace, add, remove, or make no change to a read-only SNMP community string.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If you select <strong>Replace</strong>, the new community string replaces the corresponding community string in the Device and Credential Repository (DCR). This action also deletes the current SNMP credentials on the device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If you select the <strong>Add</strong> or <strong>Remove</strong> option, the new SNMP community strings are configured in the device alone and DCR is untouched.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Community</td>
<td>Enter the community string.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>String</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify</td>
<td>Re-enter the community string.</td>
</tr>
<tr>
<td></td>
<td>Read-write</td>
<td>Action</td>
<td>Select an option to replace, add, remove, or make no change to a read-write SNMP community string.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If you select <strong>Replace</strong>, the new community string replaces the corresponding community string in the Device and Credential Repository.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If you select <strong>Add</strong> or <strong>Remove</strong>, the new SNMP community strings are configured in the device alone and DCR is untouched.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Community</td>
<td>Enter the community string.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>String</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify</td>
<td>Re-enter the community string.</td>
</tr>
<tr>
<td>IOS Parameters</td>
<td>Setup View</td>
<td>MIB View</td>
<td>Enter name of a previously defined view that defines objects available to community.</td>
</tr>
<tr>
<td></td>
<td>(Optional)</td>
<td>(Optional)</td>
<td>Optional field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OID -Tree</td>
<td>Indicates the Object Identifier of ASN.1 subtree that is to be included or excluded from the view.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To identify an Object Identifier ASN.1 subtree, enter a numerical string such as 1.3.6.2.4 or a word such as system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To identify a subtree family, enter a wildcard, for example an asterisk (<em>), where the string will read 1.3.</em>.4.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enter the MIB OID-Tree name.</td>
</tr>
</tbody>
</table>
**SNMP Security Configuration Task**

You can use this task to configure the SNMP Security feature on the following device categories:

- IOS (including Cable devices)
- Content Engine

For more details, see Table 5-5.

You can enter the details of this task in the SNMP Security Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Type</td>
<td>Include or exclude all the objects specified in the MIB OID subtree you identified in the previous field. Select <strong>Included</strong> or <strong>Excluded</strong> from the drop down list.</td>
</tr>
<tr>
<td></td>
<td>Access List (Optional)</td>
<td>Access List (Optional)</td>
<td>Enter an integer from 1 to 99 to specify a named or numbered access list of IP addresses that are allowed to use the community string to access SNMP agent. Optional field.</td>
</tr>
<tr>
<td>CatOS</td>
<td>Parameters</td>
<td></td>
<td>No category-specific parameters.</td>
</tr>
<tr>
<td>CE</td>
<td>Parameters</td>
<td></td>
<td>No category-specific parameters.</td>
</tr>
<tr>
<td>PIX</td>
<td>Parameters</td>
<td></td>
<td>No category-specific parameters.</td>
</tr>
<tr>
<td>CSS</td>
<td>Parameters</td>
<td></td>
<td>No category-specific parameters.</td>
</tr>
<tr>
<td>NAM</td>
<td>Parameters</td>
<td></td>
<td>No category-specific parameters.</td>
</tr>
</tbody>
</table>

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.
The fields in the SNMP Security Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td></td>
<td>Action</td>
<td>Select an option, to add, remove, or make no change to the common parameters.</td>
</tr>
<tr>
<td>(Drop-down list)</td>
<td></td>
<td>(Drop-down list)</td>
<td>Select the required option for SNMP Groups/Users:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Group &amp; Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group Name</td>
<td>Enter the group name. Indicates the SNMP Group in the SNMP protocol context.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNMP Versions</td>
<td>Select the SNMP version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SNMP version 1 and version 2 have No Auth and No Privacy. Version 3 has all levels of security.</td>
</tr>
<tr>
<td>Users *</td>
<td></td>
<td>User Names</td>
<td>• Username—Indicates the name of the user in the SNMPv3 protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authen Pswds</td>
<td>• Authenticating Passwords—Indicates that the user is part of the group that is assigned Auth No Privacy or Auth Privacy security level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authen Algorithm</td>
<td>• Authenticating Algorithm—Indicates the authenticating algorithm is assigned to a group with Auth No Privacy or Auth Privacy security levels.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy Paswds</td>
<td>• Privacy passwords—Indicates user is part of a group assigned Auth Privacy level of security.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>You can specify up to five usernames, for which you can enter authentication passwords, select the authentication algorithm, and specify the privacy passwords.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Config Access Control</td>
<td>This section allows you to configure access options for an SNMP group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[optional]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read View</td>
<td>Specify the read view. This view is for users assigned to a specified group. Indicates an alphanumeric label, not exceeding 64 characters, for the SNMP view entry you are creating or updating.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Write View</td>
<td>Specify the write view. Allows all users in the specified group to add, modify, or create a configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Notify View</td>
<td>Specify the notify view. This view notifies all the users in the specified group.</td>
</tr>
<tr>
<td>IOS Parameters</td>
<td></td>
<td>Access Control</td>
<td>Enter the number of an Access List (1 and 99).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[optional]</td>
<td></td>
</tr>
</tbody>
</table>
The SNMP Security template enables you to configure Groups as well as Users with certain privileges. These Groups can be rolled back but the Users cannot be rolled back. This is because the User details will not be available in the running configuration. Since NetConfig uses the running config to do roll back, rolling back Users is not possible. You should run a separate job to remove or add Users as required.

For each device category, click on **Applicable Devices** to view the devices in your selection.

### SNMP Traps Configuration Task

You can use this task to configure the host, trap notification, and trap/inform parameters. You can specify security parameters to communicate securely with the SNMP host. See **SNMP Security Configuration Task** to configure the SNMP security.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- CSS
- NAM

For more details, see Table 5-5.

You can enter the details of this task in the SNMP Traps Configuration dialog box. (To invoke this dialog box, see **Starting a New NetConfig Job**.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see **Understanding the System-defined Task User Interface (Dialog Box)**.
The fields in the SNMP Traps Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td>Traps Notification</td>
<td>Action</td>
<td>Select to enable, disable, or make no change to the traps notification configuration. If you select <strong>Enable</strong>, the server will receive SNMP traps. If you select <strong>Disable</strong>, the server will not receive any SNMP traps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iOS Parameters</td>
<td>Type</td>
<td>Environmental</td>
<td>Select to send only environmental traps to the host.</td>
</tr>
<tr>
<td>Traps Notification Options</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Configuration</td>
<td>Action</td>
<td></td>
<td>Select to add, remove, or make no change to the host configuration.</td>
</tr>
<tr>
<td></td>
<td>Username</td>
<td></td>
<td>Specifies the user name that is used for authentication. This field is available when No Authentication, Authentication or Privacy are selected.</td>
</tr>
<tr>
<td></td>
<td>Host</td>
<td></td>
<td>Enter the hostname or IP address.</td>
</tr>
<tr>
<td>SNMP Security</td>
<td></td>
<td></td>
<td>Select the SNMP security method:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• SecureV2c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NoAuthenticationV3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• AuthenticationV3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• PrivacyV3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• None</td>
</tr>
<tr>
<td>Notification Type</td>
<td></td>
<td></td>
<td>Select the notification type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Trap</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Inform</td>
</tr>
<tr>
<td>UDP Port [0-65535]</td>
<td></td>
<td></td>
<td>Indicates the port that will receive the SNMP requests. The range for a valid port number between 0 and 65535. The default is 162.</td>
</tr>
<tr>
<td>Community String</td>
<td>String</td>
<td></td>
<td>Enter the community string.</td>
</tr>
<tr>
<td>Verify</td>
<td></td>
<td></td>
<td>Re-enter the community string to confirm.</td>
</tr>
<tr>
<td>Direct Traps To Host</td>
<td>Environmental</td>
<td></td>
<td>Select to send only environmental traps to the host.</td>
</tr>
<tr>
<td>SNMP</td>
<td></td>
<td></td>
<td>Select to send the SNMP traps to the host.</td>
</tr>
<tr>
<td>Trap/Inform Configuration</td>
<td>Traps Message</td>
<td>Action</td>
<td>Select to change, replace, disable or make no change to the trap configuration.</td>
</tr>
<tr>
<td>Trap Timeout [1-1000 s]:</td>
<td></td>
<td></td>
<td>Specify the trap timeout value. This value must be between 1 and 1000 seconds.</td>
</tr>
</tbody>
</table>
## Chapter 5  Making and Deploying Configuration Changes Using NetConfig

### Using System-defined Tasks

#### Trap Queue Length [1-1000 events]:
Specify the trap queue length. The number of events that you specify must be between 1 and 1000.

#### Inform Request
- **Action**: Select to replace, disable, or make no change to the inform request.

#### Trap Queue Length [1-1000 events]:
- **Inform Retries [0-100]**: Enter the inform retries. The value should be between 0 and 100.
- **Inform Timeout [0-4294967295]**: Specify the inform timeout value. This value must be between 0 and 4294967295.
- **Inform Pending [0-4294967295]**: Specify the inform pending value. This value must be between 0 and 4294967295.

### CatOS Parameters
- **Host Configuration**
  - **Action**: Select to add, remove, or make no change to the host configuration.
  - **Host**: Enter the hostname or IP address.
  - **Community String**: Enter the community string.
  - **Verify**: Re-enter the community string to confirm.

### ContentEngine Parameters
- **Host Configuration**
  - **Action**: Select to add, remove, or make no change to the host configuration.
  - **Host**: Enter the hostname or IP address.
  - **Community String**: Enter the community string.
  - **Verify**: Re-enter the community string to confirm.

### PIX Parameters
- **Host Configuration**
  - **Action**: Select to add, remove, or make no change to the host configuration.
  - **Host**: Specify an IP address of the SNMP management station to which traps should be sent and/or from which the SNMP requests come. You can specify up to five SNMP management stations.
  - **Interface**: Select the interface:
    - Inside [default]
    - Outside
  - **Notification Type**: Select the notification type:
    - Trap & Poll [default]—Allows both traps and polls to be acted upon.
    - Trap—Only traps will be sent. This host will not be allowed to poll.
    - Poll—Traps will not be sent. This host will be allowed to poll.
<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSS Parameters</td>
<td></td>
<td>Action</td>
<td>Select to add, remove, or make no change to the parameters such as host name or IP address, trap community, source IP address in traps, specific host, trap type, and event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Host Name or IP Address</td>
<td>Enter the hostname or IP address of an SNMP host that has been configured to receive traps. A maximum of 5 hosts can be configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trap Community</td>
<td>Enter the trap community string/name to be used when sending traps to the specified SNMP host. Enter an unquoted text string with no spaces and with maximum length of 12 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify</td>
<td>Re-enter the trap community string to confirm.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source IP Address in Traps</td>
<td>Select the source IP address in traps. To set the source IP address in the traps generated by CSS select one of these options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Egress Port—Obtains the source IP address for the SNMP traps from the VLAN circuit IP address configured on the egress port used to send the trap. You do not need to enter an IP address because the address is determined dynamically by the CSS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Management—Places the management port IP address in the source IP field of the trap. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Specific Host—Allows the user to enter the IP address to be used in the, source IP field of the traps. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) in the Specific Host field (the next field).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No Change (No change will be made to the source IP address if you select this option.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specific Host</td>
<td>In the previous field, that is, Source IP Address in Traps, if you have selected the Specific Host option, then specify the IP Address of the specific host in this field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trap Type</td>
<td>Select the trap type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No Change (No change will be made to the trap type if you select this option).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Enterprise—When you use this keyword alone, it enables enterprise traps. You must enable enterprise traps before you configure an enterprise trap option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Generic—The generic SNMP traps consist of cold start, warm start, link down, and link up.</td>
</tr>
</tbody>
</table>
### Using System-defined Tasks

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

#### Smart Call Home Task

You can use the Smart Call Home task to configure the LMS managed Cisco Catalyst 6500 devices with the Call Home feature.

You can enter the details for this task in the Smart Call Home Configuration dialog box. To invoke this dialog box, see **Starting a New NetConfig Job**.

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td></td>
<td></td>
<td>Select the event:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Module Transition</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Power Supply Transition</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Illegal Packet DOS attack</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• LAND DOS attack</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Smurf DOS attack</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• SYN DOS attack</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Lifetick message failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Login Failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• System reload</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Reporter state transitions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Service transition</td>
</tr>
</tbody>
</table>

#### NAM Syslog Host Configuration Parameters

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select to add, remove, or make no change to the syslog host configuration.</td>
</tr>
</tbody>
</table>

| Index[1-65535] | Enter the syslog host index. The value should be between 1 and 65535.         |
| Host IP Address | Enter the host name or IP address.                                              |
| Community String | Enter the community string.                                                   |
| Verify | Verify the community string.                                                 |
| UDP Port[1-65535] | Enter the UDP port. The value should be between 1 and 65535.                  |
The fields in the Smart Call Home Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Call Home Service</td>
<td>Select any of these:</td>
</tr>
<tr>
<td>• Enable</td>
<td>Enables Smart Call Home service.</td>
</tr>
<tr>
<td>• Disable</td>
<td>Disables Smart Call Home service.</td>
</tr>
<tr>
<td>• No Change</td>
<td>No change is made to Smart Call Home Service.</td>
</tr>
</tbody>
</table>

| **Contact E-mail Addresses** |
| Action                     | Select any of these: |
| • Add                      | Adds the contact e-mail addresses |
| • Remove                   | Removes the contact e-mail addresses |
| • No Change                | The contact e-mail addresses is not changed. This is the default option. |

| Contact E-mail Address     | Enter contact email address. You can enter one or more e-mail IDs. Each e-mail ID to be entered on a separate line. |

| **E-mail Server**          |
| Action                     | Select any of these: |
| • Add                      | Adds one or more e-mail servers. |
| You can add a maximum of five e-mail servers. |
| • Replace                  | Adds new e-mail servers after removing all earlier e-mail servers. |
| • Remove                   | Removes one or more e-mail servers |
| • No Change                | The e-mail servers are not changed. This is the default option. |

| E-mail Servers             | Enter one or more e-mail servers. Enter each e-mail server on a separate line and specify priority for each of them. The priority can be between 1 and 100. |

| **Sender From E-mail Address** |
| Action                        | Select any of these: |
| • Add                         | Adds a sender e-mail address |
| • Remove                      | Removes the sender e-mail address |
| • No Change                   | The sender e-mail address is not changed. This is the default option. |

| Sender E-mail Address (from) | Enter the e-mail address from which the mail is sent. |

| **Sender Reply-to Address** |
| Action                     | Select any of these: |
| • Add                       | Adds a sender reply-to e-mail address |
| • Remove                    | Removes the sender reply-to e-mail address |
| • No Change                 | Not to change the sender reply-to e-mail address. This is the default option. |

| Sender Reply-to Address     | Enter a sender reply to e-mail ID. |
### Using System-defined Tasks

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Install Cisco Security Certificate</strong></td>
<td>Check to install the HTTP certificate.</td>
</tr>
<tr>
<td><strong>Profile Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Profile</td>
<td>Select either:</td>
</tr>
<tr>
<td>• CiscoTAC-1 Profile</td>
<td>Or</td>
</tr>
<tr>
<td>• Other Profiles</td>
<td></td>
</tr>
<tr>
<td>Profile Name</td>
<td>Enter a profile name. This option is activated only if you have selected Other Profiles option in the Profile field.</td>
</tr>
<tr>
<td>Activate Profile</td>
<td>Select any of these:</td>
</tr>
<tr>
<td>• Enable — Activates the selected profile.</td>
<td></td>
</tr>
<tr>
<td>• Disable — Deactivates the selected profile.</td>
<td></td>
</tr>
<tr>
<td>• No Change — Not to add or remove a profile. This is the default option</td>
<td></td>
</tr>
<tr>
<td><strong>Transport Options</strong></td>
<td></td>
</tr>
<tr>
<td>Connect To</td>
<td>Select:</td>
</tr>
<tr>
<td>• Cisco.com if you want to connect to Smart Call Home using Cisco.com</td>
<td></td>
</tr>
<tr>
<td>• Transport Gateway, if you want to connect to Smart Call Home using a transport gateway.</td>
<td></td>
</tr>
<tr>
<td>• Other, if you want to connect to Smart Call Home using transport option other than Cisco.com or Transport Gateway.</td>
<td></td>
</tr>
<tr>
<td>CiscoTAC-1 profile does not support the Transport Gateway and Other option. So this option is not activated when you select CiscoTAC-1 profile.</td>
<td></td>
</tr>
<tr>
<td><strong>Transport Details</strong></td>
<td></td>
</tr>
<tr>
<td>Transport Method</td>
<td>Select:</td>
</tr>
<tr>
<td>• No Change — To make no change to the transport settings</td>
<td></td>
</tr>
<tr>
<td>• E-mail — To use e-mail as the transport method. This option is selected if Transport Gateway is selected as the Connect to option and the HTTPS option is not activated.</td>
<td></td>
</tr>
<tr>
<td>• HTTPS — To use HTTPS as the transport method.</td>
<td></td>
</tr>
<tr>
<td>E-mail Address</td>
<td>Enter the e-mail address, if you have selected E-mail as the transport method.</td>
</tr>
<tr>
<td>HTTPS URLs</td>
<td>Enter the HTTPS URL, if you have selected HTTPS as the transport method.</td>
</tr>
<tr>
<td><strong>Alert Groups</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Inventory</strong></td>
<td>Select any of the following:</td>
</tr>
<tr>
<td>• Enable if you want to subscribe to the Inventory Alert Group.</td>
<td></td>
</tr>
<tr>
<td>• Disable if you do not want to subscribe to the Inventory Alert Group.</td>
<td></td>
</tr>
<tr>
<td>• No Change if you do not want to subscribe to or unsubscribe from Inventory Alert Groups. This is the default option.</td>
<td></td>
</tr>
</tbody>
</table>

If you have selected CiscoTAC-1 Profile, you cannot change the Alert groups or Alert group settings.

If you have selected Other Profiles, you can change the Alert groups and Alert group settings.
### Field/Button | Description
--- | ---
**Periodicity** | Specify the periodicity for receiving these Inventory alerts. You can select:
- **Asynchronous** — To receive the Inventory alerts on a specified day or time. In other words, not in a periodic manner.
- **Daily** — To receive the Inventory alerts every day
- **Weekly** — To receive the weekly consolidated Inventory alerts.
- **Monthly** — To receive the monthly consolidated Inventory alerts

**DOW** | DOW refers to Date of Week.

This list box is activated only if you select Weekly as the periodicity for receiving the Inventory alerts. Select any of the following days of the week:
- **Sun**
- **Mon**
- **Tue**
- **Wed**
- **Thu**
- **Fri**
- **Sat**

**Sun** is the default value.

For example:
Select **Tue** if you want to receive Inventory alerts every Tuesday.

**DOM** | DOM refers to Date of Month.

This list box is activated only if you select **Monthly** as the periodicity for receiving the Inventory alerts. Select any value from 1 and 31 to receive Inventory alerts every month on the specified date.

Day 1 is the default value.

For example:
Select 5, if you want to receive Inventory alerts on the 5th day of every month.

**Begin Time** | Specify the date and time at which you want to receive the Inventory alerts.

The format supported is *hh:mm*, where *hh* refers to hours and *mm* refers to minutes.

**Configuration** | Select any of the following:

- **Enable** if you want to subscribe to the Configuration Alert Group.
- **Disable** if you do not want to subscribe to the Configuration Alert Group.
- **No Change** if you do not want to subscribe to or unsubscribe from Configuration Alert Groups. This is the default option.

If you have selected CiscoTAC-1 Profile, you cannot change the Alert groups or Alert group settings.

If you have selected Other Profiles, you can change the Alert groups and Alert group settings.
## Using System-defined Tasks

### Field/Button | Description
--- | ---
**Periodicity** | Specify the periodicity for receiving these Configuration alerts. You can select:
- **Asynchronous** — To receive the Configuration alerts on a specified day or time. In other words, not in a periodic manner.
- **Daily** — To receive the Configuration alerts every day.
- **Weekly** — To receive the weekly consolidated Configuration alerts.
- **Monthly** — To receive the monthly consolidated Configuration alerts.

**DOW** | DOW refers to Date of Week.
This list box is activated only if you select Weekly as the periodicity for receiving the Configuration alerts.
Select any of the following days of the week:
- Sun
- Mon
- Tue
- Wed
- Thu
- Fri
- Sat

Sun is the default value.
For example:
Select Tue if you want to receive Configuration alerts every Tuesday.

**DOM** | DOM refers to Date of Month.
This list box is activated only if you select Monthly as the periodicity for receiving the Configuration alerts.
Select any value from 1 and 31 to receive Configuration alerts every month on the specified date.
Day 1 is the default value.
For example:
Select 5, if you want to receive Inventory alerts on the 5th day of every month.

**Begin Time** | Specify the date and time at which you want to receive the Configuration alerts.
The format supported is hh:mm, where hh refers to hours and mm refers to minutes.

**Syslog** | Select any of the following:
- **Enable** if you want to subscribe to the Syslog Alert Group.
- **Disable** if you do not want to subscribe to the Syslog Alert Group.
- **No Change** if you do not want to subscribe to or unsubscribe from Syslog Alert Groups. This is the default option.

If you have selected CiscoTAC-1 Profile, you cannot change the Alert groups or Alert group settings.
If you have selected Other Profiles, you can change the Alert groups and Alert group settings.
### Field/Button | Description
--- | ---
**Severity** | Select from any of these severities:
- catastrophic
- disaster
- fatal
- critical
- major
- minor
- warning
- notification
- normal
- debugging
You will be notified when a syslog of the selected severity occurs.

**Patterns** | Specify a pattern of Syslogs for which you want to receive alerts.

**Environment** | Select any of the following:
- **Enable** if you want to subscribe to the Environmental Alert Group.
- **Disable** if you do not want to subscribe to the Environmental Alert Group.
- **No Change** if you do not want to subscribe to or unsubscribe from Environment Alert Groups. This is the default option.

If you have selected CiscoTAC-1 Profile, you cannot change the Alert groups or Alert group settings.
If you have selected Other Profiles, you can change the Alert groups and Alert group settings.

**Severity** | Select from any of these severities:
- catastrophic
- disaster
- fatal
- critical
- major
- minor
- warning
- notification
- normal
- debugging
You will be notified when an environment event of the selected severity occurs.
Chapter 5      Making and Deploying Configuration Changes Using NetConfig

Using System-defined Tasks

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Diagnostics</strong></td>
<td>Select any of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable</strong> if you want to subscribe to the Diagnostics Alert Group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable</strong> if you do not want to subscribe to the Diagnostics Alert Group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No Change</strong> if you do not want to subscribe to or unsubscribe from the Diagnostics Alert Groups. This is the default option.</td>
</tr>
<tr>
<td></td>
<td>If you have selected CiscoTAC-1 Profile, you cannot change the Alert groups or Alert group settings.</td>
</tr>
<tr>
<td></td>
<td>If you have selected Other Profiles, you can change the Alert groups and Alert group settings.</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Select from any of these severities:</td>
</tr>
<tr>
<td></td>
<td>• <strong>catastrophic</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>disaster</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>fatal</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>critical</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>major</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>minor</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>warning</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>notification</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>normal</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>debugging</strong></td>
</tr>
<tr>
<td></td>
<td>You will be notified when a diagnostics alert of the selected severity occurs.</td>
</tr>
<tr>
<td><strong>Applicable Devices</strong></td>
<td>Allows you to view the IOS devices in your selection.</td>
</tr>
<tr>
<td><strong>Save</strong></td>
<td>Saves the information you have specified.</td>
</tr>
<tr>
<td><strong>Reset</strong></td>
<td>Clears all fields and reverts to the default settings.</td>
</tr>
<tr>
<td><strong>Cancel</strong></td>
<td>Ignores your changes.</td>
</tr>
</tbody>
</table>
Syslog Task

You can use the Syslog system-defined task to configure the collection of syslog messages from devices. The following device categories are supported by this task:

- IOS (including Cable devices)
- Content Engine
- CSS
- NAM
- PIX OS

For more details, see Table 5-5.

You can enter the details of this task in the Syslog Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Syslog Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td>Logging Host</td>
<td>Action</td>
<td>Select the required option to enable, disable, or make no change to list of hosts that receive syslog messages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ex:</td>
<td>Enter the IP addresses of hosts to be added to or removed from the list of hosts that receive syslog messages. Separate multiple addresses with commas.</td>
</tr>
<tr>
<td>IOS Parameters</td>
<td>Logging On</td>
<td>Action</td>
<td>Select the required option to enable, disable, or make no change to syslog state. Select No Change to make syslog setup changes without enabling or disabling syslog logging.</td>
</tr>
<tr>
<td></td>
<td>Logging Facility</td>
<td>Action</td>
<td>Select the required option to enable, disable, or make no change to syslog logging facility.</td>
</tr>
<tr>
<td></td>
<td>Logging Level</td>
<td>Parameter</td>
<td>Select the logging facility to which the syslog messages are logged.</td>
</tr>
<tr>
<td></td>
<td>Buffered</td>
<td>Action</td>
<td>Select the required option to enable, disable, or make no change to the buffered logging level.</td>
</tr>
</tbody>
</table>
### Conditions

Select the required logging level from the drop-down list:
- Default
- alerts
- critical
- debugging
- emergencies
- errors
- informational
- notifications
- warnings

### Console Action

Select the required option to enable, disable, or make no change to the console logging level.

### Conditions

Select the required logging level from the drop-down list.

### Monitor Action

Select the required option to enable, disable, or make no change to the monitor logging level.

### Conditions

Select the required logging level from the drop-down list.

### Trap Action

Select the required option to enable, disable, or make no change to the trap logging level.

### Conditions

Select the required logging level from the drop-down list.

### CatOS Parameters

#### Console Logging On

Action

Select the required option to enable, disable, or make no change to console logging.

#### Server Logging On

Action

Select the required option to enable, disable, or make no change to server logging.

#### Logging Level

Action

Select the required option to enable, disable, or make no change to the logging level.

#### Facility

Select the logging facility to which the syslog messages are logged.

#### Level

Select the required logging level from the drop-down list.

### Content Engine Parameters

#### Logging On

Action

Select the required option to enable, disable, or make no change to logging.

#### Destination

Console

Select this option to specify the console as the logging destination.

Disk

Select this option to specify the disk as the logging destination.

#### Logging Facility

Action

Select the required option to enable, disable, or make no change to syslog logging facility.

Parameter

Select the logging facility to which the syslog messages are to be logged.
<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Priority</td>
<td>Console</td>
<td>Action</td>
<td>Select the required option to enable, disable, or make no change to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>console logging priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Conditions</td>
<td>Select the required logging priority from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>Disk</td>
<td>Action</td>
<td>Select the required option to enable, disable, or make no change to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>disk logging priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Conditions</td>
<td>Select the required logging priority from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>Host</td>
<td>Action</td>
<td>Select the required option to enable, disable, or make no change to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>host logging priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Conditions</td>
<td>Select the required logging priority from the drop-down list.</td>
</tr>
<tr>
<td>PIX Parameters</td>
<td>Time Stamp</td>
<td>Action</td>
<td>Select the required option to enable, disable, or make no change to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>syslog logging facility.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Parameter</td>
<td>Select the logging facility to which the syslog messages are to be logged.</td>
</tr>
<tr>
<td></td>
<td>Syslog Message ID</td>
<td>Enter the syslog message ID.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Conditions</td>
<td>Select the required logging level from the drop-down list.</td>
</tr>
<tr>
<td>Logging Facility</td>
<td>Action</td>
<td></td>
<td>Select the required option to enable, disable, or make no change to the</td>
</tr>
<tr>
<td></td>
<td>Parameter</td>
<td></td>
<td>syslog logging facility.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Select the logging facility to which the syslog messages are to be logged.</td>
</tr>
<tr>
<td></td>
<td>Monitor</td>
<td>Action</td>
<td>Select the required option to enable, disable, or make no change to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>syslog logging facility.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Conditions</td>
<td>Select the required logging level from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>Trap</td>
<td>Action</td>
<td>Select the required option to enable, disable, or make no change to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>syslog logging facility.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Conditions</td>
<td>Select the required logging level from the drop-down list.</td>
</tr>
<tr>
<td>CSS Parameters</td>
<td>Facility</td>
<td></td>
<td>Select the logging facility to which to log syslog messages.</td>
</tr>
<tr>
<td></td>
<td>Logging Level</td>
<td></td>
<td>Select the required logging level from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>CLI Command</td>
<td></td>
<td>Select the required option to add, remove, or make no change to the CLI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>commands.</td>
</tr>
<tr>
<td></td>
<td>Logging to Disk</td>
<td></td>
<td>Select the required option to add, remove, or make no change to the option</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>of logging to disk.</td>
</tr>
</tbody>
</table>
### Using System-defined Tasks

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Logfile Name</td>
<td></td>
<td>Enter the log file name.</td>
</tr>
<tr>
<td></td>
<td>Buffer</td>
<td></td>
<td>Select the required option to add, remove, or make no change to the buffer configuration.</td>
</tr>
<tr>
<td></td>
<td>Size [0-64000]</td>
<td></td>
<td>Enter the size of the buffer. Enter a value between 0 and 64000 bytes.</td>
</tr>
<tr>
<td></td>
<td>To sys.log</td>
<td></td>
<td>Select the required option to add, remove, or make no change to the option of logging to a file called sys.log.</td>
</tr>
<tr>
<td>Logging to</td>
<td>Line</td>
<td></td>
<td>Choose this option to send the log activity of a subsystem to an active CSS session.</td>
</tr>
<tr>
<td>Line</td>
<td>Active Session</td>
<td></td>
<td>Enter the name of the active session. Enter a case-sensitive unquoted text string with a maximum length of 32 characters.</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging to</td>
<td>Send Mail</td>
<td></td>
<td>Select the required option to add, remove, or make no change to the e-mail option.</td>
</tr>
<tr>
<td>Mail</td>
<td>Mail Address</td>
<td></td>
<td>Enter the e-mail IDs (comma separated).</td>
</tr>
<tr>
<td></td>
<td>SMTP Host</td>
<td></td>
<td>Enter the SMTP hostname or the IP address.</td>
</tr>
<tr>
<td></td>
<td>(Name or IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Address)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Logging Level</td>
<td></td>
<td>Select the required logging level from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>Domain Name</td>
<td></td>
<td>Enter the domain name of the SMTP host. This is an optional field.</td>
</tr>
<tr>
<td></td>
<td>(Optional)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAM Parameters</td>
<td>MIB Threshold</td>
<td>Local</td>
<td>Select the required option to enable, disable, or make no change to the local MIB threshold.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote</td>
<td>Select the required option to enable, disable, or make no change to the remote MIB threshold.</td>
</tr>
<tr>
<td></td>
<td>Voice</td>
<td>Local</td>
<td>Select the required option to enable, disable, or make no change to the voice (local).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote</td>
<td>Select the required option to enable, disable, or make no change to the voice (remote).</td>
</tr>
<tr>
<td></td>
<td>System</td>
<td>Local</td>
<td>Select the required option to enable, disable, or make no change to the system (local).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote</td>
<td>Select the required option to enable, disable, or make no change to the system (remote).</td>
</tr>
<tr>
<td></td>
<td>Debug</td>
<td>System</td>
<td>Select the required option to enable, disable, or make no change to the Debug (system).</td>
</tr>
</tbody>
</table>
SSH Configuration Task

You can use the SSH system-defined task to configure SSH on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Content Engine
- CSS
- NAM

For more details, see Table 5-5.

You can enter the details of this task in the SSH Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For this task to work correctly, you must use a CLI-based protocol (Telnet or SSH) as the download protocol.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

For each device category, click on Applicable Devices to view the devices in your selection, to which this task applies.

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td>Key Configuration</td>
<td>Action</td>
<td>Select the required option to enable, disable, or make no change to the key configuration.</td>
</tr>
<tr>
<td>IOS Parameters</td>
<td>Prerequisites</td>
<td>Number of Key Bits [360-2048]</td>
<td>Enter the number of Key bits to be used for Key generation. The value must be between 360 and 2048 Key bits.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timeout</td>
<td>Action</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timeout Value [1-120]:</td>
<td>Enter timeout value for SSH sessions. The value should be between 1 and 120.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Retries</td>
<td>Action</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of Retries [1-5]</td>
<td>Enter the number of retries allowed. The number must be between 1 and 5.</td>
</tr>
<tr>
<td>CE Parameters</td>
<td>SSH Prerequisites</td>
<td>SSH Daemon</td>
<td>Select the required option to enable, disable, or make no change to the SSH daemon.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of Key Bits [512-2048]</td>
<td>Enter the number of Key bits to be used for Key generation. The value must be between 512 and 2048 Key bits.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSH Timeout</td>
<td>Enter login grace time for SSH sessions, in seconds. Value must be between 1 and 99999.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password-guesses [1-99]</td>
<td>Specify the number of password retries allowed. The value must be between 1 and 99.</td>
</tr>
</tbody>
</table>
For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

### TACACS Configuration Task

You can use the TACACS system-defined task to configure TACACS authentication. This task supports the IOS device category including Cable devices.

For more details, see Table 5-5.

You can enter the details of this task in the TACACS Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSS Parameters</td>
<td></td>
<td>Number of Server Key Bits</td>
<td>Enter the number of Key bits to be used for Key generation. The value must be between 512 and 32768 Key bits.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key Bits [512-32768]</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Action</td>
<td>Port Number [22-65535]</td>
<td>Enter the port number. This value can be between 22 and 65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KeepAlive</td>
<td>Select the required option to add, remove, or make no change to keepalive.</td>
</tr>
</tbody>
</table>

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).
TACACS+ Configuration Task

You can use the TACACS+ system-defined template to configure TACACS+ on devices. This task supports the following device categories:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- NAM

For more details, see Table 5-5.

You can enter the details of this task in the TACACS+ Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Parameters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TACACS Server Configuration</td>
<td>Server</td>
<td>Action</td>
<td>Select to enable, disable, or make no change to the TACACS Server configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hostname or IP Address</td>
<td>Enter the hostname or the IP address of the TACACS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key</td>
<td>Select to add, remove, or make no change to the TACACS encryption Key.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key</td>
<td>Enter the TACACS encryption key. The key is used to set authentication and encryption. This key must match the key used on the TACACS+ daemon. The key can be of any size.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify Key</td>
<td>Re-enter the Key to confirm.</td>
</tr>
</tbody>
</table>
## Login Authentication

### Using System-defined Tasks

**Action**
Select to enable, disable, or make no change to the TACACS+ authentication.

- If login authentication is enabled, then when you try to login to the device, you are authenticated by the TACACS server.
- If login authentication is disabled, then you are not authenticated by the TACACS server when you log in to the device.

### Credentials

**Username**
Enter TACACS+ username. These values are entered only in the Device and Credential Repository. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.

**Password**
Enter TACACS+ password. For details see Understanding the NetConfig Credentials Configuration Tasks.

**Verify**
Re-enter the password to confirm. For details see Understanding the NetConfig Credentials Configuration Tasks.

## IOS Parameters

### Enable mode Authentication

**Action**
Select to enable, disable, or make no change to the enable mode authentication.

### Credentials

**Password**
Enter the enable password.

**Verify**
Re-enter the enable password.

**Name**
Enter default or named list.

**Set to Default**
Select to set the default list.

### Type

(Drop-down list)
Select the required option:
- No Choice
- radius
- tacacs+
- line
- enable
- local
- none

Similarly, select the type from the other three drop-down lists.

## CatOS Parameters

### Enable mode Authentication

**Action**
Select to add, remove, or make no change to the enable mode authentication.

### Credentials

**Password**
Enter the enable password.

**Verify**
Re-enter the enable password.

### Server Options

**Primary**
Click to designate specified server as primary TACACS server.
Chapter 5  Making and Deploying Configuration Changes Using NetConfig

Using System-defined Tasks

### Telnet Password Configuration Task

You can use the Telnet Password system-defined configuration task to change the Telnet password on devices.

This task supports the following device categories:

- IOS (including Cable devices)
- Catalyst OS
- PIX OS

For more details, see Table 5-5.

You can enter the details of this task in the Telnet Password Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

For details on the NetConfig credentials configuration tasks, see Understanding the NetConfig Credentials Configuration Tasks.

If you change the Telnet password on a Catalyst device with an RSM module using this template, the RSM Telnet password is also changed.

---

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ContentEngine Parameters</td>
<td>Server Option</td>
<td>Primary</td>
<td>Select to specify the server as primary.</td>
</tr>
<tr>
<td></td>
<td>Password Option</td>
<td>ASCII Password</td>
<td>Select for an ASCII password.</td>
</tr>
<tr>
<td></td>
<td>Connection Options</td>
<td>Timeout</td>
<td>Enter the timeout value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Retries</td>
<td>Enter the number of retries.</td>
</tr>
</tbody>
</table>
| NAM Parameters        |            |        | No category-specific commands  
|                       |            |        | The TACACS Server Key should be DES encrypted for NAM devices.             |

At the time of enabling login authentication or enable mode authentication, it is mandatory for you to enter the username and password.

At the time of disabling login authentication or enable mode authentication, these fields are optional. While disabling login authentication or enable mode authentication, if username and password are not provided, then the corresponding fields in DCR are cleared and left blank. This may make the device unreachable. Therefore we recommend that you provide the username and password at the time of disabling login authentication.
The fields in the Telnet Password Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Parameters</td>
<td>Vty Lines</td>
<td>Action</td>
<td>Select an option to enable, disable, or make no change to the Vty Line password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password</td>
<td>Enter the Vty Line password. If you select vty, the change affects all device vty lines, and the Device and Credential Repository is updated with the new password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify</td>
<td>Re-enter the Vty Line password to confirm.</td>
</tr>
<tr>
<td></td>
<td>Console Line</td>
<td>Action</td>
<td>Select an option to enable, disable, or make no change to the Console Line password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password</td>
<td>Enter the Console Line password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify</td>
<td>Re-enter the Console Line password to confirm.</td>
</tr>
<tr>
<td></td>
<td>Aux Line</td>
<td>Action</td>
<td>Select an option to enable, disable, or make no change to the Auxiliary (AUX) Line password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password</td>
<td>Enter the Aux Line password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify</td>
<td>Re-enter the Aux Line password to confirm.</td>
</tr>
<tr>
<td>CatOS Parameters</td>
<td>Telnet Password</td>
<td>Action</td>
<td>Select an option to enable, disable, or make no change to the Telnet password. The Device and Credential Repository is updated with the new password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password</td>
<td>Enter the Telnet password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify</td>
<td>Re-enter the Telnet password to confirm.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Apply command on modules</td>
<td>Select this option to update only the non IP addressable modules. If you select the Action as Disable, the password will be removed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disable will set an empty password</td>
<td></td>
</tr>
<tr>
<td>PIX Parameters</td>
<td>Action</td>
<td>Select the required option to replace, reset, or make no change to the password.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>Enter the password.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify</td>
<td>Re-enter the password to confirm.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Encrypted Password</td>
<td>Select this option, if the password you are entering is already encrypted.</td>
<td></td>
</tr>
</tbody>
</table>

**Transform System-Defined Task**

You can use the Transform system-defined task to configure IPSec on devices. You must configure the IKE configuration system-defined task before configuring the Transform system-defined task.

This task supports the following device categories:

- IOS (including Cable devices)
- PIX OS

For more details, see Table 5-5.
You can enter the details of this task in the Transform Set Configuration dialog box. (To invoke this
dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog
box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Transform Set Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Parameters</td>
<td></td>
<td>Seconds</td>
<td>Enter the number of seconds that will be used for negotiating IPSec security association (SA).</td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td>Configuration</td>
<td><strong>Seconds</strong></td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td></td>
<td>Select this option to remove previously specified seconds value, if any.</td>
</tr>
<tr>
<td></td>
<td>Kilo Bytes Configuration</td>
<td>Kilo Bytes</td>
<td>[2560-536870912]</td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td></td>
<td>Select this option to remove previously specified value, if any.</td>
</tr>
<tr>
<td></td>
<td>IPSec Transform Set Configuration</td>
<td>Action</td>
<td>Select the required option to add, remove or make no change to transform set configuration.</td>
</tr>
<tr>
<td></td>
<td>Note: Only for IOS 12.1 and higher.</td>
<td></td>
<td>This sub-group of fields is applicable only to IOS version 12.1 and above.</td>
</tr>
<tr>
<td></td>
<td>Transform Set Name</td>
<td></td>
<td>Enter a name for the transform set.</td>
</tr>
<tr>
<td></td>
<td>Auth Header</td>
<td></td>
<td>Select the type of authentication algorithm.</td>
</tr>
<tr>
<td></td>
<td>ESP Encryption</td>
<td></td>
<td>Select the type of encryption algorithm with ESP.</td>
</tr>
<tr>
<td></td>
<td>ESP Authentication</td>
<td></td>
<td>Choose the type of authentication algorithm with ESP.</td>
</tr>
<tr>
<td></td>
<td>IP Compression</td>
<td></td>
<td>Select to use IP compression with LZS algorithm.</td>
</tr>
<tr>
<td></td>
<td>Transport Mode</td>
<td></td>
<td>Select the mode of transport.</td>
</tr>
<tr>
<td>PIX Parameters</td>
<td></td>
<td></td>
<td><strong>Seconds</strong></td>
</tr>
<tr>
<td></td>
<td>Kilo Bytes</td>
<td></td>
<td>Enter the amount of traffic in kilobytes that will be used for negotiating IPSec SA. \The value must be between 2560 and 536870912 kilobytes.</td>
</tr>
<tr>
<td></td>
<td>IPSec Transform Set Configuration</td>
<td>Action</td>
<td>Select the required option to add, remove or make no change to transform set configuration.</td>
</tr>
<tr>
<td></td>
<td>Transform Set Name</td>
<td></td>
<td>Enter the name for the transform set.</td>
</tr>
<tr>
<td></td>
<td>Auth Header</td>
<td></td>
<td>Select the type of authentication algorithm.</td>
</tr>
</tbody>
</table>
Chapter 5  Making and Deploying Configuration Changes Using NetConfig

Using System-defined Tasks

You can use the Web User configuration task to configure the web user for NAM devices. This is a System-defined task. For more details, see Table 5-5. You can enter the details of this task in the Web User Configuration dialog box.

To invoke this dialog box, see Starting a New NetConfig Job.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).. The fields in the in the Web User Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAM Parameters</td>
<td>Web User</td>
<td>Action</td>
<td>Select an option to add, remove, or make no change to the web user group of fields.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Username</td>
<td>Enter the username of the web user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password</td>
<td>Enter the password for the username.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify</td>
<td>Re-enter the password to confirm.</td>
</tr>
<tr>
<td>Privileges</td>
<td>Account Management</td>
<td>System Config</td>
<td>Select the required option to enable, disable or make no change to system configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Capture</td>
<td>Select the required option to enable, disable or make no change to the capture configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alarm Config</td>
<td>Select the required option to enable, disable or make no change to the alarm configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Collection Config</td>
<td>Select the required option to enable, disable or make no change to the collection configuration.</td>
</tr>
</tbody>
</table>

Click Applicable Devices to view the devices in your selection to which this task applies.

User-defined Protocol Task

You can use the User-defined Protocol task to configure the user-defined protocol on NAM devices. This is a system-defined task.

For more details, see Table 5-5.

You can enter the details of this task in the User-defined Protocol Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)
For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the User-defined Protocol Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAM Parameters</td>
<td>User Defined Protocol</td>
<td>Action</td>
<td>Select an option to add, remove or replace the user-defined protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protocol</td>
<td>Select the protocol:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• TCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port [0 - 65535]</td>
<td>Enter the port number. You can enter any port number in the range of 0—65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Name</td>
<td>Enter the name of the user-defined protocol.</td>
</tr>
<tr>
<td>Affected Stats</td>
<td>Host</td>
<td></td>
<td>Select this option to enable host—Examines a stream of packets; produces a table of all network addresses observed in those packets (also known as the collection data). Each entry records the total number of packets and bytes sent and received by that host and the number of non-unicast packets sent by that host.</td>
</tr>
<tr>
<td></td>
<td>Conversations</td>
<td></td>
<td>Select this option to enable host conversations.</td>
</tr>
<tr>
<td></td>
<td>ART</td>
<td></td>
<td>Select this option to enable Application Response Time.</td>
</tr>
</tbody>
</table>

Click **Applicable Devices** to view the devices in your selection to which this task applies.

### Cable BPI/BPI+ Task

You can use the Cable BPI/BPI+ Task to assign BPI/BPI+ options.

This task is applicable to the Cable device category. For more details, see **Table 5-5**.

You can enter the details of this task in the Cable BPI/BPI+ Configuration dialog box. (To invoke this dialog box, see **Starting a New NetConfig Job**.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see **Understanding the System-defined Task User Interface (Dialog Box)**.
The fields in the Cable BPI/BPI+ Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPI/BPI+</td>
<td>Interface Configuration</td>
<td>Cable Interface</td>
<td>Allows you to select an interface to modify the other fields. You must select at least one interface. Select the cable interface that you want to change.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BPI</td>
<td>Select the appropriate option:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No Change—Does not change the existing configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Enable—Enables this option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Disable—Disables this option.</td>
</tr>
<tr>
<td>Key Lifetime</td>
<td></td>
<td>Action</td>
<td>Select the appropriate option:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No Change—Does not modify this option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Replace—Modifies this option to your specification.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Default—Resets this option to the system default.</td>
</tr>
<tr>
<td></td>
<td>[300 - 604800]</td>
<td>KEK Lifetime</td>
<td>Replaces the time (in seconds) using the specified values or resets the time using the system default. Enter time in seconds to reset the time. Enter a value from 300—604800 seconds. The default is 604800 seconds. Select the check box to reset the field to system default.</td>
</tr>
<tr>
<td></td>
<td>[180 - 604800]</td>
<td>TEK Lifetime</td>
<td>Replaces the time (in seconds) using your values or resets the time using the system default. Enter time in seconds to reset the time using your values. The range is 180 - 604,800 seconds and the default is 43,200 seconds. Select the check box to reset the field to system default.</td>
</tr>
<tr>
<td>BPI/BPI+ Options</td>
<td></td>
<td>Action</td>
<td>Select the required options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No Change—Does not change the existing configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Enable—Enables this option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Disable—Disables this option.</td>
</tr>
<tr>
<td>Mandatory</td>
<td></td>
<td></td>
<td>Select to force all modems to use BPI.</td>
</tr>
<tr>
<td>Authenticate Modem</td>
<td></td>
<td></td>
<td>Select to turn the BPI modem authentication on or off.</td>
</tr>
<tr>
<td>Authorize Multicast</td>
<td></td>
<td></td>
<td>Select to turn BPI Multicast option on or off.</td>
</tr>
<tr>
<td>OAEP Support</td>
<td></td>
<td></td>
<td>Select to enable or disable Optimal Asymmetric Encryption Padding (OAEP) BPI+ encryption.</td>
</tr>
<tr>
<td>DSX Support</td>
<td></td>
<td></td>
<td>Select to enable or disable encryption for dynamic services SIDs.</td>
</tr>
<tr>
<td>40 Bit Des</td>
<td></td>
<td></td>
<td>Select to indicate that you have chosen the 40 bit DES encryption. The system default is 56 DES encryption. This is the Cisco recommended encryption.</td>
</tr>
</tbody>
</table>
Click Applicable Devices to see the devices in your selection, to which this task applies.

**Cable DHCP-GiAddr and Helper Task**

You can use this task to configure the GiAddr field of DHCPDISCOVER and DHCPREQUEST packets with a relay IP address before they are forwarded to the DHCP server. You can apply this task only for a single Cable-CMTS device at a time.

This task is applicable to the Cable device category. For more details, see Table 5-5.

You can enter the details of this task in the Cable DHCP-GiAddr and Helper Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

**Note**
You can apply this task only to a single device at a time because cable templates configure interfaces on devices.

The fields in the Cable DHCP-GiAddr and Helper Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Setup</td>
<td></td>
<td>Cable Interface</td>
<td>Select a cable interface to make the configuration changes to the selected interface, from the drop-down list. If there are no interfaces available, you will see the option No Interfaces Found in the drop-down list. You should make sure that the device is reachable and then select a valid interface.</td>
</tr>
</tbody>
</table>
|              |           | Action | Select an option from the drop-down list. The options are:  
• No Change—Does not change the current configuration.  
• Add/Modify—Adds a new GiAddr or Helper Address or both, or modifies an existing GiAddr or Helper Address or both.  
• Remove—Removes the GiAddr or Helper Address or both.  
Select an option to Add or Modify, from the drop-down list:  
• DHCP-Giaddr & Helper-Address—Enables you to set the DHCP GiAddr to Policy or Primary. You can also specify values for the fields in the Cable Helper Addresses group.  
• DHCP-Giaddr—Enables you to set the DHCP GiAddr to Policy or Primary.  
• Helper-Address—Enables you to specify values for the fields in the Cable Helper Addresses group. |
Using System-defined Tasks

Click Applicable Devices to view the devices in your selection to which this task applies.

### Cable Downstream Task

You can use this task to configure the Annex, Channel-ID, Frequency, Modulation, Interleave depth, and Set rate limit of a downstream cable interface. You can also configure the Radio Frequency (RF) output of a downstream cable interface on a Cisco uBR7100 router.

This task is applicable only to Cable devices.

For more details, see Table 5-5.

You can enter the details of this task in the Downstream Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

**Note** You can apply this task to a maximum of one Cable-CMTS device at a time.
The fields in the Downstream Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable Parameters</td>
<td></td>
<td>Cable Interface</td>
<td>Select the required option from the drop-down list. Select a cable interface to make the required configuration changes. If you do not want to select any cable interface, choose the Not Selected option.</td>
</tr>
<tr>
<td>Activate/Configure</td>
<td>Shutdown</td>
<td>Action</td>
<td>Allows you to shutdown or activate the selected interface. The options are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No Change—Does not allow modification of any fields in this sub-group of fields.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Shutdown—Deactivates the DS port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No Shutdown—Activates the DS port.</td>
</tr>
<tr>
<td>Interleave Depth</td>
<td>Interleave Depth</td>
<td>Allows you to select the interleave depth of a channel. The depth can be between 8 and 128. The default is 32. Specify the interleave depth by selecting the appropriate option from the drop-down list.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td>Select to remove the interleave depth configuration.</td>
<td></td>
</tr>
<tr>
<td>Framing Format</td>
<td>MPEG Framing Format</td>
<td>Select the MPEG framing format from the drop-down list. The options are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No Change—Does not allow modification of any fields in this sub-group of fields.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Annex A—for Cisco uBR-MC16E cable interface card and Cisco uBR7111E and Cisco uBR7114E Universal Broadband Routers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Annex B—for all other Cisco cable interface cards.</td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td>Select to remove a previously-specified MPEG framing format configuration.</td>
<td></td>
</tr>
<tr>
<td>Modulation</td>
<td>Modulation</td>
<td>Sets the modulation for a downstream port on a cable interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the required option. The options are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No Change—Does not allow modification of any fields in this sub-group of fields.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 64 qam</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 256 qam</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td>Select to remove a previously-specified modulation configuration.</td>
<td></td>
</tr>
<tr>
<td>Channel</td>
<td>Channel ID (0-255):</td>
<td>Channel-ID can be from 0 and 255. Specify the channel-ID.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td>Select to remove the Channel ID.</td>
<td></td>
</tr>
<tr>
<td>Frequency</td>
<td>Frequency (54-858 MHz)</td>
<td>Frequency range can be from 54MHz -1,000MHz. Enter the frequency.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td>Select to remove a previously-specified frequency range.</td>
<td></td>
</tr>
</tbody>
</table>
## Using System-defined Tasks

### Cable Upstream Task

Use this task to configure the frequency, minislot size, power level and admission control on upstream cable interfaces. You can apply this task to a maximum of one Cable-CMTS device at a time.

This task is applicable only to Cable devices.

For more details, see Table 5-5.

You can enter the details of this task in the Upstream Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Traffic Shaping     |                   | Rate Limit                                 | Select the required option from the drop-down list. The options are:  
  - No Change—Does not allow modification of any fields in this group of fields.  
  - Enable—Enables this option.  
  - Disable—Disables this option.                                                                                                                                                                                                                                               |
|                     |                   | Rate Limit Algorithm (Optional):           |  
  - None—Does not modify the rest of the fields.  
  - Token-bucket with DS Traffic Shaping—Modifies the Token Bucket Algorithm option.  
  - Token-bucket without DS Traffic Shaping—Modifies the Token Bucket without DS Traffic Shaping Algorithm option  
  - Weighted-discard—Modifies the Weighted Discard option.                                                                                                                                                                                                                     |
|                     | Token Bucket      | Granularity in Milliseconds (Optional):    | Specifies traffic shaping granularity in milliseconds.  
  This field is enabled only if you have selected the Rate Limit Algorithm as Token-bucket with DS Traffic Shaping.  
  Select the required value from the drop-down list. You can choose a value between 1 and 16 msec.                                                                                                                                                                           |
|                     | Max Delay in       | Granularity in Milliseconds (Optional):    | Sets the maximum buffering delay in milliseconds.  
  This field is enabled only if you have selected the Rate Limit Algorithm as Token-bucket with DS Traffic Shaping.  
  Select the required value from the drop-down list. You can choose a value between 128 and 1024.                                                                                                                                                                      |
|                     | Weighted Discard   | Weight for the exponential moving average of loss rate | Sets the weighted discard algorithm.  
  This field is enabled only if you have selected the Rate Limit Algorithm as Weighted Discard.  
  Enter a weight between 1 and 4.                                                                                                                                                                                                                                             |

Click **Available Devices** to view the list of devices from your selection, to which this task applies.
### Note
You can apply this task to a maximum of one cable device at a time.

The fields in the Upstream Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Setup</td>
<td></td>
<td>Cable Interface</td>
<td>Allows you to select cable interfaces for configuration. Select the cable interfaces from the drop-down list.</td>
</tr>
</tbody>
</table>
|                         | Activate/Deactivate US Port      | Activate/Deactivate US Port | Select one of these options from the drop-down list. The options are:  
• No Change—Does not change the existing configuration.  
• Shutdown—Deactivates this port.  
• No Shutdown—Activates this port. |
| Frequency               | Value [5-42 MHz]                 | Enter the required frequency value in the range 5—42 MHz. The range for the frequency is:  
• 5—65 MHz for Cisco uBR-MC16E cable interface line card  
• 5—42 MHz for all other cable interface line cards. |
|                         | Set to Default                   | Select this option to set the default frequency. A negation command is generated to remove the frequency value and set the default. This is because the default frequency value is dynamic and varies from device to device. |
| Power Configuration     | Power Level Value [-10-+25 dBmV]: | Enter the power level. The valid range for the power level is between -10dBmV and +25dBmV. |
|                         | Set to Default                   | Select this option to set the default power level. The default is 0dBmV. |
|                         | Power Adjustment Continue [2-15 dB] | Enter the power adjustment value. The valid range for power adjustment value is between 2dB and 15dB. |
|                         | Set to Default                   | Select this option to set the default power adjustment value. The default is 2dB. |
|                         | Noise                            | Enter the power adjustment noise level. The valid range for the power adjustment noise value between 10 and 100%. |
|                         | Set to Default                   | Select this option to set the default noise value. The default is 30%. |
|                         | Threshold [0-10 dB]              | Enter the power adjustment threshold value. The valid range for the power adjustment threshold value is between 1dB and 10dB. |
|                         | Set to Default                   | Select this option to set the default power adjustment threshold value. The default is 1dB. |
### Using System-defined Tasks

#### Admission Control

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value [0 - 1000%]</td>
<td>Indicates the maximum cumulative bandwidth reservation allowed before new CMs are rejected. The valid range is between 10% and 1000%.</td>
</tr>
<tr>
<td>Set to Default</td>
<td>Select this option to set the default admission control value. The default value is 100%.</td>
</tr>
</tbody>
</table>

#### Minislot Size

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>Select the required options. The options are:</td>
</tr>
<tr>
<td></td>
<td>• No Change</td>
</tr>
<tr>
<td></td>
<td>• 2</td>
</tr>
<tr>
<td></td>
<td>• 4</td>
</tr>
<tr>
<td></td>
<td>• 8</td>
</tr>
<tr>
<td></td>
<td>• 16</td>
</tr>
<tr>
<td></td>
<td>• 32</td>
</tr>
<tr>
<td></td>
<td>• 64</td>
</tr>
<tr>
<td></td>
<td>• 128</td>
</tr>
<tr>
<td></td>
<td>• [default]</td>
</tr>
</tbody>
</table>

Select **No Change** to make no changes in this field.

#### Channel Width(Hz)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>Select the required channel width option. The options are:</td>
</tr>
<tr>
<td></td>
<td>• No Change—Does not modify the existing configuration.</td>
</tr>
<tr>
<td></td>
<td>• 200000</td>
</tr>
<tr>
<td></td>
<td>• 400000</td>
</tr>
<tr>
<td></td>
<td>• 800000</td>
</tr>
<tr>
<td></td>
<td>• 1600000 (default)</td>
</tr>
<tr>
<td></td>
<td>• 3200000</td>
</tr>
</tbody>
</table>

Select **No Change** to make no changes in this field.

#### Concatenation

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concatenation</td>
<td>Select one of these options:</td>
</tr>
<tr>
<td></td>
<td>• No Change—Does not modify the existing configuration</td>
</tr>
<tr>
<td></td>
<td>• Enable—Enables this option.</td>
</tr>
<tr>
<td></td>
<td>• Disable—Disables this option.</td>
</tr>
</tbody>
</table>

#### FEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEC</td>
<td>Select one of the following options for Enable Forward Error Correction (FEC):</td>
</tr>
<tr>
<td></td>
<td>• No Change - Does not modify the existing configuration.</td>
</tr>
<tr>
<td></td>
<td>• Enable - Enables this option.</td>
</tr>
<tr>
<td></td>
<td>• Disable - Disables this option.</td>
</tr>
</tbody>
</table>

#### Fragmentation

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragmentation</td>
<td>Select the required fragmentation option. The options are:</td>
</tr>
<tr>
<td></td>
<td>• No Change—Does not modify the existing configuration.</td>
</tr>
<tr>
<td></td>
<td>• Enable—Enables this option.</td>
</tr>
<tr>
<td></td>
<td>• Disable—Disables this option.</td>
</tr>
<tr>
<td>Group</td>
<td>Sub-Group</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Rate Limit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Backoff</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automatic</td>
</tr>
<tr>
<td></td>
<td>Start Value [0-15]</td>
</tr>
<tr>
<td></td>
<td>End Value [0-15]</td>
</tr>
<tr>
<td>Range Backoff</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automatic</td>
</tr>
<tr>
<td></td>
<td>Start Value (0-15)</td>
</tr>
<tr>
<td></td>
<td>End Value (0-15)</td>
</tr>
</tbody>
</table>

Click **Available Devices** to view the list of devices from your selection, to which this task applies.
Cable Interface Bundling Task

You can use this task to configure the interface bundling. You can apply this task only to a single Cable-CMTS device at a time.

This task is applicable to the Cable device category. For more details, see Table 5-5.

You can enter the details of this task in husbanded Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

**Note**

At a time, you can apply this task only to a single device, because cable templates configure interfaces on devices.

The fields in the Bundle Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable Parameters</td>
<td>Action</td>
<td>Select one of these options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No Change—Does not modify the existing parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add—Enables you to configure an interface as a master interface or a slave interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remove—Enables you to change the previous configuration of the interface (master to slave or vice versa).</td>
</tr>
<tr>
<td></td>
<td>Bundle ID (1-255)</td>
<td>Indicates the bundle identifier.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter a bundle ID between 1 and 255.</td>
</tr>
<tr>
<td></td>
<td>Master Interface</td>
<td>Allows you to configure the primary interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the cable interface from the list of primary interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select <strong>Not Selected</strong> if you do not want to select a primary interface.</td>
</tr>
<tr>
<td></td>
<td>Slave Interface</td>
<td>Allows you to configure the secondary interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the cable interface from the list of secondary interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select <strong>Not Selected</strong> if you do not want to select a secondary interface.</td>
</tr>
</tbody>
</table>

Click **Applicable Devices** to view the devices in your selection to which this task applies.

Cable Spectrum Management Task

You can use this task to create and assign spectrum groups to cable interfaces and upstream interfaces. This task supports cable devices.

For more details, see Table 5-5.

You can enter the details of this task in the Cable Spectrum Management Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.
For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Cable Spectrum Management Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Spectrum Management | Spectrum Group | Action | Select one of these options:  
  • No Change—Does not allow you to make any changes in the Spectrum group of fields.  
  • Add—Allows you to add options.  
  • Remove—Allows you to remove options. |
| Spectrum Group ID [1 - 32] | | | Enter the Spectrum Group ID. The range for Spectrum Group ID is 1—32. |
| Frequency Setting | | | Select one of these frequency settings:  
  • Band—Enter a range of frequencies.  
  • Fix—Enter a fixed frequency. |
| Start Frequency [5 - 42 MHz] | | | Enter the start frequency.  
  The range of frequencies is:  
  • uBR-MC16E cable interface card  
  • 5MHz—65MHz for Cisco  
  • 5MHz—42MHz for all other cable interface cards |
| End Frequency [5 - 42 MHz] | | | Enter the end frequency.  
  The range of frequencies is:  
  • uBR-MC16E cable interface card  
  • 5MHz—65MHz for Cisco  
  • 5MHz—42MHz for all other cable interface cards.  
  This field is enabled only if you choose Fix as the value in the Frequency Setting field, in the Spectrum Group. |
| Optional Configuration | Power Level [-10 - 25 dBmV] | | Enter the Power Level.  
  The valid power levels are between -10dBmV and +25dBmV. The default is 0dBmV. |
| Hop Period [5 - 300 Sec] | | | Enter the Hop period.  
  The valid range for a Hop Period (in seconds) is between 1 and 3600. The default for Advanced Spectrum Management is 25 seconds. For all others, the default is 300 seconds.  
  This field is enabled only if you choose Add as the value in the Action field, in the Spectrum Group. |
| Hop Threshold [0 - 100%] | | | Enter the Hop Threshold.  
  The valid range for Hop Threshold is between 1 and 100%. The default is 20%.  
  This field is enabled only if you select Add as the value in the Action field, in the Spectrum Group. |
### Cable Trap Source Task

You can use this task to configure SNMP Traps hosts, notification, message and notification of SNMP Traps on a cable interface.

This task supports cable devices.

For more details, see Table 5-5.

You can enter the details of this task in the Trap Source Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Trap Source Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Sub-Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap Source</td>
<td>Trap Source Interface</td>
<td>Action</td>
<td>Select the required option to add, remove or make no change to a Trap Source interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trap Source</td>
<td>Select the required trap source interface from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Interface</td>
<td></td>
</tr>
</tbody>
</table>

Click **Applicable Devices** to view the devices in your selection to which this task applies.
Using System-defined Tasks

Support for Auto Smartports and Smartports

Smartport macros provide an easy way to save and share common configurations. Each Smartport macro is a group of CLI commands. When you apply a Smartport macro on a port, the CLI commands within the macro will be deployed on the port. If the command fails when applying a macro, either due to a syntax error or a configuration error, the macro continues to apply the remaining commands on the port.

Auto Smartports macros apply the configuration commands on a port automatically based on the policy definitions configured in the device.

As part of provisioning Smartports and Auto Smartports, LMS provides the following Netconfig tasks:

- **Auto Smartports** — Task applicable for Device based Netconfig flow
- **Manage Auto Smartports** — Task applicable for Port based Netconfig flow
- **Smartports** — Task applicable for Port based Netconfig flow

**Auto Smartports**

LMS allows you to configure Auto Smartports macro policies on a device.

If Auto Smartports macro is enabled at device level, all the available ports in the device will be enabled for auto smartports, except for the ports that are in disabled state.

You can use the Auto Smartports task to:

- Enable or disable auto smartports functionality at device level
- Apply or remove auto smartports policy definitions

You can enter the details of this task in the Auto Smartports Configuration dialog box.

To invoke this dialog box, see **Starting a New NetConfig Job**.

**Note**

The Auto Smartports task is available only in the Device based flow of a NetConfig job. For applying Auto Smartports task, the minimum supported version of the IOS image should be 12.2(50) SE.
The fields in the Auto Smartports Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| IOS Parameters               | Enable/Disable Auto Smartports | You can select the following actions to enable or disable auto smartports functionality at device level:  
  • Enable—Select this action to enable auto smartports  
  • Disable—Select this action to disable auto smartports |
|                              |Action                       | Enable CDP fallback                                                        |
|                              | Event trigger identifier     | Select the following event trigger identifier from the drop-down list:  
  • CISCO_PHONE_EVENT  
  • CISCO_ROUTER_EVENT  
  • CISCO_SWITCH_EVENT  
  • CISCO_WIRELESS_AP_EVENT  
  • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT |
|                              | Associated macro            | The macro associated with the event trigger identifier.  
  The field is automatically populated based on the event trigger identifier selected.  
  The following are the macros associated with the event trigger identifier:  
  • CISCO_PHONE_AUTO_SMARTPORT—Macro associated with the event trigger identifier CISCO_PHONE_EVENT  
  • CISCO_SWITCH_AUTO_SMARTPORT—Macro associated with the event trigger identifier CISCO_SWITCH_EVENT  
  • CISCO_ROUTER_AUTO_SMARTPORT—Macro associated with the event trigger identifier CISCO_ROUTER_EVENT  
  • CISCO_AP_AUTO_SMARTPORT—Macro associated with the event trigger identifier CISCO_WIRELESS_AP_EVENT  
  • CISCO_LWAP_AUTO_SMARTPORT—Macro associated with the event trigger identifier CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT |
|                              | Access VLAN                 | Enter the Access VLAN value.  
  The value entered must be greater than zero. For example, 2.  
  By default, the value for Access VLAN will be 1.  
  This field is enabled only if you have selected the following event trigger identifier:  
  • CISCO_PHONE_EVENT  
  • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT |
<table>
<thead>
<tr>
<th><strong>Group</strong></th>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice VLAN</td>
<td>Enter the Voice VLAN value.</td>
<td>The value entered must be greater than zero. For example, 1. By default, the value for Voice VLAN will be 2. This field is enabled only if you have selected the event trigger identifier CISCO_PHONE_EVENT.</td>
</tr>
</tbody>
</table>
| Native VLAN                     | Enter the Native VLAN value. | The value entered must be greater than zero. For example, 1. By default, the value for Native VLAN will be 1. This field is enabled only if you have selected the following event trigger identifier:  
  - CISCO_ROUTER_EVENT  
  - CISCO_SWITCH_EVENT  
  - CISCO_WIRELESS_AP_EVENT  
  - CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT |
| User-defined Auto Smartports macro | Action                      | You can select the following actions to apply or remove auto smartports policy:  
  - Apply—Select this action to define auto smartports policy  
  - Remove—Select this action to remove the existing auto smartports policy |
| Event trigger type              | Select the following event trigger type:  
  - Pre-defined trigger—To associate the auto smartports macro with a pre-defined event trigger.  
  - User-defined trigger—To associate the auto smartports macro with a user-defined event trigger. |
| Event trigger identifier        | Select the following event trigger identifier from the drop-down list:  
  - CISCO_PHONE_EVENT  
  - CISCO_ROUTER_EVENT  
  - CISCO_SWITCH_EVENT  
  - CISCO_WIRELESS_AP_EVENT  
  - CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT  
  This drop-down list is enabled only if you have selected the Event trigger type as Pre-defined trigger. |
| User-defined event trigger identifier | Enter the name of the event trigger identifier.  
  This field is enabled only if you have selected the Event trigger type as User-defined trigger. |
Using System-defined Tasks

<table>
<thead>
<tr>
<th>Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
|       | User defined macro input mode | Enter the auto smartports CLI commands either through CLI command interface or import from a file (.txt) that has CLI commands. You can select the following options:  
• CLI command  
• Import CLI command from the file |
|       | Macro command(s) | Enter the CLI commands. For example,  
```
if [[ $LINKUP -eq YES ]]; then
    conf t
    interface $INTERFACE
    macro description $TRIGGER
    switchport access vlan 1
    exit
end
fi
if [[ $LINKUP -eq NO ]]; then
    conf t
    interface $INTERFACE
    no macro description
    no switchport access vlan 1
    exit
end
fi
```
This field is enabled only if you have selected the User-defined macro input mode as CLI command. |
|       | Select macro command input file from the server | Files |
|       | | Click Browse and select the file (.txt) that has the CLI commands. The CLI command file (.txt) should reside in the default location:  
• On Solaris and Soft Appliance:  
/var/adm/CSCOpx/files/rme/netconfig/  
• On Windows:  
NMSROOT\files\rme\netconfig\  
Where, NMSROOT is the LMS install directory. |

<table>
<thead>
<tr>
<th>Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable Devices (Button)</td>
<td>Allows you to view the IOS devices in your selection on which you want to configure Auto Smartports macros.</td>
<td></td>
</tr>
<tr>
<td>Save (Button)</td>
<td>Saves the information you have specified.</td>
<td></td>
</tr>
<tr>
<td>Reset (Button)</td>
<td>Clears all fields and reverts to the default setting.</td>
<td></td>
</tr>
<tr>
<td>Cancel (Button)</td>
<td>Ignores your changes.</td>
<td></td>
</tr>
</tbody>
</table>
Manage Auto Smartports

You can use the Manage Auto Smartports task to enable or disable auto smartports functionality on a port.

You can enter the details of this task in the Manage Auto Smartports Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

Note

The Manage Auto Smartports task is available only in the Port based flow of a NetConfig job.

The fields in the Manage Auto Smartports Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Parameters</td>
<td>Action</td>
<td>Select the following actions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enable—Enables auto smartports functionality on the port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disable—Disables auto smartports functionality on the port.</td>
</tr>
<tr>
<td></td>
<td>Enable Auto Smartports at device level</td>
<td>Check the checkbox to enable auto smartports at a device level.</td>
</tr>
<tr>
<td></td>
<td>Enable CDP fallback</td>
<td>Check to enable CDP fallback.</td>
</tr>
<tr>
<td>Applicable Devices</td>
<td>(Button)</td>
<td>Allows you to view the IOS devices in your selection on which you want to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configure auto smartports macros.</td>
</tr>
<tr>
<td></td>
<td>Save (Button)</td>
<td>Saves the information you have specified.</td>
</tr>
<tr>
<td></td>
<td>Reset (Button)</td>
<td>Clears all fields and reverts to the default setting.</td>
</tr>
<tr>
<td></td>
<td>Cancel (Button)</td>
<td>Ignores your changes.</td>
</tr>
</tbody>
</table>

When you schedule a NetConfig job for Manage Auto Smartports task and if you have selected any of the following Failure Policies, in the Job Schedule and Options dialog box, the rollback functionality will happen only if the archived configuration contains the command `macro auto global processing [cdp-fallback].`

• Rollback device and stop
• Rollback device and continue
• Rollback job on failure
Smartports

You can use the Smartports task to apply Smartports to a port by selecting the predefined smartports macros.

You can enter the details of this task in the Smartports Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

Note

The Smartports task is available only in the Port based flow of a NetConfig job.

The fields in the Smartports Configuration dialog box are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Parameters</td>
<td>Smartport Macro</td>
<td>Select the following predefined smartport macros from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cisco-desktop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cisco-phone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cisco-switch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cisco-router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cisco-wireless</td>
</tr>
<tr>
<td></td>
<td>Access VLAN</td>
<td>Enter the Access VLAN value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value entered must be greater than zero. For example, 2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This field is enabled only if you have selected the following smartports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>macros:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cisco-desktop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cisco-phone</td>
</tr>
<tr>
<td></td>
<td>Voice VLAN</td>
<td>Enter the Voice VLAN value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value entered must be greater than zero. For example, 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This field is enabled only if you have selected cisco-phone as the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>smartports macro</td>
</tr>
<tr>
<td></td>
<td>Native VLAN</td>
<td>Enter the Native VLAN value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value entered must be greater than zero. For example, 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This field is enabled only if you have selected the following smartports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>macros:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cisco-switch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cisco-router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cisco-wireless</td>
</tr>
<tr>
<td></td>
<td>Applicable Devices (Button)</td>
<td>Allows you to view the IOS devices in your selection on which you want to configure auto smartports macros.</td>
</tr>
</tbody>
</table>
When you schedule a NetConfig job for Smartports task and if you have selected any of the following Failure Policies, in the Job Schedule and Options dialog box, the rollback functionality will not happen.

- Rollback device and stop
- Rollback device and continue
- Rollback job on failure

**PoE Task**

You can use the PoE task to configure Power and Power Policing in ports. Power Policing allows you to turn off power while generating syslogs. This is needed if the real-time power consumption exceeds the maximum power allocation on the port.

Power policing and ePoE are supported only on Catalyst 3750-E and Catalyst 3560-E switches with PoE ports.

You can enter the details of this task in the PoE Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

**Note**

The PoE task is available only in the Port based flow of a NetConfig job.

The fields in the PoE Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Management</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Power Mode | Select the following power modes:  
- Auto  
- Static  
- Disable  
If you select Disable as the power mode, the detection and power for the inline power capable interface will be disabled. |
| Max Power | Enter the maximum power for the selected mode.  
Maximum power can be up to 20,000 milliwatts. |
Using System-defined Tasks

Chapter 5  Making and Deploying Configuration Changes Using NetConfig

#### Using System-defined Tasks

You can generate PoE MAX Power Violation syslog report for this task. See *Reports Management with Cisco Prime LAN Management Solution 4.2* for more information.

### Catalyst Integrated Security Features

You can use the Catalyst Integrated Security Features task to configure Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard and Security Violation on ports.

The Catalyst Integrated Security Feature is supported only on Catalyst 2960, 3560, 3560E, 3750, 3750E switches.

You can enter the details of this task in the Catalyst Integrated Security Features Configuration dialog box. To invoke this dialog box, see *Starting a New NetConfig Job*.

**Note**

The Catalyst Integrated Security Features task is available only in the Port based flow of a NetConfig job.

The fields in the Catalyst Integrated Security Features Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Parameters</td>
<td></td>
</tr>
<tr>
<td>Port Security</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Select the following actions to limit the number of MAC addresses that can be learned through a port:</td>
</tr>
<tr>
<td></td>
<td>• Change</td>
</tr>
<tr>
<td></td>
<td>• Disable</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Maximum Number of MAC Addresses | Enter the number of MAC addresses.  
This field is enabled only if the action Change is selected.

### Security Violation
Select the following security violation modes for a port:
- **Protect**—Packets with unknown source addresses are dropped until the sufficient number of secure MAC addresses drops below the maximum value.
- **Restrict**—Packets with unknown source addresses are dropped until the sufficient number of secure MAC addresses drops below the maximum value, and the Security Violation counter is incremented.
- **Shutdown**—Interface immediately goes into an error-disabled state and sends an SNMP trap notification.
- **Disable**—Disables security violations

### DHCP Snooping
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global DHCP Snooping</td>
<td>Enables or disables DHCP Snooping globally.</td>
</tr>
<tr>
<td>VLAN DHCP Snooping</td>
<td>Enables or disables DHCP Snooping only on VLAN.</td>
</tr>
</tbody>
</table>
| VLAN ID or VLAN Range | Enter the VLAN ID or VLAN range or both.  
For example,  
- You can enter the VLAN ID as 10.  
- You can enter the VLAN range separated by a space or a hyphen as 1 4, 4-8.  
- You can enter both VLAN ID and VLAN range as 10, 4-8. |

### Port Trusting
Configure port trusting by selecting the following options:
- **Trust**
- **UnTrust**

### DHCP Messages Per Second
Configure the DHCP messages rate limit for the ports and enter the number of DHCP messages that can be received per second.

### Dynamic ARP Inspection
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Dynamic ARP Inspection</td>
<td>Enables or disables Dynamic ARP Inspection only on VLAN.</td>
</tr>
</tbody>
</table>
| VLAN ID or VLAN Range | Enter the VLAN ID or VLAN range or both.  
For example,  
- You can enter the VLAN ID as 10.  
- You can enter the VLAN range separated by a space or a hyphen as 1 4, 4-8.  
You can enter both VLAN ID and VLAN range as 10, 4-8. |

### Port Trusting
Configure port trusting by selecting the following options:
- **Trust**
- **UnTrust**

### ARP Messages Per Second
Configure the ARP messages rate limit for the ports and enter the number of ARP request messages that can be received per second.

### IP Source Guard
Using System-defined Tasks

Chapter 5  Making and Deploying Configuration Changes Using NetConfig

Using System-defined Tasks

You can generate a Syslog Analyzer report for this task, which lists only the Syslogs that are specific to Catalyst Integrated Security Features. See Reports Management with Cisco Prime LAN Management Solution 4.2 for more information.

EEM Environmental Variables Task

You can use this task to configure EEM Environmental Variables (that are used by the TCL script) on Cisco Catalyst 6500, 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches.

You can enter the details for this task in the Environmental Variables Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

The fields in the EEM Environmental Variables Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Select either:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong> - to add one or more variables.</td>
</tr>
<tr>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remove</strong> - to remove one or more variables.</td>
</tr>
<tr>
<td>Variable Name</td>
<td>Enter the name for the variable.</td>
</tr>
<tr>
<td>Example: my_counter</td>
<td>You can create a maximum of five variables at a time. If you want to create more variables, create another instance by clicking Add Instance Button.</td>
</tr>
</tbody>
</table>
You can use this task to configure EEM Scripts or Applets on Cisco Catalyst 6500, 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches.

You can enter the details for this task in the Embedded Event Manager Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

The fields in the Embedded Event Manager Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
<td>Enter the value for the variable.</td>
</tr>
<tr>
<td>Example: 15</td>
<td>Now the variable my_counter will have the value 15.</td>
</tr>
<tr>
<td><strong>Applicable Devices</strong></td>
<td>Allows you to view the IOS devices in your selection, to which these variables would be applied to.</td>
</tr>
<tr>
<td><strong>Save</strong></td>
<td>Saves the information you have specified.</td>
</tr>
<tr>
<td><strong>Reset</strong></td>
<td>Clears all fields and reverts to the default setting.</td>
</tr>
<tr>
<td><strong>Cancel</strong></td>
<td>Ignores your changes.</td>
</tr>
</tbody>
</table>

**Embedded Event Manager Task**

You can use this task to configure EEM Scripts or Applets on Cisco Catalyst 6500, 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches.

You can enter the details for this task in the Embedded Event Manager Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

The fields in the Embedded Event Manager Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IOS Parameters</strong></td>
<td></td>
</tr>
<tr>
<td><strong>EEM Configuration</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Policy Type</strong></td>
<td>Select either Script or Applet as the policy.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Select Register or Unregister to register or unregister a script or applet.</td>
</tr>
</tbody>
</table>
Using System-defined Tasks

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Directory Options</td>
<td></td>
</tr>
<tr>
<td>Create New Directory</td>
<td>Check this option if you want to create a new directory on the device to copy the applet or script. If you select this checkbox, the input given in the Directory Name textbox is used to create a new directory. This option is activated only when the Script Policy and Register Action options are selected.</td>
</tr>
<tr>
<td>Directory Name</td>
<td>Enter the absolute path of the directory where the file needs to be placed on the device. Example: <code>disk0:/Testing</code> Here a new directory Testing is created in the device under disk0 Partition. Ensure that the selected directory has enough space before the script files are copied. This option is activated only when the Script Policy and Register Action options are selected.</td>
</tr>
<tr>
<td>Upload Script/Applet files from Server</td>
<td></td>
</tr>
<tr>
<td>Files</td>
<td>Use this option to either:</td>
</tr>
<tr>
<td>• Enter the file location to upload the scripts to deploy on the device. Ensure that you enter the absolute path along with the filename. You can specify multiple filenames separated by commas. Or • Browse to the directory and select one or more scripts to deploy on the device. – Use CTRL to select more than one file. – Use Browse to browse to the directory. You cannot combine tcl files and applet files in a single NetConfig task.</td>
<td></td>
</tr>
<tr>
<td>Applicable Devices</td>
<td>Allows you to view the IOS devices in your selection, to which the scripts or applets apply.</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the information you have specified.</td>
</tr>
<tr>
<td>Reset</td>
<td>Clears all fields and reverts to the default setting.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Ignores your changes.</td>
</tr>
</tbody>
</table>

For more information, see *Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.2*.

**EnergyWise Configuration Task**

You can use the EnergyWise Configuration Task to configure EnergyWise on devices.

You can enter the details of this task in the EnergyWise dialog box. To invoke this dialog box, see **Starting a New NetConfig Job**.

**Note** The EnergyWise Configuration task is available only in the Device based flow of a NetConfig job.
The fields in the EnergyWise Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IOS Parameters</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Enable/Disable EnergyWise</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Configure EnergyWise         | Select the following options to enable or disable EnergyWise configuration on the devices:  
  - **Enable**—To enable EnergyWise configuration on the devices  
  - **Disable**—To disable EnergyWise configuration on the devices  
  - **No Change**—To make no change to the EnergyWise configuration on the device. |
| **Domain Configuration**     |                                                                              |
| EnergyWise Entity Domain     | Enter an EnergyWise domain name. For example, myDomain  
  This field is disabled if you have selected **Disable** as the Configure EnergyWise option. |
| EnergyWise Entity Secret     | Enter the EnergyWise Entity secret name.  
  This field is disabled if you have selected **Disable** as the Configure EnergyWise option. |
| **Advanced Configuration**   |                                                                              |
| Entity Importance (1-100)    | Enter the value for EnergyWise Importance.  
  Importance allows you to differentiate among devices in the domain. The value for Importance ranges from 1 to 100, where a value of 1 is the lowest and a value of 100 is the highest.  
  This field is disabled if you have selected **Disable** as the Configure EnergyWise option. |
| Entity Keywords (comma separated) | Enter the keyword. For example, myLobbyphones.  
  You can set Keyword to identify a specific device or group of devices. You can use these keywords to query the devices for specific data.  
  This field is disabled if you have selected **Disable** as the Configure EnergyWise option. |
| Entity Role                  | Enter the role for a specific device or device group access.  
  This field is disabled if you have selected **Disable** as the Configure EnergyWise option. |
EnergyWise Level

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnergyWise Level</td>
<td>Select the following EnergyWise level to be configured on the devices:</td>
</tr>
<tr>
<td></td>
<td>• 0 - Shut</td>
</tr>
<tr>
<td></td>
<td>• 1 - Hibernate</td>
</tr>
<tr>
<td></td>
<td>• 2 - Sleep</td>
</tr>
<tr>
<td></td>
<td>• 3 – Standby</td>
</tr>
<tr>
<td></td>
<td>• 4 – Ready</td>
</tr>
<tr>
<td></td>
<td>• 5 – Low</td>
</tr>
<tr>
<td></td>
<td>• 6 – Frugal</td>
</tr>
<tr>
<td></td>
<td>• 7 – Medium</td>
</tr>
<tr>
<td></td>
<td>• 8 – Reduced</td>
</tr>
<tr>
<td></td>
<td>• 9 – High</td>
</tr>
<tr>
<td></td>
<td>• 10 - Full</td>
</tr>
<tr>
<td></td>
<td>This drop-down list is disabled if you have selected <strong>Disable</strong> as the Configure EnergyWise option.</td>
</tr>
</tbody>
</table>

Management Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnergyWise Port Number</td>
<td>Enter the EnergyWise port number that sends and receives queries.</td>
</tr>
<tr>
<td></td>
<td>The range is from 1 to 65000. The default is 43440.</td>
</tr>
<tr>
<td></td>
<td>After entering the EnergyWise port number, you must select either:</td>
</tr>
<tr>
<td></td>
<td>• Interface—Select <strong>Interface</strong> and specify the EnergyWise Interface ID.</td>
</tr>
<tr>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>• IP Address—Select <strong>IP Address</strong> and specify the EnergyWise IP Address.</td>
</tr>
<tr>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>• Use Mgmt IP Address of Devices—Select to use the management IP Address of</td>
</tr>
<tr>
<td></td>
<td>devices added in the DCR.</td>
</tr>
<tr>
<td>EnergyWise Interface</td>
<td>Specify the EnergyWise Interface ID from which the EnergyWise messages are sent.</td>
</tr>
<tr>
<td></td>
<td>For example, FastEthernet0/2.</td>
</tr>
<tr>
<td>EnergyWise IP Address</td>
<td>Specify the EnergyWise IP Address from which the EnergyWise messages are sent.</td>
</tr>
<tr>
<td>Applicable Devices</td>
<td>Allows you to view the IOS devices in your selection on which you want to configure EnergyWise.</td>
</tr>
<tr>
<td>(Button)</td>
<td></td>
</tr>
<tr>
<td>Save (Button)</td>
<td>Saves the information you have specified.</td>
</tr>
<tr>
<td>Reset (Button)</td>
<td>Clears all fields and reverts to the default setting.</td>
</tr>
<tr>
<td>Cancel (Button)</td>
<td>Ignores your changes.</td>
</tr>
</tbody>
</table>

For more information, see *Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.2*. 
EnergyWise Parameters Task

You can use the EnergyWise Parameters task to configure EnergyWise on ports. You can enter the details of this task in the EnergyWise Parameters Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

Note

The EnergyWise Parameters task is available only in the Port based flow of a NetConfig job.

The fields in the EnergyWise Parameters Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure EnergyWise Parameters</td>
<td></td>
</tr>
<tr>
<td>Entity Keywords (comma separated)</td>
<td>Enter the keyword name. Keywords can be set to identify a specific interface or group of interfaces. For example, lab1</td>
</tr>
<tr>
<td>Entity Role</td>
<td>Enter the role for a specific device or device group access. For example, lobbyaccess</td>
</tr>
<tr>
<td>Entity Importance (1-100)</td>
<td>Enter the value for Importance. Allows you to differentiate among devices in the domain. The value for Importance ranges from 1 to 100, where a value of 1 is the lowest and a value of 100 is the highest.</td>
</tr>
<tr>
<td>Applicable Devices (Button)</td>
<td>Allows you to view the IOS devices in your selection on which you want to configure EnergyWise.</td>
</tr>
<tr>
<td>Save (Button)</td>
<td>Saves the information that you have specified.</td>
</tr>
<tr>
<td>Reset (Button)</td>
<td>Clears all fields and reverts to the default setting.</td>
</tr>
<tr>
<td>Cancel (Button)</td>
<td>Ignores your changes.</td>
</tr>
</tbody>
</table>

EnergyWise Events Task

You can use the EnergyWise Events task to configure EnergyWise events on ports of EnergyWise supported devices.

You can enter the details of this task in the EnergyWise Events Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

Note

The EnergyWise Events task is available only in the Port-based flow of a NetConfig job.
Using System-defined Tasks

Chapter 5  Making and Deploying Configuration Changes Using NetConfig

The fields in the EnergyWise Events Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IOS Parameters</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Action</td>
<td>Select the following actions to enable or disable EnergyWise events on ports:</td>
</tr>
<tr>
<td></td>
<td>• Enable—To enable EnergyWise events configurations on ports</td>
</tr>
<tr>
<td></td>
<td>• Disable—To disable EnergyWise events configurations on ports</td>
</tr>
<tr>
<td>EnergyWise Level</td>
<td>Select the following EnergyWise event levels:</td>
</tr>
<tr>
<td></td>
<td>• 0 - Shut</td>
</tr>
<tr>
<td></td>
<td>• 1 - Hibernate</td>
</tr>
<tr>
<td></td>
<td>• 2 - Sleep</td>
</tr>
<tr>
<td></td>
<td>• 3 – Standby</td>
</tr>
<tr>
<td></td>
<td>• 4 – Ready</td>
</tr>
<tr>
<td></td>
<td>• 5 – Low</td>
</tr>
<tr>
<td></td>
<td>• 6 – Frugal</td>
</tr>
<tr>
<td></td>
<td>• 7 – Medium</td>
</tr>
<tr>
<td></td>
<td>• 8 – Reduced</td>
</tr>
<tr>
<td></td>
<td>• 9 – High</td>
</tr>
<tr>
<td></td>
<td>• 10 - Full</td>
</tr>
<tr>
<td></td>
<td>This drop-down list is disabled if you have selected Disable as the Action.</td>
</tr>
<tr>
<td><strong>Recurrence</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Configure Recurrence</td>
<td>Check the checkbox to configure event recurrence level.</td>
</tr>
<tr>
<td>level</td>
<td>Enter the value for Importance. Allows you to differentiate among devices in</td>
</tr>
<tr>
<td></td>
<td>the domain. The value for Importance ranges from 1 to 100, where a value of</td>
</tr>
<tr>
<td></td>
<td>1 is the lowest and a value of 100 is the highest.</td>
</tr>
<tr>
<td>Importance (1-100)</td>
<td>Allow you to configure the event recurrence interval.</td>
</tr>
<tr>
<td>Hour [00 - 23]</td>
<td>Select the hour interval to configure the event recurrence interval.</td>
</tr>
<tr>
<td></td>
<td>You can select the hourly time between 00 and 23 hours.</td>
</tr>
<tr>
<td>Minute [00 - 59]</td>
<td>Select the minute interval to configure event recurrence interval.</td>
</tr>
<tr>
<td></td>
<td>You can select the minute interval between 00 and 59 minutes</td>
</tr>
<tr>
<td>Month [1 - 12]</td>
<td>Enter the month in number format, separated by comma.</td>
</tr>
<tr>
<td></td>
<td>You can enter the value for one month [3], or for a range of months [7-9],</td>
</tr>
<tr>
<td></td>
<td>or both [3, 7-9].</td>
</tr>
<tr>
<td></td>
<td>If this field is left blank, the Netconfig job considers the value as applied</td>
</tr>
<tr>
<td></td>
<td>for all the months [1-12].</td>
</tr>
<tr>
<td>Day of the Month [1 - 31]</td>
<td>Enter the day of the month in number format, separated by comma.</td>
</tr>
<tr>
<td></td>
<td>You can enter the value for one day [20], or for range of days [15-19], or</td>
</tr>
<tr>
<td></td>
<td>both [10, 15-20].</td>
</tr>
<tr>
<td></td>
<td>If this field is left blank, the Netconfig job considers the value applied</td>
</tr>
<tr>
<td></td>
<td>for all the days of a month [1-31].</td>
</tr>
</tbody>
</table>
### GOLD Boot Level Task

You can use this task to configure Boot Level Diagnostics tests on the following device category:

- Cisco Catalyst 6500 devices

You can enter the details for this task in the GOLD Boot Level Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

The fields in the GOLD Boot Level Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Select either <strong>Enable</strong> to enable the actions or <strong>Disable</strong> to disable the actions</td>
</tr>
<tr>
<td>Level</td>
<td>Select either <strong>Complete</strong> to set the boot level to Complete or <strong>Minimal</strong> to set the boot level to Minimal</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the information you have specified.</td>
</tr>
<tr>
<td>Reset</td>
<td>Clears all fields and reverts to the default setting.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Ignores your changes.</td>
</tr>
</tbody>
</table>

For more information, see *Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.2*. 

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day of the Week</td>
<td>Select the day of the week by checking the checkbox. If all the days of the week are left unchecked, the Netconfig job considers the value being checked for all the days of a week [Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday].</td>
</tr>
<tr>
<td>Time Range</td>
<td>Enter the EnergyWise IOS time-range configured in the Global Config mode. For example, if you have configured the time range “Periodic Friday 07:00 to 20:00” to a time-range name “Friday” in the Global Config mode in the EnergyWise IOS, you must enter “Friday” in this Time Range field. This option is applicable for EnergyWise enabled devices running EnergyWise 2.0 software image.</td>
</tr>
<tr>
<td>Applicable Devices</td>
<td>Allows you to view the IOS devices in your selection.</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the information that you have specified.</td>
</tr>
<tr>
<td>Reset</td>
<td>Clears all fields and reverts to the default setting.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Ignores your changes.</td>
</tr>
</tbody>
</table>
GOLD Monitoring Test Task

You can use this task to configure GOLD Monitoring tests on the following device categories:

- Cisco Catalyst 6500 IOS switches
- Cisco Catalyst 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E Switches

You can enter the details of this task in the GOLD Monitoring Tests Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

The fields in the GOLD Monitoring Test Configuration dialog box are:

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOLD Monitoring Test Configuration</td>
<td>Select any of the following:</td>
</tr>
<tr>
<td>Action</td>
<td>• <strong>Add Interval</strong> - To add an interval</td>
</tr>
<tr>
<td></td>
<td>• <strong>No Interval</strong> - To not add an interval</td>
</tr>
<tr>
<td></td>
<td>• <strong>No Change</strong> - To make no change</td>
</tr>
<tr>
<td>Enter Vendor Type or Name</td>
<td>Enter the Vendor type or Module Name. You can enter one or more comma separated module names. Example: cevCat6kVsS72010G This is a mandatory field and is available only if you select Cisco Catalyst 6500 devices.</td>
</tr>
<tr>
<td>Enter Switch ID</td>
<td>Enter the Switch ID. You can enter a single switch ID or a number of switch IDs separated by comma. Example 1: Enter 2 if you want to include switch with ID 2. Example 2: Enter 3, 6 if you want to include switches with IDs 3 and 6. This is a mandatory field and is available only if you select Cisco Catalyst 2900XL, 2970, 2960, 3550, 3560, 3750, or 3750E stack switches.</td>
</tr>
<tr>
<td>Enable/Disable Health Diagnostics</td>
<td>Select any of the following:</td>
</tr>
<tr>
<td>Action</td>
<td>• <strong>Enable</strong> - To start the Health Monitoring tests</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable</strong> - To stop the running Health Monitoring tests. The tests once stopped, will not start again until the Action is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No Change</strong> - No change to Action</td>
</tr>
<tr>
<td>Test Details</td>
<td>Allows you to configure all diagnostic tests.</td>
</tr>
<tr>
<td>All</td>
<td>Allows you to manually enter the test names.</td>
</tr>
<tr>
<td>Enter Testnames</td>
<td>Enter one or more test names separated by comma.</td>
</tr>
<tr>
<td></td>
<td>This option is activated only if the Enable Action is selected.</td>
</tr>
</tbody>
</table>
Chapter 5      Making and Deploying Configuration Changes Using NetConfig

Using System-defined Tasks

You can use this task to configure GOLD Health Monitoring tests on Cisco Catalyst 6500 IOS switches device categories.

This task is available only for the Module-based netconfig job wizard.

You can enter the details of this task in the Gold Health Monitoring Test Configuration dialog box. To invoke this dialog box, see Create a NetConfig Job based on Module or Port.
The fields in the GOLD Health Monitoring Test Configuration dialog box are:

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GOLD Health Monitoring Test Configuration</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Configuring Health-Monitoring Diagnostics for Cat6k Devices</strong></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Select any of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Run Test</strong> - To run a test</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add Test</strong> - To add a test</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remove Test</strong> - To remove a test</td>
</tr>
<tr>
<td><strong>Test Details</strong></td>
<td></td>
</tr>
<tr>
<td>All</td>
<td>Allows you to configure all diagnostic tests.</td>
</tr>
<tr>
<td>Pre-defined</td>
<td>Allows you to select the following pre-defined tests:</td>
</tr>
<tr>
<td></td>
<td>• TestLoopback</td>
</tr>
<tr>
<td></td>
<td>• TestNetflowInlineRewrite</td>
</tr>
<tr>
<td></td>
<td>• TestEobcStressPing</td>
</tr>
<tr>
<td></td>
<td>• TestFirmwareDiagStatus</td>
</tr>
<tr>
<td></td>
<td>• TestAsicSync</td>
</tr>
<tr>
<td>Enter Testnames</td>
<td>Allows you to manually enter the test names.</td>
</tr>
<tr>
<td></td>
<td>Enter one or more test names separated by comma.</td>
</tr>
<tr>
<td>Range</td>
<td>Allows you to enter a range for tests to be run.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Enter <strong>2-8</strong> if you want to run tests with IDs from 2 to 8.</td>
</tr>
<tr>
<td><strong>Configure Health Monitoring Interval</strong></td>
<td></td>
</tr>
<tr>
<td>No. of Days</td>
<td>Enter the number of days till which you require the tests to be run on the devices.</td>
</tr>
<tr>
<td></td>
<td>The number of days can be any value between 0 - 20.</td>
</tr>
<tr>
<td></td>
<td>The default value is one day.</td>
</tr>
<tr>
<td></td>
<td>This field is enabled only if you have selected <strong>Add Test</strong>.</td>
</tr>
<tr>
<td>Hours</td>
<td>Select the hour frequency at which the tests should be run. You can enter any value between 00 and 23 for the hour.</td>
</tr>
<tr>
<td></td>
<td>This field is enabled only if you have selected <strong>Add Test</strong>.</td>
</tr>
<tr>
<td>Minutes</td>
<td>Select the minute frequency at which the tests should be run. You can enter any value between between 00 and 59 for the minute.</td>
</tr>
<tr>
<td></td>
<td>This field is enabled only if you have selected <strong>Add Test</strong>.</td>
</tr>
<tr>
<td>Seconds</td>
<td>Enter the seconds frequency at which the tests should be run. You can enter any value between 00 and 59 for the second.</td>
</tr>
<tr>
<td></td>
<td>This field is enabled only if you have selected <strong>Add Test</strong>.</td>
</tr>
<tr>
<td>Milliseconds</td>
<td>Enter the millisecond frequency at which the tests should be run. You can enter any value between 0 and 999 for the millisecond.</td>
</tr>
<tr>
<td></td>
<td>This field is enabled only if you have selected <strong>Add Test</strong>.</td>
</tr>
</tbody>
</table>
### SRE Operation Task

You can use the SRE Operation task to perform the following operations in the service modules of SRE supported devices:

- Install application in service modules
- Uninstall application from service modules
- Understand:
  - Status of the service module
  - Application that is running on the module
  - Status of the current installation in the service module
  - Status of uninstallation in the service module
- Stop the installation on a set of service modules in a SRE device
- Reset service modules in a SRE device
- Shutdown the set of service modules in a SRE device

You can enter the details of the SRE Operation task in the SRE Operation Configuration dialog box. To invoke this dialog box, see Create a NetConfig Job based on Module or Port.

### Table: Panes and Description

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply the Monitoring Test</strong></td>
<td></td>
</tr>
<tr>
<td>Run the above monitoring test case</td>
<td>Check the checkbox to run the above monitoring test case.</td>
</tr>
<tr>
<td>Configure Syslog</td>
<td>Check the checkbox and select the following options to enable or disable Syslog:</td>
</tr>
<tr>
<td></td>
<td>• Enable</td>
</tr>
<tr>
<td></td>
<td>• Disable</td>
</tr>
<tr>
<td>Applicable Devices (Button)</td>
<td>Allows you to view the IOS devices in your selection that you want to monitor with GOLD Health Monitoring Tests.</td>
</tr>
<tr>
<td>Save (Button)</td>
<td>Saves the information you have specified.</td>
</tr>
<tr>
<td>Reset (Button)</td>
<td>Clears all fields and reverts to the default setting.</td>
</tr>
<tr>
<td>Cancel (Button)</td>
<td>Ignores your changes.</td>
</tr>
</tbody>
</table>

For more information, see *Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.2*. 

---

For more information, see Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.2.
The fields in the SRE Operation Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td>Select the following actions:</td>
</tr>
<tr>
<td></td>
<td>• Install—Install application in service modules.</td>
</tr>
<tr>
<td></td>
<td>• Uninstall—Uninstall application from service modules.</td>
</tr>
<tr>
<td></td>
<td>• Status—Displays the following:</td>
</tr>
<tr>
<td></td>
<td>– Status of the service module</td>
</tr>
<tr>
<td></td>
<td>– The applicable running on the module</td>
</tr>
<tr>
<td></td>
<td>– Status of the installation and uninstallation being performed in the</td>
</tr>
<tr>
<td></td>
<td>service module</td>
</tr>
<tr>
<td></td>
<td>• Abort—Stop installation on a set of service modules in a SRE device.</td>
</tr>
<tr>
<td></td>
<td>• Shutdown—Shutdown the set of service modules in a SRE device</td>
</tr>
<tr>
<td></td>
<td>• Reset—Reset service modules in a SRE device.</td>
</tr>
<tr>
<td><strong>Script Name [Optional]</strong></td>
<td>Name of the script file that should be picked up during installation.</td>
</tr>
<tr>
<td></td>
<td>This field is optional and is enabled only if the Install action is selected.</td>
</tr>
<tr>
<td><strong>Argument to the Script</strong></td>
<td>String argument passed to the script.</td>
</tr>
<tr>
<td>[Optional]</td>
<td>The string argument must be entered within quotes. For example, “argument”.</td>
</tr>
<tr>
<td></td>
<td>This field is optional and enabled only if Install action is selected.</td>
</tr>
<tr>
<td><strong>URL of the installation</strong></td>
<td>URL path of the package from where the device needs to download the image</td>
</tr>
<tr>
<td>source directory</td>
<td>for installation.</td>
</tr>
<tr>
<td></td>
<td>For example, ftp://180.180.180.80/nibbler/012609/pkg1/foundation.sme.1.4.40.18.pkg</td>
</tr>
<tr>
<td></td>
<td>This is a mandatory field. If this field is blank, an error message appears.</td>
</tr>
<tr>
<td><strong>Applicable Devices</strong></td>
<td>Allows you to view the devices in your selection that you want to configure</td>
</tr>
<tr>
<td></td>
<td>SRE operation.</td>
</tr>
<tr>
<td><strong>Save</strong></td>
<td>Saves the information you have specified.</td>
</tr>
<tr>
<td>(Button)</td>
<td></td>
</tr>
<tr>
<td><strong>Reset</strong></td>
<td>Clears all fields and reverts to the default setting.</td>
</tr>
<tr>
<td>(Button)</td>
<td></td>
</tr>
<tr>
<td><strong>Cancel</strong></td>
<td>Ignores your changes.</td>
</tr>
<tr>
<td>(Button)</td>
<td></td>
</tr>
</tbody>
</table>

cwcli netconfig

This command is described in the cwcli framework chapter. For details see Running the cwcli netconfig Command.
Use Case: Using NetConfig Templates to change Configurations for many Devices

Case
As a Network Administrator, you would want to change configuration for a set of devices in few simple steps.

Solution
You can use NetConfig to change the configurations of many devices in one step. You can select the devices and the corresponding system-defined or user-defined tasks and schedule a NetConfig job.

Let us say, you want to change the Local Username and Telnet password for a few devices. To perform this:

Step 1
Go to Configuration > Configuration > NetConfig.
The Devices And Tasks dialog box appears.

Step 2
Select the required devices from the Device Selector.

Step 3
Select the Local Username and Telnet Password tasks from the Task Selector.

NetConfig Tasks are also referred to as NetConfig templates.

Step 4
Click Next.
From your selection, only the tasks that are applicable to at least one device that you have selected, appear here. If the task that you have selected do not apply to the categories of any of the devices that you have selected, it will not be displayed in the Applicable Tasks pane.

Step 5
Select a task and click Add to create an instance for the task.

Step 6
After creating the instances, select the Local Username_1 instance and click View CLI button to view the CLI commands that will be deployed onto the applicable and non applicable devices.
Alternatively, you can click Edit to edit the selected instance or click Delete to delete an instance. You can only delete one instance at a time.

Step 7
Click Next.
The Job Schedule and Options page appears.

Step 8
Provide the required information in the Job Schedule and Options dialog box and click Finish.
The Job Work Order screen appears.

Step 9
Click Finish.
A notification indicating the successful creation of a job appears.

Example
Job 1007 was created successfully.

The NetConfig job will be executed at the scheduled date and time. The Local Username Configuration and Telnet Password Configuration changes effected will be deployed on the selected applicable devices.

To know the status of the job scheduled, go to Configuration > Configuration > NetConfig > NetConfig Jobs.
cwcli netconfig
Archiving Configurations and Managing them using Configuration Archive

Configuration Archive maintains an active archive of the configuration of devices managed by LMS. It enables you to perform the following tasks:

- Fetch, archive, and deploy device configurations
- Search and generate reports on archived data
- Compare and label configurations, compare configurations with a baseline, and check for compliance.

You can also perform some of the Configuration Archive tasks using command line utility `cwcli config`.

You can also export the configuration data using the `cwcli export config` command.

**Note**
Device configuration archive file size should be less than or equal to 2.5 MB.

See CLI Utilities for further details on `cwcli config` and `cwcli export config` commands.

This chapter gives information on performing Configuration Archive tasks (see Performing Configuration Archive Tasks for details).

This chapter contains:

- Performing Configuration Archive Tasks
- Checking Configuration Archival Status
- Scheduling Sync Archive Job
- Using the Config Fetch Protocol Usage Report
- Generating an Out-of-Sync Report
- Scheduling Sync on Device Job
- Using the Configuration Version Tree
- Understanding the Config Viewer Window
- Viewing the Configuration Version Summary
Performing Configuration Archive Tasks

Configuration Archive allows you to:

- **Check archival status**
  You can check the overall status of the configuration archive (For example, Successful, Partially Successful, etc.).
  See [Checking Configuration Archival Status](#) for further details.

- **Update the archive**
  In addition to scheduling configuration archive update, you can also update the archive manually.
  This ensures that you have the latest configurations.
  See [Scheduling Sync Archive Job](#) for more details. To define the Configuration Collection Settings, see [Administration of Cisco Prime LAN Management Solution 4.2](#).

- **Determine Configuration Protocol usage details**
  You can view the protocol usage details for successful configuration fetches for devices. You can also change the transport protocol order after analyzing the protocol usage trends.
  See [Using the Config Fetch Protocol Usage Report](#) for more details.

- **Determine out-of-sync configuration files**
  You can list the devices for which running configurations are out-of-sync- with the startup configuration.
  See [Generating an Out-of-Sync Report](#) and [Scheduling Sync on Device Job](#) for further details.

- **View Version Tree**
  You can view all configuration versions of selected devices in the form of a graphical display.
  See [Using the Configuration Version Tree](#) for further details.

- **View Version Summary**
  You can view the latest three archived configurations for selected devices. It also has a link to view a particular configuration running on the device and to generate differences between versions in the archive.
  See [Viewing the Configuration Version Summary](#) for further details.

- **Search for device configuration files**
  You can search the archive for configuration containing text patterns for selected devices.
  See [Using Search Archive](#) for further details.
• Create custom configuration queries (See Creating a Custom Query.)
  You can create and run custom queries that generate reports. These reports display device
  configuration files from the archive for the devices you specify. You can use custom queries while
  searching archives.
• Compare configurations
  You can compare the following:
  – Startup and running configurations
  – Running and latest archived configurations
  – Two configuration versions of the same device
  – Two configuration versions of different devices
  – Base configuration and latest version of different devices
  See Comparing Configurations for further details.
• Configuration Quick Deploy
  You can create an immediate job to deploy the version of configuration that you are viewing on the
  device. You can deploy the configuration either in the Overwrite or Merge mode. You can also use
  job-based password.
  See Configuration Quick Deploy for further details.
• Configuration Archive Job Browser
  You can see the status of your Configuration Archive jobs.
  See Using Configuration Archive Job Browser for further details.
• Label Configuration
  You can select configuration files from different managed devices and then group and label them.
  See Configuring Labels for further details.
• Set the debug mode for Configuration Archive
  You can set the debug mode for Configuration Archive feature in the Log Level Settings dialog box
  (Admin > System > Debug Settings).
  See Administration of Cisco Prime LAN Management Solution 4.2 for more details.

Checking Configuration Archival Status

After you add devices, their configurations are gathered and stored in the configuration archive. You can
check the overall status of the configuration archive (Successful, Partially Successful, and Failed). It
provides the status of the last archival attempt.

<table>
<thead>
<tr>
<th>Refresh (Icon)</th>
<th>Click on this icon to refresh the configuration archive status window.</th>
</tr>
</thead>
</table>

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required
privileges to perform this task.
To check the configuration archive status:

**Step 1**

Select **Configuration > Configuration Archive > Summary.**

The Configuration Archival Summary dialog window appears with the following information.

<table>
<thead>
<tr>
<th>Archival Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful</td>
<td>Number of devices for which all supported configurations have been fetched successfully. Click <strong>No.of Devices</strong> to see the Successful Devices Report.</td>
</tr>
<tr>
<td>Failed</td>
<td>Number of devices for which fetch of all supported configurations has failed. Click <strong>No.of Devices</strong> to see the Failed Devices Report.</td>
</tr>
<tr>
<td>Partial Successful</td>
<td>Number of devices for which fetch of any one of the supported configurations has failed. Number of Catalyst 5000 devices for which sub-modules were not pulled into archive. Only the main configuration of supervisor engine module is archived for Catalyst 5000 devices. Click <strong>No.of Devices</strong> to see the Partially Successful Devices Report.</td>
</tr>
<tr>
<td>Configuration Never Collected</td>
<td>Number of devices for which the supported configurations has never been collected. Click <strong>No.of Devices</strong> to see the Configuration Never Collected Devices Report.</td>
</tr>
</tbody>
</table>

**Step 2**

Select one or all of the Config Archival Status and click **Sync Archive** to schedule an immediate job to update the archive status.

You can check the status of your scheduled **Sync Archive** job by selecting **Configuration > Job Browsers > Configuration Archive.**

**Configuration Archival Reports**

The following are the Config Archival reports:

- Successful Devices Report
- Failed Devices Report
- Partially Successful Devices Report
- Configuration Never Collected Devices Report
Successful Devices Report

A device appears in this report if all supported configurations have been fetched successfully.

Note
These dates do not necessarily reflect when the archive was last updated.

This report contains the following information:

<table>
<thead>
<tr>
<th>Column Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.</td>
</tr>
<tr>
<td>Config Type</td>
<td>Defines the type of configuration PRIMARY, SECONDARY, or VLAN.</td>
</tr>
<tr>
<td></td>
<td>• PRIMARY/SECONDARY—Contains the Running and Startup configuration files information.</td>
</tr>
<tr>
<td></td>
<td>• VLAN—Contains running vlan.dat configuration file information. This config type does not contain Startup configuration file information.</td>
</tr>
<tr>
<td></td>
<td>For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.</td>
</tr>
<tr>
<td>File Type</td>
<td>Defines the configuration file type as either Running or Startup configuration.</td>
</tr>
<tr>
<td>Accessed At</td>
<td>Date and time at which LMS pulled running configuration from device in an attempt to archive. The configuration is archived only if there has been a change.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the archival status.</td>
</tr>
</tbody>
</table>

Failed Devices Report

A device appears in this report if fetch for all of the supported configurations has failed. This report also contains the reasons configuration could not be pulled.

This report contains the following information:

<table>
<thead>
<tr>
<th>Column Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.</td>
</tr>
<tr>
<td>Config Type</td>
<td>Defines the type of configuration as PRIMARY, SECONDARY, or VLAN.</td>
</tr>
<tr>
<td></td>
<td>• PRIMARY/SECONDARY—Contains information about the Running and Startup configuration files.</td>
</tr>
<tr>
<td></td>
<td>• VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information.</td>
</tr>
<tr>
<td></td>
<td>For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.</td>
</tr>
<tr>
<td>File Type</td>
<td>Defines the configuration file type as either Running or Startup configuration.</td>
</tr>
<tr>
<td>Accessed At</td>
<td>Date and time that LMS pulled running configuration from device in an attempt to archive. The configuration is archived only if there has been a change.</td>
</tr>
<tr>
<td>Description</td>
<td>Reason why LMS could not pull running and startup configuration from device.</td>
</tr>
</tbody>
</table>
If you have enabled TACACS for a device and configured custom TACACS login and passwords prompts, you may experience Telnet problems, since LMS may not recognize the prompts.

To make your prompts recognizable, you must edit the TacacsPrompts.ini file in:

- `NMSROOT\objects\cmf\data\TacacsPrompts.ini` (On Windows)
- `NMSROOT\objects\cmf\data\TacacsPrompts.ini` (On Solaris and Soft Appliance)

NMSROOT is the LMS install directory. For Solaris and Soft Appliance, it will be `/opt/CSCOpx`.

**Partially Successful Devices Report**

A device shows up in this report if fetch for any one of the supported configurations has failed.

The Partially Successful Devices report lists the Catalyst 5000 family devices for which sub-module information could not be pulled from the device. Only the main configuration of the supervisory module is archived for Catalyst 5000 devices.

This report contains the following information:

<table>
<thead>
<tr>
<th>Column Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.</td>
</tr>
<tr>
<td>Config Type</td>
<td>Defines the type of configuration as PRIMARY, SECONDARY, or VLAN.</td>
</tr>
<tr>
<td></td>
<td>- PRIMARY/SECONDARY—Contains the Running and Startup configuration files information.</td>
</tr>
<tr>
<td></td>
<td>- VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information.</td>
</tr>
<tr>
<td></td>
<td>For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.</td>
</tr>
<tr>
<td>File Type</td>
<td>Defines the configuration file type as either Running or Startup configuration.</td>
</tr>
<tr>
<td>Accessed At</td>
<td>Date and time that LMS pulled running configuration from device in an attempt to archive. The configuration is archived only if there has been a change.</td>
</tr>
<tr>
<td>Description</td>
<td>Reason why LMS could not pull running or startup configuration from device.</td>
</tr>
</tbody>
</table>

**Configuration Never Collected Devices Report**

A device appears in this report if fetch for the supported configuration has never been collected.
Chapter 6      Archiving Configurations and Managing them using Configuration Archive

Scheduling Sync Archive Job

This report contains the following information:

<table>
<thead>
<tr>
<th>Column Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.</td>
</tr>
<tr>
<td>Config Type</td>
<td>Defines the type of configuration as PRIMARY, SECONDARY, or VLAN.</td>
</tr>
<tr>
<td></td>
<td>• PRIMARY/SECONDARY—Contains the Running and Startup configuration files information.</td>
</tr>
<tr>
<td></td>
<td>• VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information.</td>
</tr>
<tr>
<td></td>
<td>For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.</td>
</tr>
<tr>
<td>File Type</td>
<td>Defines the configuration file type as either Running or Startup configuration.</td>
</tr>
<tr>
<td>Accessed At</td>
<td>Date and time that LMS pulled running configuration from device in an attempt to archive. The configuration is archived only if there has been a change.</td>
</tr>
<tr>
<td>Description</td>
<td>Reason why LMS could not pull running or startup configuration from device.</td>
</tr>
</tbody>
</table>

**Scheduling Sync Archive Job**

You can schedule a job to update the configuration archive for a selected group of devices. You have an option to poll device configuration before updating the archive and to fetch Startup configuration.

**Note**

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

**Note**

When config collection is fetched via TFTP protocol, ensure Read-Write Community String is configured in DCR under SNMP credential section.

To schedule a job to update the device configuration:

**Step 1**

Select **Configuration > Configuration Archive > Synchronization.** The Sync Archive dialog box appears.

**Step 2**

Select either:

- **Device Selector** — To schedule a job for a static set of devices.
  
  The sync archive job fails if devices are removed from the DCR. For example, a sync archive job is scheduled to run for all the devices that are part of the selected group in Device Selector. If a device, part of the selected group in Device Selector, is deleted from DCR while the job is running then the job fails for that particular device. However, the job succeeds for the remaining devices in the group, but the status of the job still remains failed.

Or

- **Group Selector** — To schedule a job for a dynamic group of devices.
The job is scheduled only for the devices that are present in the selected group at the time when the job is run. The customizable group selector for jobs evaluates static groups also as dynamic during run time.

**Step 3** Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Scheduling | You can specify when you want to run the Sync Archive job. To do this, select one of these options from the drop-down menu:  
  - Immediate—Runs this task immediately.  
  - 6-hourly—Runs this task every 6 hours, starting from the specified time.  
  - 12-hourly—Runs this task every 12 hours, starting from the specified time.  
  - Once—Runs this task once at the specified date and time.  
  - Daily—Runs daily at the specified time.  
  - Weekly—Runs weekly on the specified day of the week and at the specified time.  
  - Monthly—Runs monthly on the specified day of the month and at the specified time.  
  The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete.  
  For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed.  
  If the 10:00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3. |
| Date | You can select the date and time (hours and minutes) to schedule the job. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field. |
| Job Information | Enter a description for the job. This is mandatory. You can enter only alphanumeric characters. |
| Job Description | Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender’s address. |
| E-mail | Configuration Archive polls the device and compares the time of change currently on the device with the time of last archival of configuration to determine if configuration has changed on a device. If the polling is not supported on the device, then configuration fetch will be initiated without checking for the changes.  
  See “Understanding Configuration Retrieval and Archival” section in Administration Guide for Cisco Prime LMS 4.2 for further details on configuration polling. |
| Job Options | Configuration Archive fetches the startup configuration. |
Step 4  
Click **Submit**.

A message appears, **Job ID** is created successfully.

Where **ID** is a unique Job number.

Step 5  
Click **OK**.

You can check the status of your scheduled **Sync Archive** job by selecting **Configuration > Job Browsers > Configuration Archive**.

---

**Using the Config Fetch Protocol Usage Report**

You can view the configuration protocol usage details for successful configuration fetches using the Config Fetch Protocol Usage Report.

**Note**

View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Select **Configuration > Configuration Archive > Protocol Usage Summary** to generate a Config Fetch Protocol Usage Report.

The Config Fetch Protocol Usage Report window displays the following information:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Protocols used by LMS for configuration fetches.</td>
</tr>
<tr>
<td>Config Type</td>
<td>The Configuration types for the various protocols. The available types are:</td>
</tr>
</tbody>
</table>

- **Running** — Count of the successful running configuration fetches for each protocol
- **Startup** — Count of the successful startup configuration fetches for each protocol
- **VLAN** — Count of the successful VLAN configuration fetches for each protocol. This configuration fetch is supported by only Telnet and SSH protocols.

Click on the Count link to view a detailed report for a protocol and corresponding Config Type. The detailed report shows the list of devices which are accessed using a particular protocol and for which successful Config Fetch has happened.

**Example:**

If you click on a Count link, 20, for Telnet protocol and Running config type, a detailed report is generated with the following fields:

- **Device Name** — Name of each device.
- **Accessed At** — Date and time at which each device was accessed for Config Fetch purpose.
- **Config Type** — Configuration type for each device.
- **File Type** — Configuration file type for each device.

This detailed report shows only the devices for which Telnet has successfully fetched configurations.

You can use the export icon to export the list of devices from this detailed report to the device selector.
Generating an Out-of-Sync Report

You can generate an Out-of-Sync report for the group of devices for which running configurations are not synchronized with the startup configuration.

**Note** View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

Select Configuration > Compliance > Out-of-Sync Summary to generate an Out-of-sync report. The Startup and Running Out-Of-Sync Summary window displays the following information:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository.</td>
</tr>
<tr>
<td>Startup</td>
<td>Startup configuration of the device. This configuration is fetched from the configuration archive. Click on the displayed date to view the configuration.</td>
</tr>
<tr>
<td>Diff</td>
<td>Difference between the archived Startup and archived Running configurations. Click on the icon to see the difference between the archived Startup and archived Running configurations.</td>
</tr>
<tr>
<td>Running</td>
<td>Running configuration of the device. This configuration is fetched from the configuration archive. Click on the displayed date to see detailed information on the Running configuration.</td>
</tr>
<tr>
<td>Sync on Device (Button)</td>
<td>Use this button to schedule a Sync on device job. You can schedule a Sync on device job to copy the running configuration of a device to the startup configuration. For more information see, Scheduling Sync on Device Job.</td>
</tr>
</tbody>
</table>

Scheduling Sync on Device Job

You can schedule a Sync on device job using the Sync on Device button on Startup and Running Out-Of-Sync Summary window.

**Note** View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.
To schedule a Sync on device job:

**Step 1** Select **Configuration > Compliance > Out-of-Sync Summary**.

The Startup and Running Out-Of-Sync Summary dialog box appears.

**Step 2** Select a device.

**Step 3** Click **Sync on Device**.

The Job Schedule and Options dialog box appears.

**Step 4** Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td>You can specify when you want to run the Startup and Running Out-Of-Sync Summary report. To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td>Run Type</td>
<td>You can specify when you want to run the Startup and Running Out-Of-Sync Summary report. To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs the report immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs the report once at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>• Daily—Runs daily at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly—Runs weekly on the specified day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Monthly—Runs monthly on the specified day of the month and at the specified time.</td>
</tr>
<tr>
<td>Date</td>
<td>You can select the date and time (hours and minutes) to schedule the job. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.</td>
</tr>
<tr>
<td>Job Information</td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.</td>
</tr>
<tr>
<td>Approver Comments</td>
<td>Enter comments for the job approver. This field appears only if you have enabled Job Approval for Configuration Archive.</td>
</tr>
<tr>
<td>Maker E-Mail</td>
<td>Enter the e-mail-ID of the job creator. This is a mandatory field. This field appears only if you have enabled Job Approval for Configuration Archive.</td>
</tr>
</tbody>
</table>
Using the Configuration Version Tree

You can view all configuration versions of the selected devices in the form of a graphical display. You can also perform a configuration quick deploy for a selected device.

Note: View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To view the configuration Version Tree:

Step 1  Select Configuration > Configuration Archive > Views > Version Tree

The Device Selection dialog box appears.

Step 2  Select a device. See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to use the Device Selector.
Step 3  
Click **OK**.  
The Config Version Tree dialog box appears.

Step 4  
Click either the configuration version which is a hyper link or select the radio button for the configuration version.  
To expand the configuration version folder, click on the plus icon and select the configuration version to view the configuration.  
The Config Viewer dialog box appears. See **Understanding the Config Viewer Window** for further information.  
If you want to perform a configuration quick deploy (**Configuration Quick Deploy**), click the Deploy button.

---

**Understanding the Config Viewer Window**

The Config Viewer is a HTML-based window that displays the configurations of specified devices.  
You can specify how you want to view the contents of the configurations by selecting one of the options under Show:

- Click **Raw** to view data exactly as it appears in the configuration file.  
- Click **Processed** to view data with the commands ordered and grouped.  
The Config Viewer window contains two columns.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configlets</td>
<td>Click on any configlets to display the corresponding information. The available configlets vary from device to device; the following are examples:</td>
</tr>
<tr>
<td></td>
<td>• All—Entire contents of the configuration files.</td>
</tr>
<tr>
<td></td>
<td>• SNMP—SNMP configuration commands. For example, <code>snmp-server community public RO</code>.</td>
</tr>
<tr>
<td></td>
<td>• IP Routing—IP routing configuration commands. For example, <code>router abcd 100</code>.</td>
</tr>
<tr>
<td></td>
<td>• Interface folder—The different interface configuration commands. For example, <code>Interface Ethernet0</code> and <code>Interface TokenRing</code>.</td>
</tr>
<tr>
<td></td>
<td>• Global—Global configuration commands. For example <code>no ip address</code>.</td>
</tr>
<tr>
<td></td>
<td>• Line con 0—configuration commands for line console 0.</td>
</tr>
<tr>
<td></td>
<td>• IP—IP configuration commands. For example, <code>ip http server</code>.</td>
</tr>
<tr>
<td>Configuration file name</td>
<td>View the contents of the configuration file.</td>
</tr>
</tbody>
</table>
The buttons on the Config Viewer are:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download Config</td>
<td>Downloads the configuration file to the client machine.</td>
</tr>
<tr>
<td>(Icon)</td>
<td>This option to download the configuration file is available only in the Raw mode. The configuration file will be downloaded through the Web browser with the file name convention as <code>DeviceName-Version_Number.txt</code>. You can download the configuration file only if you have the privileges of a Network Administrator.</td>
</tr>
<tr>
<td>Export</td>
<td>Export the configuration file.</td>
</tr>
</tbody>
</table>
| (Icon)       | • If you are using the Raw mode then the exported file format is cfg. The file name convention is `DeviceName-VersionNumber.cfg`.  
|              | • If you are using the Processed mode then the exported file format is XML. The file name convention is `DeviceName-VersionNumber.xml`.  
|              | Where `DeviceName` is the device name as entered in Device and Credential Repository and `VersionNumber` is the device configuration version.  
|              | The default directory to which Configuration Archive file is exported is:  
|              | On Solaris and Soft Appliance server,  
|              | `/var/adm/CSCOpx/files/rme/dcma/configexport`  
|              | On Windows server,  
|              | `NMSROOT\files\rme\dcma\configexport`  

Note: The Credentials in the configuration file will be exposed and shown as clear text.
### Chapter 6      Archiving Configurations and Managing them using Configuration Archive

#### Understanding the Config Viewer Window

**Button** | **Description**
--- | ---
Export (continue) | To export a file:
1. Click on the icon. The Export Config File dialog box appears.
2. Enter the folder name on the LMS server. You must enter the default export directory. You cannot enter any other directory. or Browse to select a folder on the LMS server. The Server Side File Browser dialog box appears.
   a. Select a folder on the LMS server.
   b. Click **OK**. The Browse button takes you to the default directory. It does not allow you to change this default export directory.
3. Click **OK**.
   If you have exported configuration in the Raw mode, the notification message displays, *Config file exported as ExportedFolder\DeviceName-VersionNumber.cfg*. If you have exported configuration in the Processed mode, the notification message displays, *Config file exported as ExportedFolder\DeviceName-VersionNumber.XML*. Where *ExportedFolder* is the location where configuration file is exported.
4. Click **OK**.

| **Print (Icon)** | Generates a format that can be printed. |
| **Compare with previous version** | Compares configuration with previous version. When you click on this button, a new window Config Diff Viewer opens to show configurations side by side. See **Understanding the Config Diff Viewer Window** for further details. This button gets activated only if you have a previous version of the configuration. |
| **Compare with next version** | Compares configuration with next version. When you click on this button, a new window Config Diff Viewer opens to show configurations side by side. See **Understanding the Config Diff Viewer Window** for further details. This button gets activated only if you have a next version of configuration. |
| **Edit** | Launches Config Editor window. This button is active only if you are viewing the configuration version from the archive. See **Editing and Deploying Configurations Using Config Editor** for further details. |
| **Deploy** | Perform a quick configuration deploy. This button is active only if you are viewing the configuration version from the archive. See **Configuration Quick Deploy**. |
Viewing the Configuration Version Summary

You can view all archived configurations for selected devices. It also provides a link to view a particular configuration running on the device and to generate differences between versions in the archive.

You can view the last three configuration versions for each device regardless of the number of versions stored in the archive.

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To view the Config Summary, follow this workflow:

Step 1
Select Configuration > Configuration Archive > Views > Version Summary.

Step 2
Select a device. See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to use the Device Selector.

Step 3
Click OK.

The Summary of Archived Versions window appears with the information in Table 6-1.

<table>
<thead>
<tr>
<th>Table 6-1</th>
<th>Fields in the Summary of Archived Versions Window</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.</td>
</tr>
<tr>
<td>Config Type</td>
<td>Defines the type of configuration as PRIMARY, SECONDARY, or VLAN.</td>
</tr>
<tr>
<td></td>
<td>• PRIMARY/SECONDARY—Contains the Running and Startup configuration files information.</td>
</tr>
<tr>
<td></td>
<td>• VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information.</td>
</tr>
<tr>
<td></td>
<td>For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.</td>
</tr>
<tr>
<td>Startup</td>
<td>Configuration running when device was started. This configuration is fetched from the device. Click on the Startup icon to view the Startup configuration.</td>
</tr>
<tr>
<td>Diff</td>
<td>Differences between Startup and Running configurations. To view the difference between Startup and Running configurations, click on the Diff icon.</td>
</tr>
<tr>
<td>Running</td>
<td>Configuration currently running on device. Click on the Running icon to view the Running configuration. The configuration that appears, is fetched from the device. This happens if the fetched configuration is different from the latest configuration that is in the archive. Otherwise, the latest configuration from the archive appears.</td>
</tr>
<tr>
<td>Diff</td>
<td>Differences between the Running Configuration on the device and the most recent archived configuration. To view the difference between the two running configurations, click on the Diff icon.</td>
</tr>
</tbody>
</table>
Configuration Quick Deploy

You can create an immediate job to deploy the version of configuration being viewed on the device. You can deploy the configuration either in overwrite or merge mode.

Features of Configuration Quick Deploy

The following are the features of Configuration Quick Deploy:

- It can be performed for both running and startup configurations of all categories of devices.
- The job is executed immediately. Therefore Job approval should not be enabled at the time of Configuration Quick Deploy.
- The jobs cannot be rolled back.
- The jobs use TFTP, Telnet, SSH, SCP, RCP, HTTPs transport protocols.
- It provides an option to select either merge or overwrite mode when you deploy configuration on a device.
- It cannot be performed for VLAN configurations. However, you can deploy VLAN configurations using the CLI command, `cwcli config put`. See Overview: `cwcli config Command` for more information.
- It is supported for configuration versions in the archive only. That is, you cannot deploy for configuration version available on a device.
- The jobs use the same protocol order that you have specified in the Config Transport Settings (Admin > Collection Settings > Config > Config Transport Settings).
Performing a Configuration Quick Deploy

You can perform a configuration quick deploy using the Config Viewer window.
For example, you can launch Config Viewer window by clicking on Startup configuration or Running
Configuration links while performing tasks such as generating Out-Of-Sync Summary report, viewing
the Version Summary report etc.

**Note**
View Permission Report ([Reports > System > Users > Permission](#)) to check if you have the required
privileges to perform this task.

**Step 1**
Click **Deploy** on the Config Viewer ([Understanding the Config Viewer Window](#)) window.
The Job Option Details dialog box appears.

**Step 2**
Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job Information</strong></td>
<td></td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.</td>
</tr>
<tr>
<td><strong>Job Options</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Job Password  | • If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) enter the device login user name and password and device Enable password.  
• If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) either:  
  – Enter the device login user name and password and device Enable password or  
  – Disable the Job Password option in the Job Schedule and Options dialog box. |
Step 3  Click *Submit*.

An immediate Quick Deploy of Configuration on Device job will be scheduled.

A message appears, *Job ID is created successfully.*

Where ID is a unique Job number.

Step 4  Click *OK*.

You can check the status of your scheduled *Config Quick Deploy* job by selecting *Configuration > Job Browsers > Configuration Archive*.

---

**What Happens During Configuration Quick Deploy**

Before Configuration Management deploys the configuration on the device, it verifies whether the device is locked.

The deploy process follows the configured transport protocol order and the fallback option is active.

At end of this task, Configuration Management will:

- Unlock the device
- Check in the new version of configuration if the deploy completes successfully.

After uploading the configuration on the device, Configuration Management writes to the Change Audit log.
Configuring Labels

A label is a name given to a group of customized selection of configuration files. You can select configuration files from different devices, group and label them.

These labeled files are not purged along with the other configuration files. You have to explicitly select the Purge labeled files option to purge the labeled files. These labeled files are not purged if this option is not enabled.

You can purge the label config files using Admin > Network > Purge Settings.

See Inventory Management with Cisco Prime LAN Management Solution 4.2 for further details.

The Label Config window displays the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label Name</td>
<td>Displays the label name.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the label description.</td>
</tr>
<tr>
<td>Created by</td>
<td>Displays the user who created this label.</td>
</tr>
<tr>
<td>Created on</td>
<td>Displays the label creation time.</td>
</tr>
</tbody>
</table>

You can click on any column heading to sort the information by that column. If you double-click a heading, the order is reversed.

The Label Configs window contains the following buttons:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>Create a label. See Creating a Label for further details.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit a labeled configuration. See Editing a Labeled Configuration for further details. This button is active only after you select a Label.</td>
</tr>
<tr>
<td>View</td>
<td>View a labeled configuration. See Viewing the Labeled Configuration for further details. This button is active only after you select a Label.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete labeled configuration. See Deleting the Labeled Configuration for further details. This button is active only after you select a Label.</td>
</tr>
</tbody>
</table>
Creating a Label

You can use Label Configuration to create a group of configuration files from selected devices.

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

You can create a label file using the following workflow:

Step 1
Select Configuration > Configuration Archive > Label Configs.

The Label Configs dialog box appears.

Step 2
Click Create.

The Device Selection dialog box appears.

Step 3
In Device Selector pane, select the devices. See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to use the Device Selector.

Step 4
Go to the Label selection pane and:

- Enter the Label Name. You can enter up to 64 characters.
- Enter the Label Description. You can enter up to 128 characters.

Step 5
Go to the Config Type pane and select Primary or VLAN.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Contains the Running and Startup configuration files information.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information.</td>
</tr>
</tbody>
</table>

Step 6
Go to the Version pane and select Latest to include the most recent configuration only, or All to view all configuration versions.

- If you have selected Latest, you can click Finish button in the Select Devices page and complete the Label creation.
- If you have selected All, go to Step 7.

Step 7
Click Next.

The Select Configs to be Labelled dialog box appears.

- To view the configuration, select a configuration version file from the left pane and click View. The Config Viewer (Understanding the Config Viewer Window) window appears.
- To add the selected configuration, select a configuration version file from the left pane and click Add.
- To remove the selected configuration, select a configuration version file from the right pane and click Remove.
Step 8  
Click **Finish**.
A message appears, *Label LabelName created successfully.*
Where *LabelName* is the name of the label that you entered.

Step 9  
Click **OK**.

---

**Editing a Labeled Configuration**

You can make the following changes to a label:

- Modify the Label Description.
- Remove configuration files from the Selected Versions list.
- Add new configuration files from the Devices list.

**Note**  
View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

You can edit a label file using the following workflow:

**Step 1**  
Select **Configuration > Configuration Archive > Label Configs**.
The Label Configs dialog box appears.

**Step 2**  
Select a label and click **Edit**.
The Device Selection dialog box appears. The devices that are already part of the labeled file are selected.

**Step 3**  
Go to the Device Selector pane and select a new device or deselect a device. See *Inventory Management with Cisco Prime LAN Management Solution 4.2* for information on how to use the Device Selector.

**Step 4**  
Go to the Version pane and select **Latest** to include the most recent configuration only, or **All** to view all configuration versions.

**Step 5**  
Click **Next**.
The Label Details dialog box appears with the current details of the label.

**Step 6**  
Do either of the following:

- Change the Label Description. You can enter up to 128 characters.
- Select a configuration version file from the left pane, click **Add** to add the selected configuration file.
  - If you selected **Latest** in the previous dialog box, the left pane will show devices and the latest archived configuration file. The right pane contains labeled configuration.
  - If you selected **All** in the previous dialog box, the left pane will show devices and all available archived configuration files. The right pane contains labeled configuration.

**Note**  
You can select only one configuration file for a device.
• To remove the selected configuration, select a configuration version file from the right pane and click **Remove**.

• To view the configuration, select a configuration version file from the left pane and click **View**. The Config Viewer (**Understanding the Config Viewer Window**) window appears.

**Step 7** Click **Finish**.

A message appears, *Label LabelName updated.*

Where *LabelName* is the name of the label as entered by you.

**Step 8** Click **OK**.

### Viewing the Labeled Configuration

You can view configurations of a label from the label listing.

**Note**

View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

**Step 1** Select **Configuration > Configuration Archive > Label Configs**.

The Label Configs dialog box appears.

**Step 2** Select a label and click **View**.

The Label Config Viewer window appears with the following information:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository.</td>
</tr>
<tr>
<td>Config Type</td>
<td>Defines the type of configuration PRIMARY, SECONDARY, or VLAN.</td>
</tr>
<tr>
<td></td>
<td>• PRIMARY/SECONDARY—Contains the Running and Startup configuration files information.</td>
</tr>
<tr>
<td></td>
<td>• VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information.</td>
</tr>
<tr>
<td></td>
<td>For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of configuration file.</td>
</tr>
<tr>
<td></td>
<td>Click on the version to display Config Viewer (see <strong>Understanding the Config Viewer Window</strong>), which shows contents of corresponding configuration file.</td>
</tr>
<tr>
<td></td>
<td>In the Config Viewer window, you can click the Deploy button if you want to perform a Configuration Quick Deploy (<strong>Configuration Quick Deploy</strong>)</td>
</tr>
<tr>
<td>Created On</td>
<td>Date and time at which configuration file was created.</td>
</tr>
<tr>
<td>Change Description</td>
<td>Description of the configuration change.</td>
</tr>
</tbody>
</table>
Deleting the Labeled Configuration

You can delete a label from the list of labels in the label configuration dialog box:

| Note | View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task. |

**Step 1**
Select **Configuration > Configuration Archive > Label Configs**.
The Label Configs dialog box appears.

**Step 2**
Select the labels and click **Delete**.
A message appears, **Are you sure you want to delete the label(s)?**

**Step 3**
Click **OK** to delete the labels.

Using Search Archive

You can search the archive for configuration containing text patterns for selected devices. You can specify ten different combinations of patterns or strings as part of search criteria.

For example:
- Search all devices for configurations having pattern `set banner motd` and `set banner exec`.
- Search all devices for configurations having pattern `set banner motd` and `set banner exec` and `set password`.

You can also specify an option to ignore or consider the case sensitive property.

You can create a custom configuration query that searches information about the specified configuration files.

If you monitor devices X, Y, and Z every morning, you can create a custom query on them. When you run the query, LMS quickly gathers all the archived configuration files for these devices and displays them in a report.

The Custom Queries window displays the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Name</td>
<td>Custom Query name.</td>
</tr>
<tr>
<td>Description</td>
<td>Custom Query description.</td>
</tr>
<tr>
<td>Created By</td>
<td>User who created this Custom Query.</td>
</tr>
<tr>
<td>Created On</td>
<td>Custom Query creation time.</td>
</tr>
</tbody>
</table>

You can click on any column heading to sort the information by that column. If you double-click a heading, the order is reversed.
The Custom Queries window contains the following buttons:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>Create a custom query. See Creating a Custom Query for further details.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit a custom query. See Editing a Custom Query for further details. This button is active only after you select a custom query.</td>
</tr>
<tr>
<td>Run</td>
<td>Run a custom query. See Running a Custom Query for further details. This button is active only after you select a custom query.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete custom queries. See Deleting the Custom Queries for further details. This button is active only after you select a custom query.</td>
</tr>
</tbody>
</table>

The user who creates the custom query has full permission to perform tasks such as edit and run on the Custom Queries.

See Searching Archive for the procedure to search the configuration with and without a search pattern.

Creating a Custom Query

To create a custom query:

**Note** View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

**Step 1** Select Configuration > Configuration Archive > Views > Custom Queries.

The Custom Queries dialog box appears

**Step 2** Click Create.

**Step 3** Do any of the following:

- Enter the Custom Query name. You can enter up to 64 characters.
- Enter the Custom Query description. You can enter up to 128 characters.
- Enter patterns to search for, for example, http server. You can enter text patterns up to 64 characters.
  
  To search for more than one pattern, enter the second and third patterns in the Pattern 2 and Pattern 3 fields. You can specify ten different combinations of patterns as part of search criteria.

  You cannot search for special characters or regular expressions, for example, Control-C, boot*, etc.

- Select the search criteria Contains/Does Not Contain.
- If you have entered string as a search pattern, you can select Match Any to search for any given pattern string or Match All to search for all pattern strings.
- Click Match Case to perform a case-sensitive search, which is more efficient when you know the exact pattern you want to match. By default, Match Case is disabled.
Using Search Archive

Step 4  Click OK.
A message appears, Custom Query CustomQueryName created successfully.
Where CustomQueryName is the name of the custom query as entered by you.

Step 5  Click OK.

Running a Custom Query

To run a custom query:

Note View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

Step 1  Select Configuration > Configuration Archive > Views > Custom Queries.
The Custom Queries dialog box appears.
Step 2  Select a Custom Query and click Run.
The Device Selection dialog box appears.
Step 3  Select the devices. See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to use the Device Selector.
Step 4  Click OK.
The Custom Query Search Result window appears with the following information:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.</td>
</tr>
<tr>
<td>Version</td>
<td>Versions of configuration file. Click on the version to display Config Viewer (see Understanding the Config Viewer Window), which shows contents of corresponding configuration file. In the Config Viewer window, you can click on the Deploy button if you want to perform a configuration quick deploy (Configuration Quick Deploy)</td>
</tr>
<tr>
<td>Created On</td>
<td>Date and time at which the configuration file was created.</td>
</tr>
</tbody>
</table>

You can perform the following tasks from this window:
- Select the devices and click NetConfig to make any changes to the device configuration using NetConfig templates.
- Select a device and click Edit to edit the device configuration using the Config Editor application.
Chapter 6      Archiving Configurations and Managing them using Configuration Archive

Using Search Archive

Editing a Custom Query

You can edit the Custom Query description and modify the search patterns and their criteria. To edit a custom query:

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

Step 1 Select Configuration > Configuration Archive > Views > Custom Queries.

Step 2 Select a Custom Query and click Edit.

Step 3 Do any of the following:

- Update the Custom Query description. You can enter up to 128 characters.
- Either add a new search pattern or delete or update an existing search pattern and its criteria. You can enter up to 64 characters.
- Modify the string search option Match Any to Match All or vice versa.
- Enable or Disable the case-sensitive search.

Step 4 Click OK.

A message appears, Custom Query CustomQueryName updated successfully.

Where CustomQueryName is the name of the Custom Query.

Step 5 Click OK.

Deleting the Custom Queries

To delete the custom queries:

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

Step 1 Select Configuration > Configuration Archive > Views > Custom Queries.

Step 2 Select a Custom Query and click Delete.

A message appears, The query will be deleted.

Step 3 Click OK.
Searching Archive

You can search the device configuration file with or without the search pattern. You can also narrow down your search using Label Configuration files and Custom Queries.

You can view the search report in two ways:
- Search Archive Result
- Device Configuration Quick View Report

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To search the configuration archive:

Step 1 Select Configuration > Configuration Archive > Views > Search Archive.
The Search Archive dialog box appears.

Step 2 Enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Left Pane</strong></td>
<td></td>
</tr>
<tr>
<td>Label Config</td>
<td>Enable this option and select a label name.</td>
</tr>
<tr>
<td></td>
<td>The configuration version options Latest and All are disabled.</td>
</tr>
<tr>
<td>Device Selector</td>
<td>Select the devices. See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to use the Device Selector.</td>
</tr>
<tr>
<td></td>
<td>If you have selected Label Config, you need not select devices. If you have selected any devices, only the devices that are specified in the label configuration are searched. Other devices are ignored.</td>
</tr>
<tr>
<td>Version</td>
<td>Select Latest to search the most recent configuration only or All to search all configuration versions.</td>
</tr>
<tr>
<td></td>
<td>If you have selected Label Config, then you cannot specify the versions.</td>
</tr>
<tr>
<td>View Type</td>
<td>Select one of these view types:</td>
</tr>
<tr>
<td></td>
<td>• Version to view the Device Configuration Version Report. This displays all versions of the configuration, the time and date the configurations were archived, and reason for archival.</td>
</tr>
<tr>
<td></td>
<td>• Quick View to view the Device Configuration Quick View Report. This displays the contents of the configuration files.</td>
</tr>
<tr>
<td><strong>Right Pane</strong></td>
<td></td>
</tr>
<tr>
<td>Custom Query</td>
<td>Select a Custom Query.</td>
</tr>
<tr>
<td></td>
<td>The search patterns that are defined in the Custom Query appear in the Pattern Details text boxes.</td>
</tr>
<tr>
<td></td>
<td>In addition to Custom Query search patterns, you can also add additional search patterns.</td>
</tr>
</tbody>
</table>
Using Search Archive

Step 3 Click Search.

Based on your View type selection, either Search Archive Result or Device Configuration Quick View Report appears.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Pattern Details | Perform the following tasks:  
  • Enter patterns to search for, for example, http server. You can enter text patterns up to 64 characters.  
  To search for more than one pattern, enter the second and third patterns in the Pattern 2 and Pattern 3 fields. You can specify ten different combinations of patterns as part of search criteria.  
  You cannot search for special characters, for example, Control-C, boot*.  
  You can also search the device configuration file without the search pattern. The search will list all archived configuration for all selected devices.  
    – If you have selected the version as Latest, the search will list latest archived configuration for all selected devices.  
    – If you have selected the version as All, the search will list all archived configurations for all selected devices  
  • Select the search criteria Contains/Does Not Contain.  
  • If you have entered string as a search pattern, you can select Match Any to search for any given pattern string or Match All to search for all pattern strings  
  • Click Match Case to perform a case-sensitive search, which is more efficient when you know the exact pattern you want to match. By default, Match Case is disabled.  
| Date Range | Select any of the following Date Range types:  
  • As on—Search config archives on or before the specified date and time.  
  • From—Search config archives for the specified period.  
  • Last—Search config archives for the last N number of days, weeks, months or years; where N is the value entered for the number of days, weeks, months or years.  
  The following maximum values for N can be specified:  
    – Days—The maximum number of days that can be specified is 999.  
    – Weeks—The maximum number of weeks that can be specified is 999.  
    – Months—The maximum number of months that can be specified is 99.  
    – Years—The maximum number of years that can be specified is 9.  
  If you have selected Latest as the version, the Date Range option searches for the most recent config archives.  

Chapter 6  Archiving Configurations and Managing them using Configuration Archive

Search Archive Result

The Search Archive Result displays information about the device configurations. The Search Archive Result contains the following details of the selected configurations:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.</td>
</tr>
<tr>
<td>Config Type</td>
<td>Defines the type of configuration PRIMARY, SECONDARY, or VLAN.</td>
</tr>
<tr>
<td></td>
<td>• PRIMARY/SECONDARY—Contains the Running and Startup configuration files information.</td>
</tr>
<tr>
<td></td>
<td>• VLAN—Contains running vlan.dat configuration file information. This config type does not contain Startup configuration file information. For ONS devices, the PRIMARY config type displays the configuration information from the active CPU, at that instance.</td>
</tr>
<tr>
<td>Version</td>
<td>Versions of configuration file. Click on the version to display Config Viewer (see Understanding the Config Viewer Window), which shows contents of the corresponding configuration file.</td>
</tr>
<tr>
<td>Created On</td>
<td>Date and time at which the configuration file was created.</td>
</tr>
<tr>
<td>Change Description</td>
<td>Cause of configuration change.</td>
</tr>
</tbody>
</table>

You can perform the following tasks from this window:

- Select the devices and click **NetConfig** to make changes to the device configuration using NetConfig templates.
- Select a device and click **Edit** to edit the device configuration using the Config Editor application.

Device Configuration Quick View Report

The Device Configuration Quick View report lists the devices, configuration version numbers, and configuration details of the device configuration version you specified.

You can specify how you want to view the contents of the configurations by selecting one of the options under Show:

- Click **Raw** to view data exactly as it appears in the configuration file. There are two panes, one lists all devices and the other displays the configuration.
- Click **Processed** to view data with the commands ordered and grouped. There are three panes, one lists all devices, the second pane lists all configlets, and the third pane displays the configuration.
Chapter 6      Archiving Configurations and Managing them using Configuration Archive

Using Search Archive

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>Device Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.</td>
</tr>
</tbody>
</table>
| Configlets           | You can click on any configlets to display the corresponding information. The available configlets vary from device to device. The following are examples:  
  - All—The entire contents of the configuration files.  
  - SNMP—SNMP configuration commands. For example, `snmp-server community public RO`.  
  - IP Routing—IP routing configuration commands. For example, `router abcd 100`.  
  - Interface folder—The different interface configuration commands. For example, `Interface Ethernet0` and `Interface TokenRing`.  
  - Global—Global configuration commands. For example `no ip address`.  
  - Line con 0—Configuration commands for line console 0.  
  - IP—IP configuration commands. For example, `ip http server`. |
| Configuration file name | You can view the contents of configuration file. |

The following buttons are available on the Config Viewer:

<table>
<thead>
<tr>
<th>Button (Icon)</th>
<th>Description</th>
</tr>
</thead>
</table>
| Export       | Exports the configuration file.  
  - If you are using the Raw mode then the exported file format is cfg. The file name convention is `DeviceName-VersionNumber.cfg`.  
  - If you are using the Processed mode then the exported file format is XML and the file name convention is `DeviceName-VersionNumber.xml`.  

Where `DeviceName` is the Device Name as entered in Device and Credential Repository and `VersionNumber` is the device configuration version. |

The default directory where Configuration Archive file is exported is:  
On Solaris and Soft Appliance server,  
`/var/adm/CSCOpx/files/rme/dcma/configexport`  
On Windows server,  
`NMSROOT\files\rme\dcma\configexport`
### Using Search Archive

#### Button | Description
--- | ---
**Export (continue)** | To export a file:
1. Click on the icon.
   The Export Config File dialog box appears.
2. Enter the folder name on the LMS server.
   You must enter the default export directory. You cannot enter any other directory.
   or
   Browse to select a folder on the LMS server.
   The Server Side File Browser dialog box appears.
   a. Select a folder on the LMS server.
   b. Click **OK**.
   The Browse button takes you to the default directory. The Server Side File Browser does not allow you to change this default export directory.
3. Click **OK**.
   If you have exported configuration in the Raw mode, the notification message displays,
   Config file exported as `ExportedFolder\DeviceName-VersionNumber.cfg`
   If you have exported configuration in the Processed mode, the notification message displays,
   Config file exported as `ExportedFolder\DeviceName-VersionNumber.XML`
   Where `ExportedFolder` is the location to which the configuration file is exported.
4. Click **OK**.

**Print (Icon)** | Generates a format that can be printed.

**Compare with previous version** | Compares configuration with the previous version. When you click on this button, a new window Config Diff Viewer opens to show configurations side by side.
   See [Understanding the Config Diff Viewer Window](#) for further details.
   This button is active only if you have a previous version of configuration.

**Compare with next version** | Compares configuration with the next version. When you click this button, a new window Config Diff Viewer opens to show configurations side by side.
   See [Understanding the Config Diff Viewer Window](#) for further details.
   This button is active only if you have a next version of configuration.

**Edit** | Launches Config Editor window.
   This button is active only if you are viewing the configuration version from the archive.
   See [Editing and Deploying Configurations Using Config Editor](#) for further details.

**Deploy** | You can perform a configuration quick deploy.
   This button is active only if you are viewing the configuration version from the archive.
   See [Configuration Quick Deploy](#).
Comparing Configurations

You can compare two device configuration files from version to version or from device to device. You can also compare the configuration when a device was started with the current configuration, and the current configuration with the most recently archived configuration.

You can list the commands that have to be excluded while comparing configurations.

To do this select Admin > Collection Settings > Config > Config Compare Exclude Commands Configuration.

You can compare the configurations in these ways:

• Startup vs. Running—Compares the configuration when the device was started with the current configuration. These configurations are fetched from the device.
  
  See Comparing Startup vs. Running Configurations.

• Running vs. Latest Archived—Compares the running configuration with the most recently archived configuration. The Running configuration is fetched from the device.
  
  See Comparing Running vs. Latest Archived Configurations.

• Two Versions of the Same Device—Compares two archived configuration versions.
  
  See Comparing Two Configuration Versions of the Same Device.

• Two Versions of Different Devices—Compares any two configurations in the configuration archive.
  
  See Compare Two Configuration Versions of Different Devices.

• Base Config vs. Latest Version of Different Devices—Compares the base configuration of a device with the latest configuration of other devices. These configurations are fetched from the device.
  
  See Compare Base Config vs. Latest Configuration Version of Multiple Devices.

Comparing Startup vs. Running Configurations

You can compare the configuration when a device was started with the current configuration. These configurations are fetched from the device.

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.
To compare Startup vs. Running configurations:

**Step 1** Select **Configuration > Configuration Archive > Compare Configs**.
The Compare Configurations dialog box appears.

**Step 2** Select **Startup vs. Running** and click **Compare**.
The Device Selection dialog box appears.

**Step 3** Select a device. See *Inventory Management with Cisco Prime LAN Management Solution 4.2* for information on how to use the Device Selector.

**Step 4** Click **OK**.
The **Understanding the Config Diff Viewer Window** window appears.

---

**Comparing Running vs. Latest Archived Configurations**

You can compare the configuration currently running on a device with the most recent configuration stored in the configuration archive. The Running configuration is fetched from the device.

**Note** View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To compare Running vs. latest archived configurations:

**Step 1** Select **Configuration > Configuration Archive > Compare Configs**.
The Compare Configurations dialog box appears.

**Step 2** Select **Running vs. Latest Archived** and click **Compare**.
The Device Selection dialog box appears.

**Step 3** Select a device. See *Inventory Management with Cisco Prime LAN Management Solution 4.2* for information on how to use the Device Selector.

**Step 4** Click **OK**.
The **Understanding the Config Diff Viewer Window** window appears.
Comparing Two Configuration Versions of the Same Device

You can compare two different archived configurations of the same device.

Note: View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To compare two versions of the same device:

Step 1 Select Configuration > Configuration Archive > Compare Configs.

The Compare Configurations dialog box appears.

Step 2 Select Two Versions of the Same Device and click Compare.

The Device Selection dialog box appears.

Step 3 Select a device. See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to use the Device Selector.

Step 4 Click Next.

The Select First Configuration dialog box appears with the following information:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Version</td>
<td>Versions of configuration file.</td>
</tr>
<tr>
<td>File Type</td>
<td>Defines the configuration file type as either Running or Startup configuration.</td>
</tr>
<tr>
<td>Config Type</td>
<td>Defines the type of configuration PRIMARY, SECONDARY, or VLAN.</td>
</tr>
<tr>
<td></td>
<td>• PRIMARY/SECONDARY—Contains the Running and Startup configuration files information.</td>
</tr>
<tr>
<td></td>
<td>• VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information.</td>
</tr>
<tr>
<td></td>
<td>For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.</td>
</tr>
<tr>
<td>Created On</td>
<td>Date and time at which the configuration file was created.</td>
</tr>
</tbody>
</table>

Step 5 Click on the first configuration to compare and click Next.

The Select Second Configuration dialog box appears with the same information as the Select First Configuration window.

Step 6 Click on the second configuration to compare it with first configuration and click Finish.

The Understanding the Config Diff Viewer Window appears.
Compare Two Configuration Versions of Different Devices

You can compare two archived versions of a configuration of the same or different devices.

**Note** View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To compare two versions of different devices:

---

**Step 1** Select Configuration > Configuration Archive > Compare Configs.

The Compare Configurations dialog box appears.

**Step 2** Select Two Versions of Different Devices and click Compare.

The Select Device and Pattern dialog box appears.

**Step 3** Perform the following and click Next:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Left Pane</strong></td>
<td></td>
</tr>
<tr>
<td>Device Selector</td>
<td>Select the devices. Select the devices.</td>
</tr>
<tr>
<td></td>
<td>See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to use the Device Selector.</td>
</tr>
<tr>
<td>Version</td>
<td>Select Latest to view the most recent configuration or All to view all configuration versions.</td>
</tr>
<tr>
<td><strong>Right Pane</strong></td>
<td></td>
</tr>
<tr>
<td>Pattern Details</td>
<td>Perform the following tasks:</td>
</tr>
<tr>
<td></td>
<td>1. Enter patterns to search for, for example, http server. You can enter text patterns up to 64 characters.</td>
</tr>
<tr>
<td></td>
<td>To search for more than one pattern, enter the second and third patterns in the Pattern 2 and Pattern 3 fields. You can specify ten different combinations of patterns as part of search criteria.</td>
</tr>
<tr>
<td></td>
<td>You cannot search for special characters or regular expressions, for example, Control-C, boot*.</td>
</tr>
<tr>
<td></td>
<td>You can search the device configuration file without the search pattern.</td>
</tr>
<tr>
<td></td>
<td>2. Select the search criteria Contains/Does Not Contain.</td>
</tr>
<tr>
<td></td>
<td>If you have entered string as a search pattern, you can select Match Any to search for any given pattern string or Match All to search for all pattern strings.</td>
</tr>
<tr>
<td></td>
<td>3. Click Match Case to perform a case-sensitive search, which is more efficient when you know the exact pattern you want to match. By default, Match Case is disabled.</td>
</tr>
</tbody>
</table>
The Select First Configuration dialog box appears with the following information:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository.</td>
</tr>
<tr>
<td>Config Version</td>
<td>Versions of configuration file.</td>
</tr>
<tr>
<td>File Type</td>
<td>Defines the configuration file type as either Running or Startup configuration.</td>
</tr>
</tbody>
</table>
| Config Type | Defines the type of configuration PRIMARY, SECONDARY, or VLAN.  
  • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information.  
  • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information.  
  For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance. |
| Created On | Date and time at which the configuration file was created. |

**Step 4**  
Click on the first configuration to compare and click **Next**.  
The Select Second Configuration dialog box appears with the same information as the Select First Configuration window.

**Step 5**  
Click on the second configuration to compare with first configuration and click **Finish**.  
The **Understanding the Config Diff Viewer Window** window appears.
Compare Base Config vs. Latest Configuration Version of Multiple Devices

You can compare and sync the base configuration of a device with the latest configuration version of multiple devices. The base configuration can be Running, Startup, or User archives.

Note
View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To compare the base configuration with the latest configuration version of different devices:

Step 1
Select Configuration > Configuration Archive > Compare Configs.

The Compare Configurations dialog box appears.

Step 2
Select Base Config vs. Latest Version of Multiple Devices and click Compare.

The Select a Base Device dialog box appears.

Step 3
Select a base device. See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to use the Device Selector.

Step 4
Click Next.

The Select Config Version of the Base Device to Compare dialog box appears.

Step 5
Select the configuration version of the base device from the Config Version tree.

- If you check Filter Same Device Category Devices, it displays devices that belong to the base device category. These devices are displayed in the Select Other Devices to Compare page.

- If you uncheck Filter Same Device Category Devices, it displays all devices that belong to other device categories that are managed by LMS. These devices are displayed in the Select Other Devices to Compare page.

Step 6
Click Next.

The Select Other Devices to Compare dialog box appears.

Step 7
Select the devices to compare with the configuration of the base device.

You can select devices using the Device Selector. See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to use the Device Selector.

Step 8
Click Next.

The Add Exclude Commands dialog box appears.

Step 9
Do the following in the Add Exclude Commands dialog box:
### Comparing Configurations

**Step 10**  Click **Finish**.

The Compare Config window appears, displaying the following details:

<table>
<thead>
<tr>
<th>Field Name/Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td></td>
</tr>
<tr>
<td>Total No.of Device(s) selected for comparison</td>
<td>Number of devices selected for comparison.</td>
</tr>
<tr>
<td>Number of Compliant devices</td>
<td>Number of devices that comply with the base configuration.</td>
</tr>
<tr>
<td>Number of Non-Compliant devices</td>
<td>Number of devices that do not comply with the base configuration.</td>
</tr>
<tr>
<td>Number of Excluded devices</td>
<td>Number of devices excluded from comparison.</td>
</tr>
<tr>
<td>Base Device</td>
<td>Name of the base device.</td>
</tr>
<tr>
<td>Base Config Type</td>
<td>Configuration type of the base device.</td>
</tr>
<tr>
<td>Base Config Branch</td>
<td>Configuration branch version of the base device. For example, DeviceArchive.</td>
</tr>
<tr>
<td><strong>Non-Compliant Devices</strong></td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository.</td>
</tr>
<tr>
<td>Latest Version</td>
<td>Version of configuration file against which the compliance was checked. Click on the version to display Config Viewer (see Understanding the Config Viewer Window). This shows the contents of corresponding configuration file against which the compliance was checked.</td>
</tr>
<tr>
<td>Diff</td>
<td>Differences between base configuration and the lastest configuration version of mutiple devices. To view the difference between the base configuration and the latest configuration version of other devices, click on the Diff icon. The Config Diff Viewer window appears. For more information, see Understanding the Config Diff Viewer Window.</td>
</tr>
</tbody>
</table>
Comparing Configurations

Step 11 Click **Diff** to view the differences between base configuration and the latest configuration version of multiple devices. The Config Diff Viewer window appears. For more information, see Understanding the Config Diff Viewer Window.

Step 12 Click **Deploy** to sync the base configuration with the latest configuration. The Job Options Details pop-up window appears, displaying the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job Information</strong></td>
<td></td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter the e-mail address.</td>
</tr>
<tr>
<td>Retain new config additions in &lt;&lt;config version&gt;&gt;</td>
<td>Check to retain new config additions in the configuration file.</td>
</tr>
<tr>
<td><strong>Job Options</strong></td>
<td></td>
</tr>
<tr>
<td>Job Password</td>
<td>Check to enable Job Password option</td>
</tr>
<tr>
<td>Login username</td>
<td>Enter the login username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the login password.</td>
</tr>
<tr>
<td>Enable password</td>
<td>Enter the enable password.</td>
</tr>
<tr>
<td>Submit (button)</td>
<td>Click <strong>Submit</strong> to run the job.</td>
</tr>
</tbody>
</table>

Step 13 Enter the Job Information and Job Option details.

Step 14 Click **Submit** to run the job.

**Examples for Exclude Commands**
This section contains examples for exclude commands:

<table>
<thead>
<tr>
<th>Field Name/Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Excluded Devices</strong></td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository.</td>
</tr>
<tr>
<td>Reason for Exclusion</td>
<td>Displays the cause for exclusion.</td>
</tr>
<tr>
<td><strong>Buttons</strong></td>
<td></td>
</tr>
<tr>
<td>Export (Icon)</td>
<td>Exports the data to a file of PDF or CSV format.</td>
</tr>
<tr>
<td>Print (Icon)</td>
<td>Generates a format that can be printed.</td>
</tr>
</tbody>
</table>
Understanding the Config Diff Viewer Window

The Configuration Version Compare report shows the differences between the two selected configurations. You can access the Configuration Version Compare report by comparing device configurations.

You can specify how you want to view the differences between the configurations by selecting one of the options under Show:

- Click **Raw** to view the differences between the two raw configurations.
- Click **Processed** to view the differences with the commands ordered and grouped.

The color conventions that are used on Config Diff Viewer are:

- **Black**—All unchanged text.
- **Red**—Lines that have changed from one version to another.
- **Blue**—Lines that have been added or deleted from one of the versions.

Scenario | Command Type (Examples)
--- | ---
To exclude anything after IP Address | ip address .*
To exclude IP address range from 172.20.115.1 to 255 | ip address 172\.(20|115)\.(25[0-5]|2[0-4]\[0-9]|\[01[0-9]|0\.-9]?) 255.255.255.128
To exclude SNMP host that contain either inside or outside characters | snmp host \b(inside|outside) 10.77.203.176 community public

For more information, see the regex API guide for Java 1.4.2 from Oracle [http://download.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html](http://download.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html) for other patterns.
The Configuration Versions Compare report has three columns:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configlets</td>
<td>You can click on any configlet to display the corresponding information. The available configlets vary from device to device. The following are examples:</td>
</tr>
<tr>
<td></td>
<td>• Diffs—Displays the differences between the two configuration files (if you selected more than one).</td>
</tr>
<tr>
<td></td>
<td>• All—The entire contents of the configuration files.</td>
</tr>
<tr>
<td></td>
<td>• SNMP—SNMP configuration commands. For example, <code>snmp-server community public RO</code>.</td>
</tr>
<tr>
<td></td>
<td>• IP Routing—IP routing configuration commands. For example, <code>router abcd 100</code>.</td>
</tr>
<tr>
<td></td>
<td>• Interface folder—The different interface configuration commands. For example, <code>Interface Ethernet0</code> and <code>Interface TokenRing</code>.</td>
</tr>
<tr>
<td></td>
<td>• Global—Displays global configuration commands. For example, <code>no ip address</code>.</td>
</tr>
<tr>
<td></td>
<td>• Line con 0—Displays configuration commands for line console 0.</td>
</tr>
<tr>
<td></td>
<td>• IP—Displays IP configuration commands. For example, <code>ip http server</code>.</td>
</tr>
</tbody>
</table>

| First configuration file | Contains the contents of the first configuration file. |
| Second configuration file | Contains the contents of the second configuration file. |

The buttons on the Config Diff Viewer are:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export (Icon)</td>
<td>Export the configuration file.</td>
</tr>
<tr>
<td></td>
<td>• If you are using the Raw mode then the exported file format is cfg. The file name convention is <code>DeviceName-VersionNumber.cfg</code>.</td>
</tr>
<tr>
<td></td>
<td>• If you are using the Processed mode then the exported file format is XML. The file name convention is <code>DeviceName-VersionNumber.xml</code>.</td>
</tr>
<tr>
<td></td>
<td>Where <code>DeviceName</code> is the device name as entered in Device and Credential Repository and <code>VersionNumber</code> is the device configuration version.</td>
</tr>
</tbody>
</table>

The default directory where Configuration Archive file is exported is:

On Solaris and Soft Appliance server,

\[ /var/adm/CSCOpx/files/rme/dcma/configexport \]

On Windows server,

\[ NMSROOT\files\rme\dcma\configexport \]
Chapter 6      Archiving Configurations and Managing them using Configuration Archive

Comparing Configurations

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export (continue)</td>
<td>To export a file:</td>
</tr>
<tr>
<td></td>
<td>1. Click on the icon.</td>
</tr>
<tr>
<td></td>
<td>The Export Config File dialog box appears.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the folder name on the LMS server.</td>
</tr>
<tr>
<td></td>
<td>You must enter the default export directory. You cannot enter any</td>
</tr>
<tr>
<td></td>
<td>other directory.</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>Browse to select a folder on the LMS server.</td>
</tr>
<tr>
<td></td>
<td>The Server Side File Browser dialog box appears.</td>
</tr>
<tr>
<td></td>
<td>a. Select a folder on the LMS server.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>The Browse button takes you to the default directory. It does not</td>
</tr>
<tr>
<td></td>
<td>allow you to change this default export directory.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>If you have exported configuration in the Raw mode, the notification</td>
</tr>
<tr>
<td></td>
<td>message displays, <strong>Config file exported as</strong> \ExportedFolder\DeviceName-VersionNumber.cfg**.</td>
</tr>
<tr>
<td></td>
<td>If you have exported configuration in the Processed mode, the</td>
</tr>
<tr>
<td></td>
<td>notification message displays, <strong>Config file exported as</strong> \ExportedFolder\DeviceName-VersionNumber.XML**.</td>
</tr>
<tr>
<td></td>
<td>Where <strong>ExportedFolder</strong> is the location where configuration file is</td>
</tr>
<tr>
<td></td>
<td>exported.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>This option is not available in the Config Diff Viewer page when you</td>
</tr>
<tr>
<td></td>
<td>compare Base Config vs. Latest Version of Different Devices.</td>
</tr>
<tr>
<td>Print (Icon)</td>
<td>Generates a format that can be printed.</td>
</tr>
<tr>
<td></td>
<td>This option is not available in the Config Diff Viewer page when you</td>
</tr>
<tr>
<td></td>
<td>compare Base Config vs. Latest Version of Different Devices.</td>
</tr>
</tbody>
</table>
Using Configuration Archive Job Browser

You can browse the Configuration Archive jobs that are registered on the system. From the Archive Management Jobs dialog box you can also retry, delete, stop jobs and view a job’s details.

This section details:

- Retrying a Config Job
- Stopping a Config Job
- Deleting the Config Jobs
- Viewing the Configuration Archive Job Details

The Archive Management Jobs window displays the following information:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique number assigned to the job when it is created. For periodic jobs such as Daily, Weekly, etc., the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001. Click on the Job ID to view the Configuration Archive job details (see Viewing the Configuration Archive Job Details).</td>
</tr>
<tr>
<td>Job Type</td>
<td>Type of the configuration job.</td>
</tr>
<tr>
<td></td>
<td>Sync Archive—Appears if you had scheduled a Sync Archive job (Configuration &gt; Configuration Archive &gt; Synchronization).</td>
</tr>
<tr>
<td></td>
<td>Get Config—Appears if you had scheduled a configuration fetch job using the CLI command, cwcli config get.</td>
</tr>
<tr>
<td></td>
<td>Put Config—Appears if you had scheduled a configuration retrieve job using the CLI command, cwcli config put.</td>
</tr>
<tr>
<td></td>
<td>Import Config—Appears if you had scheduled a job that retrieved the configuration from a file and if you had transferred it to the device using the CLI command, cwcli config import.</td>
</tr>
<tr>
<td></td>
<td>Write to Running Config—Appears if you had scheduled a job that downloaded the differences between the specified configuration file and the latest configuration version in the archive for the specified device, using the CLI command, cwcli config write2run.</td>
</tr>
</tbody>
</table>
### Configuration Management with Cisco Prime LAN Management Solution 4.2

#### Chapter 6 Archiving Configurations and Managing them using Configuration Archive

**Using Configuration Archive Job Browser**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job Type</strong></td>
<td><strong>(Continue)</strong></td>
</tr>
<tr>
<td>• Write to Startup Config—Appears if you had scheduled a job that erased the contents of the device Startup configuration and if you wrote contents of a specified file as new Startup configuration, using the CLI command, <code>cwcli config write2start</code>.</td>
<td></td>
</tr>
<tr>
<td>• Copy Running Config to Startup—Appears if you had scheduled a job that overwrote with the Startup configuration of the device with the Running configuration, using the CLI command, <code>cwcli config run2start</code>.</td>
<td></td>
</tr>
<tr>
<td>• Copy Startup Config to Running—Appears if you had scheduled a job that merged the Startup configuration with the Running configuration, using the CLI command, <code>cwcli config start2run</code>.</td>
<td></td>
</tr>
<tr>
<td>• Reload Device—Appears if you had scheduled a job that rebooted the devices, using the CLI command <code>cwcli config reload</code>.</td>
<td></td>
</tr>
<tr>
<td>• Config Quick Deploy—Appears if you had created an immediate Configuration Quick Deploy job, using the Config Viewer window.</td>
<td></td>
</tr>
<tr>
<td>• Compliance Check—Appears if you had scheduled a Compliance Check job (<code>Configuration &gt; Compliance &gt; Compliance Templates &gt; Compliance Check</code> and click the Compliance Check button).</td>
<td></td>
</tr>
<tr>
<td>• Check Compliance and Deploy—Appears if you had scheduled a Compliance Check job with the job option, Check compliance and deploy enabled (<code>Configuration &gt; Compliance &gt; Compliance Templates &gt; Compliance Check</code> and click the Compliance Check button).</td>
<td></td>
</tr>
<tr>
<td>• Deploy Baseline template—Appears if you had scheduled a Baseline Template deploy job (<code>Configuration &gt; Compliance &gt; Compliance Templates &gt; Direct Deploy</code> and click the Deploy button).</td>
<td></td>
</tr>
<tr>
<td>• Deploy Compliance Results—Appears if you had scheduled a Deploy job on the non-complaint devices (<code>Configuration &gt; Compliance &gt; Compliance Templates &gt; Jobs</code> and click the Deploy button).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Job states:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cancelled—Running job stopped by you.</td>
<td></td>
</tr>
<tr>
<td>• Failed—Failed job. Click on the Job ID to view the job details. The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, If the status displays Failed(5), then the count of devices that had failed is 5.</td>
<td></td>
</tr>
<tr>
<td>• Running—Job still running.</td>
<td></td>
</tr>
<tr>
<td>• Scheduled—Job scheduled to run.</td>
<td></td>
</tr>
<tr>
<td>• Rejected—Job rejected by an approver. Click on the Job ID to view the rejection details.</td>
<td></td>
</tr>
<tr>
<td>• Successful—Job completed successfully</td>
<td></td>
</tr>
<tr>
<td>• Waiting for Approval—Job waiting for approval.</td>
<td></td>
</tr>
</tbody>
</table>

**Description** | Job description entered during job definition |
| **Owner** | User who created this job. |
| **Scheduled at** | Date and time at which the job is scheduled to run. |
| **Completed at** | Date and time at which job was completed. |
| **Schedule Type** | Run type of the job: Immediate, Once, 6 - hourly, 12 - hourly, Daily, Weekly, and Monthly. |
You can click on any column heading to sort information by that column. If you double-click on a heading, the order is reversed.

You can use the Filter button to do a quick search on the Configuration Archive jobs. You can perform filters by using these options:

<table>
<thead>
<tr>
<th>Filter Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique number assigned to the job when it is created. For periodic jobs such as Daily, Weekly, etc., the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Types of Configuration Archive jobs. For example: Sync Archive, Write to Running Config.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the job. For example: Successful, Failed.</td>
</tr>
<tr>
<td>Description</td>
<td>Job description.</td>
</tr>
<tr>
<td>Owner</td>
<td>Owner of the job.</td>
</tr>
<tr>
<td>Schedule Type</td>
<td>Job schedule Type. For example: Immediate, Weekly.</td>
</tr>
<tr>
<td>Refresh (Icon)</td>
<td>Click on this icon to refresh the Configuration Archive Job Browser.</td>
</tr>
</tbody>
</table>

You can perform the following tasks on this window:

- Retrying a Config Job
- Stopping a Config Job
- Deleting the Config Jobs

## Retrying a Config Job

You can retry only a failed job. You cannot retry a job that is scheduled to run periodically (Daily, Weekly, and Monthly).

**Note**

View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To retry a job:

1. **Step 1** Select **Configuration > Job Browsers > Configuration Archive**.
   The Archive Management Jobs dialog box appears.
2. **Step 2** Select a failed job and click **Retry**.
   The Job Schedule and Options dialog box appears.
Step 3  Enter the following information:

Based on your retry job selection, some of the options may not be visible.

For example, 6 - hourly and 12 -hourly Run Type options are visible only if you are retrying a Sync Archive job. This is not visible for other types of Configuration Archive jobs.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>You can specify when you want to run the selected Retry job. To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>• 6 - hourly—Runs this task every 6 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>• 12 - hourly—Runs this task every 12 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs this task immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs this task once at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>• Daily—Runs daily at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly—Runs weekly on the specified day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Monthly—Runs monthly on the specified day of the month and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete.</td>
</tr>
<tr>
<td></td>
<td>For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed.</td>
</tr>
<tr>
<td></td>
<td>If the 10.00 a.m. November 1 job has not been completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.</td>
</tr>
<tr>
<td>Date</td>
<td>You can select the date and time (hours and minutes) at which to schedule a job. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.</td>
</tr>
</tbody>
</table>
Chapter 6  Archiving Configurations and Managing them using Configuration Archive

Using Configuration Archive Job Browser

### Stopping a Config Job

You can stop the following running job types (See Using Configuration Archive Job Browser for details on the job types):

- Put Config
- Import Config
- Write to Running Config
- Write to Startup Config
- Copy Running Config to Startup
- Copy Startup Config to Running
- Reload Device

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job Information</strong></td>
<td></td>
</tr>
<tr>
<td>Approver Comments</td>
<td>Enter comments for the job approver. This field appears only if you have enabled job approval for Configuration Archive.</td>
</tr>
<tr>
<td>Maker E-Mail</td>
<td>Enter the e-mail-ID of the job creator. This is a mandatory field. This field appears only if you have enabled job approval for Configuration Archive.</td>
</tr>
</tbody>
</table>
| Job Password           | • If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) enter the device login user name and password and device Enable password.  
  • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) either:  
    – Enter the device login user name and password and device Enable password  
    Or  
    – Disable the Job Password option in the Job Schedule and Options dialog box. |
| E-mail                 | Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS e-mail ID as the sender's address. |

**Step 4**  Click **Submit**.  
A message appears, **Job resubmitted successfully**.

**Step 5**  Click **OK**.
Chapter 6  Archiving Configurations and Managing them using Configuration Archive

Using Configuration Archive Job Browser

- Config Quick Deploy
- Check Compliance and Deploy
- Deploy Baseline template
- Compliance check

---

**Note**
View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To stop an Configuration Archive job:

**Step 1**
Select Configuration > Job Browsers > Configuration Archive.
The Archive Management Jobs dialog box appears.

**Step 2**
Select a running job and click **Stop**.
A message appears, **Selected job(s) will be stopped**.

**Step 3**
Click **OK**.

---

**Deleting the Config Jobs**

You can delete jobs with status:
- Cancelled
- Failed
- Scheduled
- Rejected
- Successful
- Waiting for Approval

You cannot delete a running job.

---

**Note**
View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To delete jobs:

**Step 1**
Select Configuration > Job Browsers > Configuration Archive.
The Archive Management Jobs dialog box appears.

**Step 2**
Select a running job and click **Delete**.
A message appears, **Selected job(s) will be deleted**.

**Step 3**
Click **OK**.
# Viewing the Configuration Archive Job Details

From the Archive Management Jobs window, you can learn more about one job by viewing its details. You can view these details by clicking the Job ID on the Config Job window.

**Note** View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

The Archive Management Job Details window contains the following information:

<table>
<thead>
<tr>
<th>Page/Folder</th>
<th>Description</th>
</tr>
</thead>
</table>
| Execution Summary | Displays summary of completed job:  
  - Execution Summary—Information about the job status, start time and end time.  
  - Device Summary—Information about the job completion status on the devices you have selected. For example, number of successful devices where the job is executed successfully.  
    Click on Device Details folder and device status link and on the Device link to see the complete job execution details.  
  - Execution Message (Pre-Execution and Post-Execution)—Information about any e-mails sent. |
| Device Details  | Contains detailed job results for each device. Displays status folders that correspond to possible device status:  
  - Successful Devices—Devices were successfully executed.  
  - Failed Devices—Devices were not successfully executed.  
  - Partially Failed Devices—Job partially failed to run on these devices.  
  - Pending Devices—Job did not try to update devices, even though they were selected.  
  - Not Attempted—Job did not attempt to run on these devices.  
  Click on Status to see the job details. Details include a record of the entire CLI session between LMS and the device.  
  When the configuration fetch takes unusually long, this error message appears,  
  Unable to get results of job execution for device. Please retry the job  
  This could happen because of slow device response, Network latency, etc. |
| Work Order      | Contains the Summary of the job definition such as,  
  - Detailed information, such as owner, schedule type, and Job Approval state.  
  - Policies configured for the job, such as E-mail Notification and Job Based Password.  
  - Devices on which the job runs. Also, gives details about the commands.  
  For retried jobs, these job definitions are not updated. For such jobs the original job definitions are retained. |
The buttons on the Job Details window are:

- Delete—You can delete jobs with the following Job Status:
  - Cancelled
  - Failed
  - Scheduled
  - Rejected
  - Successful
  - Waiting for Approval

You cannot delete a running job.

- Stop—You can stop the following running job types (See Using Configuration Archive Job Browser for details on the job types):
  - Put Config
  - Import Config
  - Write to Running Config
  - Write to Startup Config
  - Copy Running Config to Startup
  - Copy Startup Config to Running
  - Reload Device
  - Config Quick Deploy
  - Check Compliance and Deploy
  - Deploy Baseline template
  - Compliance check
Using Baseline Templates to Check Configuration Compliance

This chapter contains the following:

- What is a Baseline Template?
- Features of Baseline Templates
- Baseline Template Management Window
- Running Compliance Check
- Deploying a Baseline Template
- Using Compliance and Deploy Jobs Window

What is a Baseline Template?

Baselining refers to identifying a set of standardized policy based commands that you would want to have on a set of devices. You can create a Baseline template containing a set of commands identified through the baselining process. This template contains placeholders for device-specific values to be substituted.

For example:

```
set vtp domain [name] password [xxx]
set snmp community read-write [Read write community string]
```

Where `name`, `xxx` and `Read write community string` are variables that are substituted with the values you provide.

You can compare the Baseline template with the configuration of devices in the archive. You can also generate a non-compliance configuration report and deploy this template onto the devices to make it compliant. You can deploy a Baseline template to a group of devices by just scheduling one job.

When you add a new device of the same type to the network, you can use the existing Baseline template, which consists of two parts, command and values. You can create configurations for any device of the same type in the network by specifying the values for the variables in the Baseline template.
What is a Baseline Template?

**Sample Input file for Baseline Template**

You can use the following input file for creating Baseline template:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ConfigTemplate Name="Banner1" DeviceFamily="268437899,268438038" Version="1">
  <Commandlet Name="Commands" ControlStmt="false" Parent="none" Submode="false"
  Condition="false" Ordered="false">
    <CommandInfo CheckType="1">
      <Command>banner motd "******************** WARNING ****************************
      <NL>This is a private system and only authorized individuals are allowed!<NL>All
      others will be prosecuted to the fullest extent of the law!
      <NL>*****************************************************************************"****
    </CommandInfo>
    <ContextModeCommand />
    <PreCondition />
  </Commandlet>
</ConfigTemplate>
```
Handling Multi-line Commands in Baseline

Multi-line commands should be separated with <NL> tag and should be in the same line within the template.

You can use the following command to run the compliance check. This is considered as a single line command:

Below is the command that the customer can use in the compliance check for this use case. Please note this is a single line command.

```
+ banner motd "************************* WARNING **************************************
<NL> This is a private system and only authorized individuals are allowed! <NL> All others will be prosecuted to the fullest extent of the law! <NL> ***************************************************************************"
```

Features of Baseline Templates

The features of Baseline templates are:

- You can use this Baseline template to compare with other device configurations and generate a report that lists all the devices that are non-compliant with the Baseline template.
- You can easily deploy the Baseline template to the same category of devices in the network.
- You can schedule a compliance check job and deploy the Baseline template on the non-compliant devices. This can be performed as a single job or as a separate job.
- You can import or export a Baseline template. This template is stored in XML format.

Rules for Specifying Baseline Templates

The rules for specifying the Baseline templates are:

- All the commands that are disallowed should begin with a “-”.
- All commands that are mandatory should begin with a “+”.
- All comment entries should begin with a “#”.
- Commands that do not begin with (- or +) are considered as comments and ignored.
- The command values can be a wildcard match.

```
+ ip address [ip-address] [netmask]
+ ip address [10\.76\.38\.*\] [netmask]
+ ip address [10\.72\.*\.*\] [netmask]
```

To find a match for any octet in an IP address you must use \.\ *

In the examples shown above, the command will apply for all the devices with the IP address starting with 10.76.38.* [netmask] and 10.72.*.* [netmask].

- The regular expressions must be enclosed with #.

For example:

```
snmp-server location [.#\.*#]
```

This command will fail compliance check for snmp-server location loc1 loc2 loc3, because the check will be performed only for one word after snmp-server location.
To overcome this, you have to define the command as:

```
+ [# snmp-server location.*#]
```

Then the compliance check will be performed for all forms of snmp-server commands like
snmp-server location loc1 loc2......n, etc.

- **Negation in Regular expressions:**

  Example 1: When there are multiple entries in the configuration files.
  Let us say, the commands in the device configuration are:

  ```
  logging name1
  logging name2
  logging name3
  ```

  The command available in the template is:

  ```
  +logging [#!name1#]
  ```

  Based on the command in the template, the negation of name1 is done. This returns true as there are
  other logging commands present with other names. So the template is compliant.

  Example 2: When there is only one entry in the device configuration file.
  Let us say, the command in the device configuration is:

  ```
  logging name1
  ```

  The command available in the template is:

  ```
  +logging [#!name1#]
  ```

  Based on the command in the template, the negation of name1 is done. This returns False, as there
  is no other command in the device configuration file with logging statement except `logging name1`.
  So the template is non-compliant.

  Example 3: When there are no logging commands in the device configuration files.
  Let us say, the command in the device configuration is:

  ```
  No logging commands
  ```

  The command available in the template is:

  ```
  + logging [# !name1 #]
  ```

  Based on the command in the template, the negation of name1 is done. This returns False, as there
  are no login commands. So the template is non-compliant.

- The Baseline template uses java.util.regex engine for regular expressions. For more information, see
  the regex API guide for Java 1.4.2 from Oracle:

  [http://download.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html](http://download.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html)

- Submode commands are provided only if the commands are to be compared inside a submode.

  For example:

  ```
  interface [#Ethernet.*#]
  + no shutdown
  ```

  The no shutdown command will apply to all Ethernet interfaces.
Defining Commandsets

The commandsets are a set of one or more CLI commands. You can define a commandset while creating a Baseline template in the Advanced mode.

The features of the commandsets are:

- If the commands in commandset are in a submode (ip/interface) a submode command must be specified for such a commandset.
- Commandsets can have one or more child commandsets.
- Child commandsets inherit parent’s submode command.

You can define commandsets that have to be checked before running the actual commands.

The features of the prerequisite commandsets are:

- A commandset can have another commandset as its prerequisite.
- A prerequisite commandset is used only for comparison and is not deployed onto the device.
- A commandset is compared with the config only if its prerequisite condition is satisfied.

LMS evaluates the commandsets in different ways depending on whether you have defined the commandset as Parent or Prerequisite.

For example, assume that you have defined two commandsets, commandset1 and commandset2:

- Commandset defined as Prerequisite

  commandset1 as the Prerequisite of commandset2. When LMS evaluates the Baseline template, it evaluates commandset1 first, and commandset2 next.

  If commandset1 does not contain submode and is not present in a device, then commandset2 is not evaluated and the device is displayed in the excluded list in the compliance report.

  If commandset1 contains submode and is not present in applicable submodes, then commandset2 is not evaluated and the device is displayed in the excluded list in the compliance report.

- Commandset defined as Parent

  commandset1 as the Parent of commandset2. When LMS evaluates the Baseline template, it evaluates commandset1 first, and commandset2 next.

  If either of these commandsets are missing, the template is considered non-compliant.

Baseline Template Management Window

To access the Baseline Template Management Window go to Configuration > Compliance > Compliance Templates > Templates.

This window lists all the system-defined and user-defined Baseline templates. It also displays the following details of the Baseline template:
Baseline Template Management Window

### Chapter 7  Using Baseline Templates to Check Configuration Compliance

#### Baseline Template Management Window

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Name             | Name of the Baseline template. The following template examples are displayed, by default:  
|                  | • CISF_DHCP_Snooping—Template for Catalyst Integrated Security Feature  
|                  | • TemplateExample1—Basic template with Regular expression  
|                  | • TemplateExample2—Advanced template with Submode, Parent and child options  
|                  | • TemplateExample3—Advanced template with prerequisite options  
|                  | • TemplateExample4—Advanced template with ordered set options  
|                  | • VRFCompliance—Template for VRF Compliance  
|                  | Click the template name to view the command sets. For more information, see Command Sets.  

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Type of device for which the defined Baseline template can be used.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description of the Baseline template. If you have imported Baseline templates, the description given is Imported.</td>
</tr>
<tr>
<td>Created On</td>
<td>Displays the Baseline template creation date and time.</td>
</tr>
</tbody>
</table>

You can click on any column to sort the information by that column. If you double-click a heading, the order is reversed.

This window contains the following buttons:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| Edit    | Edit a Baseline template. This button is active only after you select a Baseline Template.  
|         | See Editing a Baseline Template for further details.  
| Export  | Export a Baseline template file. This button is active only after you select a Baseline Template.  
|         | See Exporting a Baseline Template for further details.  
| Delete  | Delete a Baseline template. This button is active only after you select a Baseline Template.  
|         | See Deleting a Baseline Template for further details.  
| Create  | Create a Baseline template. See Creating a Baseline Template for further details.  
| Import  | Import a Baseline template file. See Importing a Baseline Template for further details.  

Configuration Management with Cisco Prime LAN Management Solution 4.2

7-6
Command Sets

To view the template command sets:

### Step 1
Go to **Configuration > Compliance > Compliance Templates > Templates.**

The Baseline Templates window appears, displaying the list of all the user-defined Baseline templates.

### Step 2
Click the template name. For example, CISF_DHCP_Snooping.

The BaseLine Config Viewer window appears, displaying the command sets used in the template.

**Table 7-1** provides information on the command sets used in the template examples.

| Template               | Command Sets                                                                 | Name: Commands SubMode: No isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none                                                                                                      + ip dhcp snooping |
|------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| CISF_DHCP_Snooping     | Name: Commands SubMode: No isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none                                                                                                      + ip dhcp snooping |
| TemplateExample1       | Name: Commands SubMode: No isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none                                                                                                      + snmp-server community [.#.*#] RW |
| TemplateExample2       | Name: Global SubMode: No isPrerequisite: No Ordered: No Prerequisite-Commandset : none Parent: none                                                                                                          Name: parent SubMode: Yes isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none policy-map V3PN-teleworker Name: child SubMode: Yes isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: parent class VOICE + priority 64 |
| TemplateExample3       | Name: Global SubMode: No isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none                                                                                                          Name: prereq SubMode: No isPrerequisite: Yes Ordered: No Prerequisite-Commandset: none Parent: none                                                                 + class-map match-all GOLD Name: parent SubMode: Yes isPrerequisite: No Ordered: No Prerequisite-Commandset: prereq Parent: none policy-map GSB_Policy Name: child SubMode: Yes isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: parent class GOLD + bandwidth percent 25 |
## Table 7-1  Command Sets

<table>
<thead>
<tr>
<th>Template</th>
<th>Command Sets</th>
</tr>
</thead>
<tbody>
<tr>
<td>TemplateExample4</td>
<td>Name: Global SubMode: No isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none</td>
</tr>
<tr>
<td></td>
<td>Name: acceslist SubMode: No isPrerequisite: No Ordered: Yes Prerequisite-Commandset: none Parent: none</td>
</tr>
<tr>
<td></td>
<td>+ access-list 101 deny tcp 10.77.209.0 0.0.0.255 any</td>
</tr>
<tr>
<td></td>
<td>+ access-list 101 deny tcp any gt 1023 host 10.1.1.1 eq 23</td>
</tr>
<tr>
<td></td>
<td>+ access-list 101 permit ip any any</td>
</tr>
<tr>
<td>VRFCompliance</td>
<td>Name: Commands SubMode: Yes isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none interface [#.*#]</td>
</tr>
<tr>
<td></td>
<td>+ ip vrf forwarding [#red</td>
</tr>
</tbody>
</table>
Editing a Baseline Template

You can edit all Baseline template fields except for Template Name.

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To edit the Baseline templates:

Step 1 Select Configuration > Compliance > Compliance Templates > Templates.
The Baseline Templates dialog box appears.

Step 2 Select a Baseline template.

Step 3 Click Edit.
The Select Creation Mode dialog box appears. The mode that you have selected while creating the Baseline template is retained. You cannot change this mode.

• You can provide a description in the Description text field.
• You can select or deselect devices in the Device Type Selector listbox.

Step 4 Click Next.
The Add Template Details dialog box appears.

Step 5 Select the commandset that you want to edit.

Step 6 Edit the required information.
See Creating an Advanced Baseline Template for more information on field descriptions for the fields that appear in the Add Template Details dialog box.

Step 7 Click Finish.
A message appears, Template is modified. Do you wish to save the changes?

Step 8 Click OK.
A notification appears, Successfully updated the template BaselineTemplateName.

Step 9 Click OK to save changes.
Exporting a Baseline Template

You can export a Baseline template. The exported file is in XML format.
The default path in the LMS Server to which the XML file is exported to is:
- `NMSROOT\files\rme\dcma\baselinetemplates` (On Windows)
- `/var/adm/CSCOpx/files/rme/dcma/baselinetemplates` (On Solaris and Soft Appliance)
Where, `NMSROOT` is the LMS installed directory.
You cannot change the default export path in the LMS Server. If you do so, an error message will be displayed.

**Note**
View Permission Report (`Reports > System > Users > Permission`) to check if you have the required privileges to perform this task.

To export a Baseline Template:

**Step 1** Select `Configuration > Compliance > Compliance Templates > Templates`.
The Baseline Templates dialog box appears.

**Step 2** Select one or more Baseline templates and click **Export**.
The Export a Baseline Template dialog box appears.

**Step 3** Click **Browse**.
The Server Side File Browser dialog box appears.

**Step 4** Select a folder.

**Step 5** Click **OK** in the Server Side File Browser dialog box.

**Step 6** Click **OK**.
A message appears, CMA0086: Selected Template(s) are successfully exported.
The naming convention followed for the baseline parameter file is `Template Name.xml`.
The file will be exported to the default location at the specified path in XML format.
Deleting a Baseline Template

To delete a baseline template:

Note View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

---

**Step 1** Select Configuration > Compliance > Compliance Templates > Templates.

The Baseline Templates dialog box appears.

**Step 2** Select one or more Baseline templates and click **Delete**.

A message appears, **The selected Template will be permanently deleted**.

You can delete only user-defined templates and not system-defined templates.

**Step 3** Click **OK**.

A message appears, **Successfully deleted the template**.

**Step 4** Click **OK**.

The selected Baseline Template is removed from the Baseline Templates window

---

Note You cannot delete Example Templates.

Creating a Baseline Template

You can create a Baseline Template by:

- Creating a Basic Baseline Template
- Creating an Advanced Baseline Template

There are few example templates that are available. You can use these templates as a base to create new templates.

- Creating a Basic Baseline Template - an Example
- Creating an Advanced Baseline Template - an Example

Note View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.
Creating a Basic Baseline Template

To create a Basic Baseline template:

**Step 1** Select **Configuration > Compliance > Compliance Templates > Templates**.

The Baseline Templates window appears.

**Step 2** Click **Create**.

The Select Creation Mode dialog box appears.

**Step 3** In the Template Details section, select **Basic** as the mode.

**Step 4** Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Baseline template. You can enter up to 254 alphanumeric characters (including underscores). Do not enter special characters, including spaces and hyphens.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the Baseline template. You can enter up to 254 characters.</td>
</tr>
<tr>
<td>Device Type Selector</td>
<td>Device family to which you can apply this template. Click the check box to select the device family.</td>
</tr>
</tbody>
</table>

**Step 5** Click **Next**.

The Add Template Details dialog box appears.

**Step 6** Enter the following in the Baseline Template page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditional Block</td>
<td><strong>Check for compliance only if the following condition is satisfied.</strong> Check this option if you want to run a compliance check based on any condition.</td>
</tr>
<tr>
<td>Global</td>
<td>Select this option if you want to check the conditional commands in Global mode. This option is activated only if <strong>Check for compliance only if the following condition is satisfied</strong> is checked.</td>
</tr>
<tr>
<td>Submode</td>
<td>Select this option if you want to check the conditional commands in a specific submode. If you select this option, the textbox next to this option is activated. Enter the command for the required submode. For example: \texttt{interface [#Ethernet.#]} This option is activated only if the <strong>Check for compliance only if the following condition is satisfied</strong> option is checked.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**CLI Commands** | Enter the conditional CLI commands in this text area. This option is activated only if **Check for compliance only if the following condition is satisfied** is checked. Enter the Conditional CLI commands. For example:

```
# Routers CLI Commands
+ set snmp community read-write [read-write-community-name-string]
- set snmp community read-only public
```

Explanation:
- The first line is considered as a comment as it does not begin with either “+” or “-“.
- The second line is mandatory as it begins with “+”.
- The third line is disallowed as it begins with “-“.

In the above example, `read-write-community-name-string` is a command value. The command value should not contain spaces.

**Compliance Block**

<table>
<thead>
<tr>
<th>Global</th>
<th>Select this option if you want to check the compliance commands in global mode.</th>
</tr>
</thead>
</table>

**Use the SubMode of above condition**

This option is activated only if the Conditional Block options, **Check for compliance only if the following condition is satisfied** and the Submode options are selected.

The submode command entered in the submode textbox under the Conditional Block appears in the submode textbox of Compliance Block. So, the submode command of the Conditional Block is used by the Compliance Block.

You cannot edit the submode commands in the Compliance Block. However, you can edit the submode commands in the Conditional Block, which in turn updates the submode commands in the Compliance Block.

| Submode | Select this option if you want to check the compliance commands in a specific submode. If you select this option, the textbox next to this option is activated. Enter the command for the required submode. The compliance command will be checked for the submode that you enter. |
Chapter 7  Using Baseline Templates to Check Configuration Compliance

Baseline Template Management Window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI Commands</td>
<td>Enter the Compliance CLI commands. This is a mandatory field. For example, you can enter: Routers CLI Commands # this is the Compliance Block + set snmp community read-write [read-write-community-name-string] - set snmp community read-only public Explanation: • The first line is considered as a comment as it does not begin with either “+” or “-”. • The second line is also considered as a comment as it begins with “#”. • The third line is mandatory as it begins with “+”. • The fourth line is disallowed as it begins with “-”. In the above example, read-write-community-name-string is a command value. The command value should not contain spaces.</td>
</tr>
<tr>
<td>Order Sensitive</td>
<td>Select this option to make the system consider the order of the commands while performing a compliance check. In other words, the commands in the device config should appear in the same order as that of the CLI commands definition order in the Command Set.</td>
</tr>
</tbody>
</table>

- If you want to preview the changes to the template command details before the template is created, click Preview. The changed template details are displayed in a window.
- If you want to reset the changes click Reset.
- If you want to know about the options and the functionality of Basic flow click Help.

You can perform a Compliance check without using the Conditional Block.

A message appears, Successfully created the template BaselineTemplateName.

Where BaselineTemplateName is the Template Name as given by you.

Step 7  Click OK.

The Baseline Templates window appears with the newly created Baseline template.
Creating a Basic Baseline Template - an Example

You want to create a baseline template to check if all Ethernet interfaces that are up and running have "10.77.*.*" IP Address configured with the subnet mask 255.255.255.128.

To perform this task, you must create a template that checks for the following compliances:

- If there are interfaces that do not contain the `shutdown` command.
  and

- If all Ethernet interfaces are configured with IP address 10.77.*.* 255.255.255.128.

You can create a Basic Baseline Template by entering the condition check, as well as the compliance check.

To create a Basic Baseline Template for the above scenario:

**Step 1** Select *Configuration > Compliance > Compliance Templates > Templates*.

The Baseline Templates window appears.

**Step 2** Click *Create*.

The Select Creation Mode dialog box appears.

**Step 3** In the Template Details section, select *Basic* as the mode.

**Step 4** Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter <em>NewBaseline</em></td>
</tr>
<tr>
<td>Description</td>
<td>Enter the following description:</td>
</tr>
<tr>
<td></td>
<td><em>This is a Basic Baseline template that checks if all Ethernet interface are up and running and have &quot;10.77.</em>.<em>&quot; IP address configured with the subnet mask 255.255.255.128</em></td>
</tr>
<tr>
<td>Device Type Selector</td>
<td>Check the Routers checkbox to select all routers.</td>
</tr>
</tbody>
</table>

**Step 5** Click *Next*.

The Add Template Details dialog box appears.

**Step 6** Select *Check for compliance only if the following condition is satisfied* so that you can enter the condition to be checked.

**Step 7** Select *Submode*.

The textbox next to Submode is activated.

**Step 8** Enter the following command in the Submode textbox:

```
interface [#Ethernet.*#]
```

**Step 9** Enter the following Conditional CLI commands in the Conditional Block CLI command text area:

- shutdown

This command indicates that `shutdown` should not be present in the Ethernet interfaces.

**Step 10** Go to Compliance Block.

The *Use the SubMode of above condition* option is selected automatically.
Step 11 Enter the following CLI commands in the Compliance Block CLI command text area:
+  `ip address [#10.77.*.*] 255.255.255.128`
This command helps you to ascertain if the specified IP addresses are configured on the Ethernet interfaces.

Step 12 Click Finish
A message appears, **Successfully created the template NewBaseline.**
Where *NewBaseline* is the Template Name as entered by you.

Step 13 Click OK.
The Baseline Templates window appears with the newly created Baseline template.

---

### Creating an Advanced Baseline Template

To create an Advanced Baseline template:

Step 1 Select **Configuration > Compliance > Compliance Templates > Templates**.
The Baseline Templates dialog box appears.

Step 2 Click **Create**.
The select Creation Mode dialog box appears.

Step 3 Select **Advanced** as the mode from the Template Details section.

Step 4 Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Baseline template.</td>
</tr>
<tr>
<td></td>
<td>You can enter up to 254 alphanumeric characters (including spaces). Do not enter any special characters, including underscores and hyphens.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the Baseline template.</td>
</tr>
<tr>
<td></td>
<td>You can enter up to 254 characters.</td>
</tr>
<tr>
<td>Device Type Selector</td>
<td>Device family for which you can apply this template.</td>
</tr>
<tr>
<td></td>
<td>Check the check box to select the device family.</td>
</tr>
</tbody>
</table>

Step 5 Click **Next**.
The Add Template Details dialog box appears.

Step 6 Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commandset Options</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the commandset.</td>
</tr>
<tr>
<td></td>
<td>You can enter only alphanumeric characters up to 254 characters. Do not enter any special characters. This includes spaces, underscores and hyphens.</td>
</tr>
</tbody>
</table>
### Chapter 7 Using Baseline Templates to Check Configuration Compliance

#### Baseline Template Management Window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Parent      | Enter the parent name for the commandset, if required. This is case sensitive. You can also use this to logically group the commandsets. For example: To work on ATM permanent virtual connections (PVCs) commands, you must first get into the interface mode from the global mode and then run the PVC specific-commands. Commandset 1: ATM  
interface [#atm.*#]  
+ ip address [ip-addr] [net-mask]  
Commandset 2: PVC  
[#pvc.*#]  
+ encapsulation aal5 [encap-type]  
+ abr [output-pcr1] [output-mcr]  
+ ubr [output-pcr2]  
+ vbr-nrt [output-pcr3] [output-scr] [output-mbs]  
+ vbr-rt [peak-rate] [average-rate] [burst]  
+ protocol ip [proto-ip] [type]  
+ exit  
Here, commandset 1 is the parent for commandset 2. LMS evaluates the Baseline template, commandset 1 is evaluated first and commandset2 is evaluated next. If either of these commandsets is missing, the template is considered as non-compliant. |
| Prerequisite | Select the mandatory commandset name that you must enter before running the current commandset. In the example (See Mark as Prerequisite row), if you had marked commandset 1 as the Prerequisite, you can select commandset 1: IntCheck from the drop-down menu. Before running the commandset 2, the commandset 1 is run. That is, commandset1 is evaluated first and commandset2 is evaluated next. If there is no commandset1 or if commandset1 failed, commandset2 is not evaluated and the devices will be moved to excluded state. In this case, the template will be considered as non-compliant. |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Mark as Prerequisite   | 1. Select the checkbox to mark a particular commandset as a prerequisite.  
For example,  
Commandset 1: IntCheck  
```  
interface [intname]  
+ ip address [#10\76\38\.*#] [net-mask]  
(To find a match for any octet in an IP address you must use `\..*`)  
```  
2. Select the Mark as Prerequisite check box for the Commandset 1: IntCheck.  
For example,  
Commandset 2: IntDownload  
```  
interface [intname]  
+ no cdp enable  
```  
3. Select the Prerequisite from the dropdown menu for the Commandset 2: IntDownload.  
If a commandset has a Prerequisite commandset, you cannot select the Mark as Prerequisite check box for that particular commandset.  
That is, in the above example, you cannot select the checkbox Mark as Prerequisite for Commandset 2: IntDownload. |

### CLI Commands

| Submode    | Enter the command to get into interface mode from the global mode.  
For example: `interface [intname]`  
Here, `interface` is a command keyword and `intname` is command value. The command value should not contain spaces.  
You can also run the command for a set of interfaces.  
For example: `interface [#Ethernet.*#]`  
Here, the command will be executed on all the interfaces having Ethernet. |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------|
Chapter 7      Using Baseline Templates to Check Configuration Compliance

Baseline Template Management Window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ordered Set</td>
<td>Select this option to make the system consider the order of the commands while performing compliance check.</td>
</tr>
<tr>
<td></td>
<td>In other words, the commands in the device config should appear in the same order as that of the CLI commands definition order in the Command Set.</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">Behavior of Ordered Set for Access Lists</a> for more details.</td>
</tr>
<tr>
<td>CLI Commands</td>
<td>Enter the CLI commands.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td># Routers CLI Commands</td>
</tr>
<tr>
<td></td>
<td>+ set snmp community read-write [read-write-community-name-string]</td>
</tr>
<tr>
<td></td>
<td>- set snmp community read-only public</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong></td>
</tr>
<tr>
<td></td>
<td>• The first line is considered as a comment as it begins with a “#”.</td>
</tr>
<tr>
<td></td>
<td>• The second line is mandatory as it begins with “+”.</td>
</tr>
<tr>
<td></td>
<td>• The third line is disallowed as it begins with “-”.</td>
</tr>
<tr>
<td></td>
<td>There should be a space between the commands and the “-” or “+”. If there is no space, the commands are considered as comments and ignored.</td>
</tr>
<tr>
<td></td>
<td>In the above example, <code>read-write-community-name-string</code> is a command value. The command value should not contain spaces.</td>
</tr>
</tbody>
</table>

- If you want to add a new commandset to the template click **Add**. The CLI Commands window is displayed with the default help comments. These help comments serve as guidelines to create commandsets.
- If you want to delete a Commandset from the Command set list, click **Delete**.
- If you want to preview the changes to the Commandset details before finishing up the creation of the template, click **Preview**. The changed Commandset details is displayed in a window.
- If you click **Save**, for the first time, the following message appears,
  Do you wish to create a new template?
- If you click **Save**, for the second time, the following message appears,
  Successfully updated the template `BaselineTemplateName`.

**Note** If the Commandsets consist of Prerequisite commandset then these commandsets appear in red color in the Preview details.

- If you want to reset the changes made to a Commandset, click **Reset**

**Step 7** Click **OK**.
A message appears,

Successfully created the template `BaselineTemplateName`.
Where `BaselineTemplateName` is the name of the Baseline Template.
Baseline Template Management Window

**Chapter 7  Using Baseline Templates to Check Configuration Compliance**

**Step 8**  Click OK.
If you want to add one more commandset repeat this procedure from Step 4.

**Step 9**  Click Finish.
A message appears,
Do you wish to save the changes?

**Step 10**  Click OK.
A message appears,
Successfully created the template.

**Step 11**  Click OK.
The Baseline Configs window appears with all the available Baseline templates.

---

**Creating an Advanced Baseline Template - an Example**

This section consists of two examples:
- Example 1
- Example 2

**Example 1**
This is a procedure to create a Baseline template to disable CDP on an interface that belongs to a specific subnet.

**Step 1**  Select Configuration > Compliance > Compliance Templates > Templates.
The Baseline Templates dialog box appears.

**Step 2**  Click Create.
The Select Creation Mode dialog box appears.

**Step 3**  Select Advanced and click Next.
The Create a Baseline dialog box appears.

**Step 4**  Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>User data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>DisablingCDP &lt;br&gt;You can enter up to 254 alphanumeric characters. Do not enter any special characters, except underscores.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Routers</td>
</tr>
<tr>
<td>Description</td>
<td>Baseline Template for DisablingCDP</td>
</tr>
<tr>
<td>Commandset Option</td>
<td>PrerequisiteCheck &lt;br&gt;You can enter up to 254 alphanumeric characters. Do not enter any special characters including spaces, underscores and hyphens.</td>
</tr>
</tbody>
</table>
### Baseline Template Management Window

#### Step 5
Click **Save**.

A message appears to say that the template will be created.

#### Step 6
Click **OK**.

A message appears to say that the template is created.

#### Step 7
Click **OK**.

To add another commandset to the same Baseline template, Disabling-CDP, enter the following information.

#### Step 8
Click **Save**.

A message appears to say that the template is updated.
Step 9  Click **OK**.

Step 10 Click **Finish**.

A message appears to say that the template will be saved.

Step 11 Click **OK**.

A message appears to say that the template is updated.

Step 12 Click **OK**.

The Baseline Configs window appears with the details of Disabling-CDP Baseline template.

---

**Example 2**

This is a procedure to create an Advanced Baseline Template to check the presence of the command "ip address 10.77.209.8 255.255.255.224" in the Ethernet interfaces that have CDP disabled.

---

Step 1  Select **Configuration > Compliance > Compliance Templates > Templates**.

The Baseline Templates dialog box appears.

Step 2  Click **Create**.

The Select Creation Mode dialog box appears.

Step 3  Select **Advanced** and click **Next**.

The Create a Baseline dialog box appears.

Step 4  Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>User Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>CheckIPTemplate</td>
</tr>
<tr>
<td></td>
<td>You can enter up to 254 alphanumeric characters. Do not enter any special characters except underscores.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Routers</td>
</tr>
<tr>
<td>Description</td>
<td>Baseline Template for Interface level check.</td>
</tr>
<tr>
<td>Commandset Option</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>PrerequisiteCheck.</td>
</tr>
<tr>
<td></td>
<td>You can enter up to 254 alphanumeric characters. Do not enter any special characters including spaces, underscores and hyphens.</td>
</tr>
<tr>
<td>Parent</td>
<td>Do not enter anything.</td>
</tr>
<tr>
<td>Prerequisite</td>
<td>Do not select any value.</td>
</tr>
<tr>
<td>Mark as Prerequisite</td>
<td>Select the check box to mark the commandset as prerequisite.</td>
</tr>
<tr>
<td>CLI Commands</td>
<td>+ no cdp enable</td>
</tr>
</tbody>
</table>

---
Chapter 7  Using Baseline Templates to Check Configuration Compliance

Baseline Template Management Window

Step 5  Click **Save**.
A message appears to say that the template will be created.

Step 6  Click **OK**.
A message appears to say that the template is created.

Step 7  Click **OK**.
To add another commandset to the same Baseline template, CheckIPTemplate, enter the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>User data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Commandset Option</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Name                   | IPCheck.  
You can enter up to 254 alphanumeric characters. Do not enter any special characters including spaces, underscores and hyphens. |
| Parent                 | PrerequisiteCheck                                                        |
| Prerequisite           | Select the PrerequisiteCheck from the dropdown menu.                      |
| Mark as Prerequisite   | Do not select the checkbox.                                               |
| **CLI Commands**        |                                                                            |
| Submode                | Do not enter anything                                                     |
| Ordered Set            | Do not select the checkbox.                                               |
| CLI Commands           | + ipaddress 10.77.209.8 255.255.255.224                                     |
|                        | The above command will be deployed on the Ethernet interfaces that have CDP disabled. |

Step 8  Click **Save**.
A message appears to say that the template is updated.

Step 9  Click **OK**.

Step 10 Click **Finish**.
A message appears to say that the template will be saved.

Step 11 Click **OK**.
A message appears to say that the template is updated.

Step 12 Click **OK**.
The Baseline Configs window appears with the details of CheckIPTemplate Baseline template.
Baseline Template Management Window

Chapter 7 Using Baseline Templates to Check Configuration Compliance

Behavior of Ordered Set for Access Lists
1. Create a baseline template with few commands and ordered set option checked.
2. Compare the configurations in the device with the baseline template, to check for Compliance. The commands available in the device is compared in the same order as available in the Baseline template.
3. If the commands found in the device are not compliant with the Baseline template, the same configlet commands available in the device are negated first and then the commands available in the Baseline template are deployed on the device.

This is the recommended behavior for Access lists. This behavior is also supported by the submodes.

Importing a Baseline Template

You can import a template as Baseline template. The imported file must be in XML format.
The default path in the LMS Server from which the XML file is imported is:
- NMSROOT\files\rme\dcma\baselinetemplates (On Windows)
- /var/adm/CSCOpx/files/rme/dcma/baselinetemplates (On Solaris and Soft Appliance)

Where, NMSROOT is the LMS installed directory.

You cannot change the default import path in the LMS Server. If you do so, an error message will be displayed.

To import a Baseline Template:

Note: View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

Step 1 Select Configuration > Compliance > Compliance Templates > Templates.
The Baseline Templates dialog box appears.
Step 2 Select a Baseline template and click Import.
The Import a Baseline Template dialog box appears.
Click Browse.
The Server Side File Browser dialog box appears.
Step 3 Select the XML file.
Step 4 Click OK in the Server Side File Browser dialog box.
Step 5 Click OK.
A message appears, Template successfully imported.
Step 6 Click OK.
The imported file appears in the Baseline Templates window with the description, Imported baseline.
Running Compliance Check

To run a compliance check:

**Step 1** Select Configuration > Compliance > Compliance Templates > Compliance Check.

The Baseline Templates dialog box appears.

**Step 2** Select the template and click Compliance Check.

The Select Devices dialog box appears.

**Step 3** Select either:

- Device Selector, if you want to schedule a job for a static set of devices. See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to use the Device Selector.

  Or

- Group Selector, if you want to schedule a job for a dynamic group of devices.

  The job is scheduled only for the devices that are present in the selected group at the time when the job is run. The customizable group selector for jobs evaluate static groups also as dynamic during run time.

**Step 4** Click Next.

The Schedule dialog box appears.

**Step 5** Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>You can specify when you want to run the Baseline template compliance job.</td>
</tr>
<tr>
<td></td>
<td>To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs this task immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs this task once at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>• Daily—Runs daily at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly—Runs weekly on the specified day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Monthly—Runs monthly on the specified day of the month and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete.</td>
</tr>
<tr>
<td></td>
<td>For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed.</td>
</tr>
<tr>
<td></td>
<td>If the 10.00 a.m. November 1 job has not been completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.</td>
</tr>
<tr>
<td>Date</td>
<td>You can select the date and time (hours and minutes) at which to schedule.</td>
</tr>
<tr>
<td></td>
<td>The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.</td>
</tr>
</tbody>
</table>
### Running Compliance Check

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job Info</strong></td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.</td>
</tr>
<tr>
<td>Attachment</td>
<td>Check this option if you want the job notification mail to consist of attachments in either CSV or PDF format. Select either: • CSV if you want the attachment in CSV format. Or • PDF if you want the attachment in PDF format. This is the default format. The CSV and PDF radio options will be enabled only if the Attachment checkbox is checked. If the Attachment option is disabled, go to Admin &gt; System &gt; System Preferences to change the settings. For more information on configuring attachment settings as well as the maximum size of attachments allowed in notification mails, see Administration Online Help.</td>
</tr>
<tr>
<td><strong>Job Options</strong></td>
<td></td>
</tr>
<tr>
<td>Check compliance</td>
<td>Enable this to check the compliance of the archived file with that of the Baseline template and deploy the commands if it is non-compliant. This option is not supported for Group selector.</td>
</tr>
<tr>
<td>Copy Running Config to Startup</td>
<td>This option is active only if you select the Check compliance and deploy option. Select to make the job write the Running configuration to the Startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.</td>
</tr>
<tr>
<td>Job Password</td>
<td>• If you have enabled the Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin &gt; Network &gt; Configuration Job Settings &gt; Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin &gt; Network &gt; Configuration Job Settings &gt; Config Job Policies) either: – Enter the device login user name and password and device Enable password Or – Disable the Job Password option in the Job Schedule and Options dialog box.</td>
</tr>
</tbody>
</table>
Step 6  Click Next.

The Job Work Order window appears with the job details that you have selected.

Step 7  Click Finish.

A message appears, Job JobID is created successfully.

Where JobID is a unique Job number.

Step 8  Click OK.

You can check the status of your scheduled job by selecting Configuration > Job Browsers > Configuration Archive.

---

**Note**  View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this compliance check task.

The compliance check job requires approval if you have enabled Job Approval during the compliance check job scheduling.

For further details on the baseline template, see Understanding the Baseline Compliance Report.

### Understanding the Baseline Compliance Report

The Baseline Compliance Report contains the following information:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td></td>
</tr>
<tr>
<td>Template Name</td>
<td>Name of the Baseline template entered at the time of creating the Baseline template.</td>
</tr>
<tr>
<td>Number of Non-Compliant devices</td>
<td>Number of devices that are non-compliant.</td>
</tr>
<tr>
<td>Number of Compliant devices</td>
<td>Number of devices that are compliant.</td>
</tr>
<tr>
<td>Number of Excluded devices:</td>
<td>List of devices in which the job did not run. The jobs may have failed either because:</td>
</tr>
<tr>
<td></td>
<td>• The device configuration was not archived.</td>
</tr>
<tr>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>• The device was not reachable.</td>
</tr>
<tr>
<td></td>
<td>Further details of the failed job are given in the Configuration &gt; Job Browsers &gt; Configuration Archive (See Using Configuration Archive Job Browser).</td>
</tr>
<tr>
<td><strong>Compliant Devices</strong></td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository.</td>
</tr>
<tr>
<td>Latest Version</td>
<td>Version of configuration file against which the compliance was checked.</td>
</tr>
<tr>
<td></td>
<td>Click on the version to display Config Viewer (see Understanding the Config Viewer Window).</td>
</tr>
<tr>
<td></td>
<td>This shows the contents of the corresponding configuration file against which the compliance was checked.</td>
</tr>
</tbody>
</table>
Deploying a Baseline Template

When you add a new device of the same type to the network, you can use the existing Baseline template. This template consists of two parts, command and values.

You can create configurations for any device of the same type in the network by specifying the values for the variables in the Baseline template.

You can deploy Baseline template on the devices in two ways:

- User Interface (See Deploying a Baseline Template Using User Interface for the procedure.)
- File System (See Deploying a Baseline Template Using File System for the procedure.)

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

The deployment job requires approval if you have enabled Job Approval during the deployment job scheduling.

### Field Name | Description
--- | ---
Created On | Date and time at which the configuration file was created.

### Non-Compliant Devices

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository.</td>
</tr>
</tbody>
</table>
| Latest Version | Version of configuration file against which the compliance was checked. 
Click on the version to display Config Viewer (see Understanding the Config Viewer Window). This shows the contents of the corresponding configuration file against which the compliance was checked. |
| Created On | Date and time at which the configuration file was created. |
| Commands to Deploy | List the commands where the device configuration is non-compliant. |

### Excluded Devices

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device Name as entered in Device and Credential Repository.</td>
</tr>
<tr>
<td>Reason for Exclusion</td>
<td>Displays the cause for exclusion.</td>
</tr>
</tbody>
</table>

In addition, this report contains two buttons:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export to File (Icon)</td>
<td>Exports this report in either PDF or CSV format.</td>
</tr>
<tr>
<td>Print (Icon)</td>
<td>Generates a format that can be printed.</td>
</tr>
</tbody>
</table>
Deploying a Baseline Template Using User Interface

To deploy a Baseline template using User Interface:

**Step 1** Select Configuration > Compliance > Compliance Templates > Direct Deploy.
The Baseline Templates dialog box appears.

**Step 2** Select a Baseline template and click **Deploy**.
The Deploy Input Options dialog box appears.

**Step 3** Select **Enter Data From User Interface** and click **Next**.
The Select Devices dialog box appears.
The device list contains only devices of the type devices selected while creating the Baseline Template.
For example, if you have selected Device Type as Router, only routers are listed.

**Step 4** Select devices under the following tabs:
- In the All tab,
  Devices are grouped under All Applicable Devices and All Applicable Device Groups. All Applicable Device Groups categorizes devices under Routers, Switches, and so on.
- In the Search Results tab,
  The results of simple search and advanced search are listed here.
- In the Selection tab,
  All the devices that are selected are listed and you can deselect the devices.

**Step 5** Click **Next**.
The Select Devices dialog box appears.

**Step 6** Perform the following tasks:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description and Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device list</td>
<td>This pane lists the selected devices that you have selected in the Select Devices dialog box. Select the device for which you want to deploy the Baseline template.</td>
</tr>
<tr>
<td>Edit</td>
<td>Select a device from the device drop-down list and click <strong>Edit</strong> to edit information for the device.</td>
</tr>
<tr>
<td>Save</td>
<td>Click <strong>Save</strong> to save the changes made for the selected device. You can change the details for multiple devices in one go, by using the Save button.</td>
</tr>
<tr>
<td>Device</td>
<td>The selected device in the Device List pane is displayed in this text box.</td>
</tr>
<tr>
<td>Commandsets</td>
<td>The pane contains all the commandsets that are defined in the Baseline template. Select a commandset. While creating the Baseline template, if you have defined the multiple occurrences as the commandset feature, after selecting that particular commandset, the <strong>Add Instance</strong> button is activated.</td>
</tr>
</tbody>
</table>
### Deploying a Baseline Template

#### Step 7

Click **Next**.

The Job Schedule dialog box appears.

---

<table>
<thead>
<tr>
<th><strong>Field Name</strong></th>
<th><strong>Description and Action</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add Instance</strong></td>
<td>This button is active only if you have selected a commandset with multiple occurrences. The occurrences of a commandset are defined while creating the Baseline template. When you click on the Add Instance button, one more instance of multiple commandset is added in the Commandsets pane. Enter the command value for that commandset in the Device Data pane.</td>
</tr>
<tr>
<td><strong>Delete Instance</strong></td>
<td>Use the Delete Instance button to delete the instance after selecting the instance from the Commandsets pane. You can select one or more instances and click on the Delete Instance button to delete the instances. You can delete the selected instances. The exception being that at least one instance of the commandset is available.</td>
</tr>
<tr>
<td><strong>Templates</strong></td>
<td>The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.</td>
</tr>
</tbody>
</table>
| **Device Data** | The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command:  

```
Interface [#Ethernet[.]*]#
+ no shutdown
```

Then, `#Ethernet[.]*` is the command value. The Device Data field names appear as:  

```
#Ethernet.*[0]
```

If the commandset is a prerequisite commandset, you do not need to specify parameter values for the Device data field as they are not deployed. |
Step 8 Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
</tbody>
</table>
| Run Type    | You can specify when you want to run the Baseline template deploy job. To do this, select one of these options from the drop-down menu:  
• Immediate—Runs this task immediately.  
• Once—Runs this task once at the specified date and time.  
• Daily—Runs daily at the specified time.  
• Weekly—Runs weekly on the specified day of the week and at the specified time.  
• Monthly—Runs monthly on the specified day of the month and at the specified time.  
The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed.  
If the 10:00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3. |
| Date        | You can select the date and time (hours and minutes) to schedule the job. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field. |
| Job Info    |             |
| Job Description | Enter a description for the job. This is mandatory. You can enter only alphanumeric characters. |
| E-mail      | Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender’s address. |
| Job Options |             |
| Approver Comments | Enter comments for the job approver. This field appears only if you have enabled job approval for Configuration Archive. |
| Maker E-Mail | Enter the e-mail-ID of the job creator. This is a mandatory field. This field appears only if you have enabled job approval for Configuration Archive. |
Deploying a Baseline Template

You can deploy a Baseline template using the Baseline Parameter file.

The parameter file specifies the variable values for template deployment. To generate the parameter file:

**Step 1** Select **Configuration > Compliance > Compliance Templates > Templates**.

**Step 2** Click the hyperlink of the required template. The Baseline Config Viewer popup appears.

**Step 3** Click Generate Param File. A popup appears.

**Step 4** Click Browse to specify the folder with the parameter file.

---

See **Exporting a Baseline Template** for further information.
To deploy a Baseline template using File System:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <strong>Configuration &gt; Compliance &gt; Compliance Templates &gt; Direct Deploy.</strong> The Baseline Templates dialog box appears.</td>
</tr>
<tr>
<td>2</td>
<td>Select a Baseline template and click <strong>Deploy.</strong> The Deploy Input Options dialog box appears.</td>
</tr>
<tr>
<td>3</td>
<td>Select <strong>Enter Data From File System</strong> and click <strong>Next.</strong> The Select Input File dialog box appears.</td>
</tr>
</tbody>
</table>
| 4    | Enter the folder name and the file name with the file format extension XML. or  
  a. Click **Browse.** The Server Side File Browser dialog box appears.  
  b. Select the XML file.  
  c. Click **OK.** The Select Input File dialog box appears with the selected Baseline Parameter file. |
| 5    | Click **Next.** The Job Schedule dialog box appears. |
| 6    | Enter the following information: |

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Run Type | You can specify when you want to run the Baseline template deploy job.  
To do this, select one of these options from the drop-down menu:  
  • Immediate—Runs this task immediately.  
  • Once—Runs this task once at the specified date and time.  
  • Daily—Runs daily at the specified time.  
  • Weekly—Runs weekly on the specified day of the week and at the specified time.  
  • Monthly—Runs monthly on the specified day of the month and at the specified time.  
The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete.  
For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed.  
If the 10:00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3. |
| Date | You can select the date and time (hours and minutes) to schedule the job. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field. |
Deploying a Baseline Template

### Field Info

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Info</td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender’s address.</td>
</tr>
</tbody>
</table>
Deploying a Baseline Template

Step 7  Click Next.

The Work Order dialog box appears with job details that you have entered.

Step 8  Click Finish.

A message appears, Job JobID is created successfully.

Where JobID is a unique Job number.

If you have specified incorrect filename/XML file format or if the hostname field is not updated, an error message appears, Specified file could not be read. Please specify a valid file name.

See Exporting a Baseline Template for further information.

Check the XML file format or update the hostname field and restart this procedure from Step 2.

Step 9  Click OK.

You can check the status of your scheduled job using Configuration > Job Browsers > Configuration Archive. The Job Type for this deploy job is Deploy Baseline template result.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approver Comments</td>
<td>Enter comments for the job approver. This field appears only if you have enabled job approval for Configuration Archive.</td>
</tr>
<tr>
<td>Maker E-Mail</td>
<td>Enter the e-mail-ID of the job creator. This is a mandatory field. This field appears only if you have enabled job approval for Configuration Archive.</td>
</tr>
<tr>
<td>Copy Running Config to Startup</td>
<td>Select to make the job write the Running configuration to the Startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.</td>
</tr>
</tbody>
</table>
| Job Password               | • If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) enter the device login user name and password and device Enable password.  
                                            • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) either  
                                                – Enter the device login user name and password and device Enable password  
                                                Or  
                                                – Disable the Job Password option in the Job Schedule and Options dialog box. |

Field Options
Approver Comments Enter comments for the job approver.
This field appears only if you have enabled job approval for Configuration Archive.

Maker E-Mail Enter the e-mail-ID of the job creator. This is a mandatory field.
This field appears only if you have enabled job approval for Configuration Archive.

Copy Running Config to Startup Select to make the job write the Running configuration to the Startup configuration on each device after configuration changes are made successfully.
Does not apply to Catalyst OS devices.

Job Password
• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) enter the device login user name and password and device Enable password.
• If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) either
  – Enter the device login user name and password and device Enable password
  Or
  – Disable the Job Password option in the Job Schedule and Options dialog box.
Using Compliance and Deploy Jobs Window

You can check the status of the Baseline jobs using Configuration > Compliance > Compliance Templates > Jobs.

This section contains:

• Deploying the Commands
• Deleting the Compliance Jobs

This window contains the following information:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique number assigned to the job when it is created. For periodic jobs such as Daily, Weekly, the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001.</td>
</tr>
<tr>
<td>Description</td>
<td>Job description entered during job definition.</td>
</tr>
<tr>
<td>Compliant/Deployed Devices</td>
<td>Displays the number of devices that are compliant out of the total number of devices that were selected while creating the compliance job. See Understanding the Baseline Compliance Report to view the Baseline Compliance Report.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the job. The status can be Successful, Failed, and Running. The jobs may have failed either because: • The device configuration is not archived. Or • The device is not reachable. Further details of the failed job are given in the Configuration &gt; Job Browsers &gt; Configuration Archive. You can also check the status of the Baseline job at Configuration &gt; Job Browsers &gt; Configuration Archive.</td>
</tr>
</tbody>
</table>

The Baseline Jobs window contains the following buttons:

<table>
<thead>
<tr>
<th>Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy</td>
<td>You can schedule a job to deploy the standard configuration on all non-compliant devices. This button is active only after selecting a Job. See Deploying the Commands.</td>
</tr>
<tr>
<td>Retry</td>
<td>You can reschedule a failed job using this button. This button is active only on selecting a Failed job. Reschedule the deployment job by providing the required information.</td>
</tr>
</tbody>
</table>
Chapter 7      Using Baseline Templates to Check Configuration Compliance

Using Compliance and Deploy Jobs Window

Deploying the Commands

You can deploy the commands on the devices that are non-complaint. Before you use this Deploy button, you must run the Compliance Report,

- If there are any non-complaint device, you must select the relevant compliance job and deploy the baseline template.
- If there are no non-complaint device and if you click on the Deploy button, a message appears,
  Could not deploy selected Job.
  Reason: No Non-Compliant devices present in the report.
  Click on the Job ID to view the Baseline Compliance Report. See Understanding the Baseline Compliance Report for further details.

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To deploy the commands:

Step 1  Select Configuration > Compliance > Compliance Templates > Jobs.

The Baseline Jobs dialog box appears.

Step 2  Select a Compliance Job.

Step 3  Click Deploy.

The Substitute Parameters for Devices dialog box appears.

Step 4  Perform the following:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description and Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device list</td>
<td>The list contains all the devices which are non-complaint. Select a device.</td>
</tr>
<tr>
<td>Device</td>
<td>The selected device in the Device List pane appears in this text box.</td>
</tr>
</tbody>
</table>
Chapter 7  Using Baseline Templates to Check Configuration Compliance

Using Compliance and Deploy Jobs Window

If you have more than one device to deploy then you have to repeat Step 4 for all the devices.

Step 5  Click Next.

The Job Schedule dialog box appears.

Step 6  Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commandsets</td>
<td>The pane contains all the commandsets that are defined in the Baseline template. In the Baseline template, if you have defined the multiple occurrences as the commandset feature then based on the compliance check, the commandset will appear more than once. Select a commandset.</td>
</tr>
<tr>
<td>Templates</td>
<td>The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.</td>
</tr>
</tbody>
</table>
| Device Data         | The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command: 
+ ip address [#10.76.38.*] [netmask]
Then, #10.76.38.*# and netmask are the command values. The Device Data field names appear as: 
#10.76.38.*#[1000]
netmask[1000] |

Field Name | Description and Action
--- | ---
Commandsets | The pane contains all the commandsets that are defined in the Baseline template. In the Baseline template, if you have defined the multiple occurrences as the commandset feature then based on the compliance check, the commandset will appear more than once. Select a commandset.

Templates | The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.

Device Data | The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command: 
+ ip address [#10.76.38.*] [netmask]
Then, #10.76.38.*# and netmask are the command values. The Device Data field names appear as: 
#10.76.38.*#[1000]
netmask[1000]

Field Name | Description and Action
--- | ---
Commandsets | The pane contains all the commandsets that are defined in the Baseline template. In the Baseline template, if you have defined the multiple occurrences as the commandset feature then based on the compliance check, the commandset will appear more than once. Select a commandset.

Templates | The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.

Device Data | The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command: 
+ ip address [#10.76.38.*] [netmask]
Then, #10.76.38.*# and netmask are the command values. The Device Data field names appear as: 
#10.76.38.*#[1000]
netmask[1000]

Field Name | Description and Action
--- | ---
Commandsets | The pane contains all the commandsets that are defined in the Baseline template. In the Baseline template, if you have defined the multiple occurrences as the commandset feature then based on the compliance check, the commandset will appear more than once. Select a commandset.

Templates | The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.

Device Data | The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command: 
+ ip address [#10.76.38.*] [netmask]
Then, #10.76.38.*# and netmask are the command values. The Device Data field names appear as: 
#10.76.38.*#[1000]
netmask[1000]

Field Name | Description and Action
--- | ---
Commandsets | The pane contains all the commandsets that are defined in the Baseline template. In the Baseline template, if you have defined the multiple occurrences as the commandset feature then based on the compliance check, the commandset will appear more than once. Select a commandset.

Templates | The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.

Device Data | The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command: 
+ ip address [#10.76.38.*] [netmask]
Then, #10.76.38.*# and netmask are the command values. The Device Data field names appear as: 
#10.76.38.*#[1000]
netmask[1000]

Field Name | Description and Action
--- | ---
Commandsets | The pane contains all the commandsets that are defined in the Baseline template. In the Baseline template, if you have defined the multiple occurrences as the commandset feature then based on the compliance check, the commandset will appear more than once. Select a commandset.

Templates | The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.

Device Data | The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command: 
+ ip address [#10.76.38.*] [netmask]
Then, #10.76.38.*# and netmask are the command values. The Device Data field names appear as: 
#10.76.38.*#[1000]
netmask[1000]

Field Name | Description and Action
--- | ---
Commandsets | The pane contains all the commandsets that are defined in the Baseline template. In the Baseline template, if you have defined the multiple occurrences as the commandset feature then based on the compliance check, the commandset will appear more than once. Select a commandset.

Templates | The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.

Device Data | The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command: 
+ ip address [#10.76.38.*] [netmask]
Then, #10.76.38.*# and netmask are the command values. The Device Data field names appear as: 
#10.76.38.*#[1000]
netmask[1000]

Field Name | Description and Action
--- | ---
Commandsets | The pane contains all the commandsets that are defined in the Baseline template. In the Baseline template, if you have defined the multiple occurrences as the commandset feature then based on the compliance check, the commandset will appear more than once. Select a commandset.

Templates | The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.

Device Data | The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command: 
+ ip address [#10.76.38.*] [netmask]
Then, #10.76.38.*# and netmask are the command values. The Device Data field names appear as: 
#10.76.38.*#[1000]
netmask[1000]
### Chapter 7 Using Baseline Templates to Check Configuration Compliance

#### Using Compliance and Deploy Jobs Window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job Info</strong></td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.</td>
</tr>
<tr>
<td><strong>Attachment</strong></td>
<td>Check this option if you want the job notification mail to consist of attachments in either CSV or PDF format. Either select:</td>
</tr>
<tr>
<td></td>
<td>• CSV if you want the attachment in CSV format.</td>
</tr>
<tr>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>• PDF if you want the attachment in PDF format. This is the default format. The CSV and PDF radio options will be enabled only if the Attachment checkbox is checked. If the Attachment option is disabled, go to Admin &gt; System &gt; System Preferences to change the settings. For more information on configuring attachment settings as well as the maximum size of attachments allowed in notification mails, see Administration Online Help.</td>
</tr>
<tr>
<td><strong>Job Options</strong></td>
<td></td>
</tr>
<tr>
<td>Approver Comments</td>
<td>Enter comments for the job approver. This field appears only if you have enabled job approval for Configuration Archive.</td>
</tr>
<tr>
<td>Maker E-Mail</td>
<td>Enter the e-mail-ID of the job creator. This is a mandatory field. This field appears only if you have enabled job approval for Configuration Archive.</td>
</tr>
<tr>
<td>Copy Running Config to Startup</td>
<td>Select to make the job to write the Running configuration to the Startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.</td>
</tr>
<tr>
<td><strong>Job Password</strong></td>
<td>• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin &gt; Network &gt; Configuration Job Settings &gt; Config Job Policies) enter the device login user name and password and device Enable password.</td>
</tr>
<tr>
<td></td>
<td>• If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin &gt; Network &gt; Configuration Job Settings &gt; Config Job Policies) either:</td>
</tr>
<tr>
<td></td>
<td>– Enter the device login user name and password and device Enable password Or</td>
</tr>
<tr>
<td></td>
<td>– disable the Job Password option in the Job Schedule and Options dialog box.</td>
</tr>
</tbody>
</table>

#### Step 7

Click **Next**.

The Work Order dialog box appears with job details that you have entered.
Step 8  Click Finish.
A message appears, Job ID is created successfully.
Where ID is a unique Job number.

Step 9  Click OK.
You can check the status of your scheduled job using Configuration > Job Browsers > Configuration Archive. The Job Type for this deploy job is Deploy Baseline comparison result.

Deleting the Compliance Jobs

You can delete the job that have been completed or stopped. You cannot delete a running job.

Note  View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To delete Compliance jobs:

Step 1  Select Configuration > Compliance > Compliance Templates > Jobs.
The Compliance Jobs dialog box appears.

Step 2  Select a job and click Delete.
A message appears, The selected job will be deleted.

Step 3  Click OK.
The selected Compliance job is removed from the Compliance Jobs window.

You can also delete the compliance jobs from Configuration > Job Browsers > Configuration Archive window (see Using Configuration Archive Job Browser)
Chapter 7  Using Baseline Templates to Check Configuration Compliance

Using Compliance and Deploy Jobs Window
CHAPTER 8

Editing and Deploying Configurations Using Config Editor

The Config Editor provides easy access to configuration files. Config Editor allows a network administrator with the appropriate security privileges to edit a configuration file that exists in the configuration archive.

The Configuration Management application stores the current and a user-specified number of previous versions of the configuration files for all supported Cisco devices maintained in the Inventory. It automatically tracks changes to configuration files and updates the database if a change is made.

You can open the configuration file, change it, and download it to the device.

- To start Config Editor from the LMS desktop, select Configuration > Tools > Config Editor. The Config Editor window appears.
- To set user preferences in Config Editor, select Configuration > Tools > Config Editor > Edit Mode Preference. The User Preferences window appears.

This chapter contains:

- Config Editor Tasks
- Benefits of Configuration Editor
- Setting Up Preferences
- Overview: Editing a Configuration File
- Working With the Configuration Editor
- Removing a Configuration File
- Saving a Configuration File
- Undoing All
- Replacing All
- Printing a Configuration File
- Exporting Changes of a Configuration File
- Deploying a Configuration File
- Closing a Configuration File
- Selecting Configuration Tools
- Comparing Versions of Configuration Files
Config Editor Tasks

Config Editor users can:

- Open a configuration file version of a device for editing.
- Open configuration file version based on search criteria.
- Open an external configuration file.
- Save modified configuration file in private work area on the server and open the saved file when required.
- Save a configuration file in a public location.
- Send configuration file to syntax checker utility.
- Deploy configuration files to the device.
- Send configuration download jobs for approval.
- View all download jobs and perform job management operations.
- List out all the modified files, allow the user to select and download or close the configuration.
- Compare configurations that they are editing with the original configuration file version and other configuration versions of the selected device.
- Open a baseline configuration stored in config archive.
Benefits of Configuration Editor

Config Editor allows you to edit and download configuration files to devices using a GUI instead of the command line interface (CLI). Use Config Editor to edit individual device configurations within LMS and then download them again to the device.

A copy of the updated configuration will automatically be stored in the Configuration Archive. See Figure 8-1.

Figure 8-1 Config Editor Functional Flow

![Config Editor Functional Flow Diagram](image)

Table 8-1 shows the tasks you can accomplish with the Config Editor option.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open a configuration file.</td>
<td>Open a configuration file for editing. You can open a configuration file in four ways:</td>
<td>Select <strong>Configuration &gt; Tools &gt; Config Editor</strong> &gt; <strong>Config Editor</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Device and Version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Pattern Search</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Baseline</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• External Location</td>
<td></td>
</tr>
<tr>
<td>Edit configuration files from the archives.</td>
<td>Edit a configuration file from the archive.</td>
<td>Select <strong>Configuration &gt; Tools &gt; Config Editor</strong> &gt; <strong>Config Editor</strong> &gt; <strong>Device and Version</strong> &gt; <strong>Edit</strong>.</td>
</tr>
</tbody>
</table>

Table 8-1 Config Editor Tasks
Table 8-1  Config Editor Tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit a configuration file by pattern</td>
<td>Edit a configuration file by searching for a pattern. A pattern can be any text string.</td>
<td>Select Configuration &gt; Tools &gt; Config Editor &gt; Config Editor &gt; Pattern Search &gt; Finish.</td>
</tr>
<tr>
<td>Edit a configuration file by baseline template</td>
<td>Create a baseline configuration from the baseline template maintained in configuration archive.</td>
<td>Select Configuration &gt; Tools &gt; Config Editor &gt; Config Editor &gt; Baseline &gt; Finish.</td>
</tr>
<tr>
<td>Edit a configuration file by external location</td>
<td>Associate a device with the selected configuration file from an external location in the server.</td>
<td>Select Configuration &gt; Tools &gt; Config Editor &gt; Config Editor &gt; External Location &gt; Edit.</td>
</tr>
<tr>
<td>Print configuration files</td>
<td></td>
<td>1. Select Configuration &gt; Tools &gt; Config Editor &gt; Config Editor.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the configuration file and click Edit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select the Print icon at the top right corner.</td>
</tr>
<tr>
<td>Remove configuration file from the private area</td>
<td>Remove a configuration file from the private work area on the server.</td>
<td>1. Select Configuration &gt; Tools &gt; Config Editor &gt; Private Configs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the configuration file and click Delete.</td>
</tr>
<tr>
<td>Remove a configuration from the public work area</td>
<td>Remove a configuration file from the public work area on the server.</td>
<td>1. Select Configuration &gt; Tools &gt; Config Editor &gt; Public Configs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the configuration file and click Delete.</td>
</tr>
<tr>
<td>Save a configuration file in the public work area</td>
<td>Save an edited configuration file in the public work area on the server and retrieve the saved file when required.</td>
<td>1. Select Configuration &gt; Tools &gt; Config Editor &gt; Public Configs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the configuration file and click Edit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click Save.</td>
</tr>
<tr>
<td>Save a configuration file in the private work area</td>
<td>Save an edited configuration file in the private work area on the server and retrieve the saved file when required.</td>
<td>1. Select Configuration &gt; Tools &gt; Config Editor &gt; Private Configs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the configuration file and click Edit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click Save.</td>
</tr>
<tr>
<td>Undo editing or typing changes</td>
<td>Undo editing or typing changes when editing a file. You can undo editing changes of files in private or public work areas.</td>
<td>To undo editing changes of a file in the private work area:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Select Configuration &gt; Tools &gt; Config Editor &gt; Private Configs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the configuration file and click Edit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click Undo All.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To undo editing changes of a file in the public work area:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Select Configuration &gt; Tools &gt; Config Editor &gt; Public Configs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the configuration file and click Edit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click Undo All.</td>
</tr>
</tbody>
</table>
### Benefits of Configuration Editor

- **Find and replace text:** Find and replace all occurrences of the text when editing a configuration file in the Raw mode or find the text in a particular configlet in the Processed mode.
  - To find and replace text of a file in the private work area:
    1. Select **Configuration > Tools > Config Editor > Private Configs**
    2. Select the configuration file and click **Edit**.
    3. Click **Replace All**.
  - To find and replace text of a file in the public work area:
    1. Select **Configuration > Tools > Config Editor > Public Configs**.
    2. Select the configuration file and click **Edit**.
    3. Click **Replace All**.

- **Export Configuration File Changes:** Exporting Changes of a Configuration File to a PDF file.
  - 1. Select **Configuration > Tools > Config Editor > Config Editor**.
  - 2. Select the configuration file and click **Edit**.
  - 3. Select the **Export icon** at the top right corner.

- **Close Configuration File:** Close a configuration file.
  - To close a configuration file in the private work area:
    1. Select **Configuration > Tools > Config Editor > Private Configs**.
    2. Select the configuration file and click **Edit**.
    3. Click **Close**.
  - To close a configuration file in the public work area:
    1. Select **Configuration > Tools > Config Editor > Public Configs**.
    2. Select the configuration file and click **Edit**.
    3. Click **Close**.

- **Configure Job Policies:** Configure a default policy for job properties that applies to all future jobs. You can also specify whether the property can be modified when the job is created.
  - Select **Admin > Network > Configuration Job Settings > Config Job Policies**.
### Benefits of Configuration Editor

Config Editor remembers your preferred mode even across different invocations of the application. You can also change the mode when you open a configuration file using the Device and Version option. However, Config Editor does not remember this change across different invocations of the application. Only the changes made using the Admin function are remembered.

### Table 8-1  Config Editor Tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
</table>
| Set up the default editing mode. | Set up or change your default editing preferences.  
Config Editor remembers your preferred mode even across different invocations of the application.  
You can also change the mode when you open a configuration file using the Device and Version option.  
However, Config Editor does not remember this change across different invocations of the application. Only the changes made using the Admin function are remembered. | Select Configuration > Tools > Config Editor > Edit Mode Preference. |
| View changes              | View the changes made to the opened configuration file. LMS compares the edited file with the original version. | To view changes made to a configuration file in the private work area:  
1. Select Configuration > Configuration > Config Editor > Private Configs.  
2. Select the configuration file and click **Edit**.  
3. Click **Tools**.  
4. Select **View Changes**.  
To view changes made to a configuration file in the public work area:  
1. Select **Configuration > Tools > Config Editor > Public Configs**.  
2. Select the configuration file and click **Edit**.  
3. Click **Tools**.  
4. Select **View Changes**. |
### Benefits of Configuration Editor

To compare versions of configuration files in the private work area:

1. Select **Configuration > Tools > Config Editor > PrivateConfigs**.
2. Select the configuration file and click **Edit**.
3. Click **Tools**.
4. Select **Compare Config**.

To compare versions of configuration files in the public work area:

1. Select **Configuration > Tools > Config Editor > PublicConfigs**.
2. Select the configuration file and click **Edit**.
3. Click **Tools**.
4. Select **Compare Config**.

### Table 8-1 Config Editor Tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compare versions of the configuration files.</td>
<td>Compare the edited files with any version in the Configuration Archive.</td>
<td>To compare versions of configuration files in the private work area:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Select <strong>Configuration &gt; Tools &gt; Config Editor &gt; PrivateConfigs</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the configuration file and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click <strong>Tools</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Select <strong>Compare Config</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To compare versions of configuration files in the public work area:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Select <strong>Configuration &gt; Tools &gt; Config Editor &gt; PublicConfigs</strong>.</td>
</tr>
<tr>
<td>View list of modified files.</td>
<td>View a list of files edited by all users in private or public work areas.</td>
<td>To view a list of modified configuration files in private work area, select <strong>Configuration &gt; Tools &gt; Config Editor &gt; PrivateConfigs</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To view a list of modified configuration files in private work area, select <strong>Configuration &gt; Tools &gt; Config Editor &gt; PrivateConfigs</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To view a list of modified configuration files in public work area, select <strong>Configuration &gt; Tools &gt; Config Editor &gt; PublicConfigs</strong>.</td>
</tr>
<tr>
<td>Browse and edit Config Editor jobs.</td>
<td>Browse the Config Editor jobs that are registered on the system and edit them as necessary.</td>
<td>Select <strong>Configuration &gt; Job Browsers &gt; Config Editor &gt; Edit</strong>.</td>
</tr>
<tr>
<td>View job details.</td>
<td>View detailed information about a registered Config Editor job and perform job management operations.</td>
<td>Select <strong>Configuration &gt; Job Browsers &gt; Config Editor</strong>.</td>
</tr>
<tr>
<td>Deploy a config</td>
<td>Define a deploy job. Defines jobs to deploy configuration files to the device.</td>
<td>Select <strong>Configuration &gt; Job Browsers &gt; Config Editor &gt; Create</strong>.</td>
</tr>
<tr>
<td>Copy a job</td>
<td>Copy a job</td>
<td>Select <strong>Configuration &gt; Job Browsers &gt; Config Editor &gt; Copy</strong>.</td>
</tr>
<tr>
<td>Delete a job</td>
<td>Delete a job</td>
<td>Select <strong>Configuration &gt; Job Browsers &gt; Config Editor &gt; Delete</strong>.</td>
</tr>
<tr>
<td>Stop a job</td>
<td>Stop a job</td>
<td>Select <strong>Configuration &gt; Job Browsers &gt; Config Editor &gt; Stop</strong>.</td>
</tr>
</tbody>
</table>
Setting Up Preferences

You can use this feature to set up your editing preferences. Config Editor remembers your preferred mode, even across different invocations of the application.

You can change the mode using the Device and Version, Pattern Search, Baseline or External Configuration option but the changes do not affect the default settings.

To set up preferences:

**Step 1**
Select **Configuration > Tools > Config Editor > Edit Mode Preference**. The User Preferences dialog box appears.

**Step 2**
Set the default edit mode:
- Select **Processed** to display the file in the Processed mode.
  
  The configuration file appears at the configlet level (a set of related configuration commands). The default edit mode is Processed.

- Select **Raw** to display the file in the Raw mode.
  
  The entire file appears as shown in the device.

**Step 3**
Click **Apply** to apply the specified preferences.
Overview: Editing a Configuration File

The Editor is a core component in Config Editor. It acts as the interface to open a configuration file, make a local copy, save the changed configuration and commit the changes back to the original location.

You can edit a file by:

- Selecting the device and the version of the configuration file
- Searching for a pattern
- Selecting a baseline configuration file
- Selecting a configuration file stored in an external location

You can edit a previously opened file, that is, a file from your private area or public work area.

You can edit the files in either the Raw or Processed mode.

- Raw mode—The entire file is displayed. After you open a file in a specific mode, you can view it only in that mode.
- Processed mode—Only the file commands are displayed at the configlet (set of related configuration commands) level.

Working With the Configuration Editor

You can use the editor to:

- Edit and save changes to the configuration file in public or private work area.
- Undo editing or typing changes
- Replace a string in opened configuration files
- Compare configuration files with the same device configuration
- View changes made in the configuration file
- Run Syntax Checker

This section contains:

- Processed Mode
- Raw Mode
- Editing Configuration Files by Handling Interactive Commands in Config Editor Jobs
- Modifying Credentials

The Editor window opens in Raw or Processed mode, based on your preference.

To launch the Editor:

Step 1  Select Configuration > Tools > Config Editor > Config Editor.

Step 2  Open a configuration file using any of the following methods:

- Using the selection criteria. See Overview: Opening a Configuration File
- Using Private Configs
- Using Public Configs
Using Private Configs

a. Select Configuration > Tools > Config Editor > Private Configs to open a configuration file stored in a private work area.

The List of Private Configs window appears.

LMS converts the character “:” in the IPv6 address to “%03A”. The Archive Name field in the List of Private Configs window might not display the actual IPv6 address.

b. Select the configuration and click Edit.

Using Public Configs

a. Select Configuration > Tools > Config Editor > Public Configs to open a configuration file stored in public work area.

The User Archived Configs window appears.

LMS converts the character “:” in the IPv6 address to “%03A”. The Name field in the User Archived Configs window might not display the actual IPv6 address.

b. Select the configuration and click Edit.

Step 3  Edit the credential commands in the Raw or Processed mode. See Processed Mode and Raw Mode.

Step 4  Select any of the following:

- Save to save changes to the configuration file. See Saving a Configuration File.
- Save As to save changes to the configuration file in a specified location.
- Undo All to undo editing or typing changes. See Undoing All.
- Replace All to replace a string in the opened configuration files. See Replacing All.
- Deploy to deploy a configuration file to a device.
- Tools... to launch the Config Editor tools. See Selecting Configuration Tools.
- Close to close the Config Editor window. See Closing a Configuration File.

Processed Mode

The configuration file appears at the configlet level (a set of related configuration commands). The default is Processed.

In the Processed mode, Editor window is divided into two panes.

- The left pane displays the configuration tree according to the grouping of configlets.
- The right pane displays the commands of configlets in two sections:
  - The lower section, called the credential area contains all the credential commands with the credentials masked. Click on the encrypted link to modify credentials.
  - The upper section, called the non-credential area contains only non-credential commands. The non-credential commands are editable.
Raw Mode

The entire file appears as shown in the device. After you open a file in a specific mode, you can view it only in that mode.

In Raw mode there are two sections for the entire configuration.

- The upper section, called the non-credential area, contains only non-credential commands. The non-credential commands are editable.
- The lower section contains all the credential commands with the credentials masked. The credential commands can be edited.

Note: Do not delete or edit the placeholder that describes the credential position. If you do so, the file generates errors.

Editing Configuration Files by Handling Interactive Commands in Config Editor Jobs

An interactive command is the input you will have to enter, after a command runs.

For example, in the case of Catalyst 5000 series devices, interactive command would be:

```
set vtp v2 enable
```

This command enables version 2 of VTP on the device. This command is an interactive command and requires user intervention after running the command.

You can download this command through ConfigEditor using:

```
#INTERACTIVE
set vtp v2 enable
<RETURN>
#ENDS_INTERACTIVE
```

Such commands can be included in config jobs run using a Config Editor. You can handle interactive commands by editing configuration files.

To edit configuration files using interactive commands:

Step 1
Select Configuration > Tools > Config Editor > Private Configs to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select Configuration > Tools > Config Editor > Public Configs to open a configuration file stored in public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2
Click Edit.

The Editor window appears.
Step 3  Enter an interactive command in the configuration file, in the upper section that contains only non-credential commands using the following syntax:

```
#INTERACTIVE
command1<R>response1<R>response2
command2<R>response1<R>response2<R>response3
command3<R>response1
command4<R>response1<R>response2
#ENDS_INTERACTIVE
```

<R> tag is case-sensitive and this must be entered in uppercase only.

Step 4  Enter modification comments in the Change Description field.

---

**Modifying Credentials**

You can use this feature to modify or delete the credentials of a configuration file. To do this:

Step 1  Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location.

For more details see, **Overview: Opening a Configuration File**.

Step 2  Click **Edit**.

The Editor window appears.

Step 3  Click the masked credential link in the With Credentials pane. (The masked credential appears as multiple *s.)

The Modify Credentials dialog box appears.

Step 4  Enter the information required to modify credentials.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify</td>
<td>Modifies credentials of the selected configlets.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the existing credentials of the selected configlets.</td>
</tr>
<tr>
<td><strong>Modify Mode</strong></td>
<td></td>
</tr>
<tr>
<td>Old Credential</td>
<td>Old credential appears in clear text in a non-editable text box.</td>
</tr>
</tbody>
</table>
Removing a Configuration File

You can use this feature to remove configuration files from a private work area or a public work area using Config Editor.

To remove a configuration file stored in the private work area:

| Step 1          | Select **Configuration > Tools > Config Editor > Private Configs.**
|-----------------|---------------------------------------------------------------
| Step 2          | The List of Private Configs window appears.                  |
| Step 3          | Select the configuration files that need to be removed.      |
|                 | Click **Delete.**                                            |

To remove a configuration file stored in the public work area or the user archive:

| Step 1          | Select **Configuration > Tools > Config Editor > Public Configs.**
|-----------------|---------------------------------------------------------------
| Step 2          | The Public Configs window appears.                           |
| Step 3          | Select the configuration files that need to be removed.      |
|                 | Click **Delete.**                                            |

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, **Overview: Opening a Configuration File.**
Saving a Configuration File

You can use this feature to save your changes to the configuration file. The changes can be saved in either a private area or a public area. You can open the file later to modify it or to deploy it to the device.

To save a configuration file:

Step 1
Select Configuration > Tools > Config Editor > Private Configs to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select Configuration > Tools > Config Editor > Public Configs to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2
Select the configuration file and click Edit.

The Editor window appears.

Step 3
Click Save.

The Save Config dialog box appears, only if you are saving the configuration file for the first time. The subsequent saving of a file is done directly to its previously saved location.

Step 4
Enter the information required to save a configuration file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Saves the files in the public area.</td>
<td>None.</td>
</tr>
<tr>
<td>Private</td>
<td>Saves the files in the private area.</td>
<td>When a configuration from a list of private configs is opened and saved in the public area (user archive) with the same name as the private configuration, the private configuration with that name gets deleted. However, the reverse is not true. That is when a config is opened from the public area (user archive) and saved in the private area, the public configuration is not deleted.</td>
</tr>
<tr>
<td>Branch Name</td>
<td>Name of branch.</td>
<td>Private area to where configuration files are stored locally.</td>
</tr>
</tbody>
</table>

Step 5
Click either:
- Submit to save the configuration file.
  Or
- Cancel to return to the previous setting.

After the configuration file opened from the Device Archive is saved to the private or public archive, all the subsequent operations (compare, show changes) behave as if the configuration is opened from a private or public location.
## Undoing All

You can use this feature to undo editing or typing changes. To do this:

### Step 1
Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

### Step 2
Select the configuration file and click **Edit**.

The Editor window appears.

### Step 3
Edit the configuration file.

### Step 4
Click **Undo All**.

A message window appears with the message:

Do you want to discard all the changes?

### Step 5
Click either:

- **OK** to return to the last saved configuration file.
  
  Or
  
  - **Cancel** to avoid making any changes.

---

## Replacing All

You can use this feature to search for and replace text in the file. To do this:

### Step 1
Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.
Printing a Configuration File

You can use this feature to print the configuration file. To do this:

Step 1  Select Configuration > Tools > Config Editor > Private Configs to open a configuration file stored in a private work area.
The List of Private Configs window appears.
Or
Select Configuration > Tools > Config Editor > Public Configs to open a configuration file stored in a public work area.
The Public Configs window appears.
You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2  Select the configuration file and click Edit.
The Editor window appears.

Step 3  Select the Print icon at the top right corner.
A new browser window appears. The details are in PDF format. You can print the information, using the Print option provided by the browser.
Exporting Changes of a Configuration File

You can use this feature to export the modified configuration file to either cfg or XML formats based on the edit operation. To do this:

Step 1 Select Configuration > Tools > Config Editor > Private Configs to open a configuration file stored in a private work area.
The List of Private Configs window appears.
Or
Select Configuration > Tools > Config Editor > Public Configs to open a configuration file stored in a public work area.
The Public Configs window appears.
You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click Edit.
The Editor window appears.

Step 3 Select the Export icon at the top right corner.
A new browser window appears to select the directory to which the modified Configfile is exported either in cfg or XML formats.

• If you are using the Raw mode then the exported file format is cfg. The file name convention is DeviceName-VersionNumber-raw.cfg.
• If you are using the Processed mode then the exported file format is XML. The file name convention is DeviceName-VersionNumber-proc.xml.

Where DeviceName is the device name as entered in Device and Credential Repository and VersionNumber is the device configuration version.
The default directory where the modified Configuration file is exported is:
On Solaris and Soft Appliance server,
/var/adm/CSCOpx/files/rme/cfgedit/configexport
On Windows server,
NMSROOT\files\rme\cfgedit\configexport
Deploying a Configuration File

You can use this feature to deploy a configuration file to a device.

To deploy a configuration file:

**Step 1** Select Configuration > Tools > Config Editor > Private Configs to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select Configuration > Tools > Config Editor > Public Configs to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, **Overview: Opening a Configuration File**.

**Step 2** Select the configuration file and click **Deploy**.

The Job Option Details dialog box appears.

**Step 3** Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job Information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>E-mail</strong></td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.</td>
</tr>
<tr>
<td><strong>Job Options</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Job Password** | • If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) enter the device login user name and password and device Enable password.

• If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) either:

  – Enter the device login user name and password and device Enable password or

  – Disable the Job Password option in the Job Schedule and Options dialog box. |
Deploying a Configuration File

Chapter 8  Editing and Deploying Configurations Using Config Editor

### Step 4
Click **Submit**.

An immediate Deploy of Configuration on Device job will be scheduled.

A message appears, **Job ID** is created successfully.

Where **ID** is a unique Job number.

**Step 5**
Click **OK**.

You can check the status of your scheduled **Config Editor Deploy** job by selecting **Configuration > Job Browsers > Config Editor**.

- Configurations edited from Raw mode (.RAW) can be downloaded to both Startup or Running configuration of the device.
- Configurations edited from Processed mode (.PROC) can only be downloaded to the Running configuration of the device.

### Deploy Mode

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overwrite</strong></td>
<td>Select the Overwrite option, if you want to replace the existing running configuration on the device, with the selected configuration. This is the default option for the configuration deployment. The configuration that you have selected is compared with the latest running configuration in the Configuration Archive. (LMS assumes that the latest running configuration in the archive is the same as the configuration currently running on the device.) The Overwrite mode ensures that the running configuration on the device is overwritten with the selected configuration. This means, after the configuration is successfully deployed, the selected configuration and the running configuration on the device are the same. Overwrite mode supports Write2Run of the configuration only.</td>
</tr>
<tr>
<td><strong>Merge</strong></td>
<td>Select the Merge option, if you want to add incremental configuration to the device. The configuration that you have selected is deployed on to the device as is. This means, the existing running configuration of the device is updated incrementally with the commands in the selected configuration. The selected running configuration is not compared with the running configuration in the Configuration Archive. We recommend that you use this option on newly deployed devices. This is because, the Merge option effectively deploys the entire configuration from the archive, on to the device. Merge mode supports both Write2Run and Write2Start of the configuration.</td>
</tr>
</tbody>
</table>
Closing a Configuration File

You can use this feature to close the configuration file without exiting the application. If the file contains unsaved changes, you are prompted to save before closing.

To close the configuration file:

Step 1
Select Configuration > Tools > Config Editor > Private Configs to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select Configuration > Tools > Config Editor > Public Configs to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2
Select the configuration file and click Edit.

The Editor window appears.

Step 3
Click Close.

If the file contains any unsaved changes, a message window appears with the message:

You have done some changes since last save. Do you want to the save the changes?

Step 4
Click either:

- **OK** to save the configuration file in a private area.
  
  Your changes are saved.

  Or

- **Cancel** to ignore your changes.

Selecting Configuration Tools

You can use this feature to choose a configuration tool from the list of configuration tools. The list of configuration tools available are as follows:

- Comparing Versions of Configuration Files
- Displaying Your Changes
- Overview: Syntax Checker
To select a configuration tool:

Step 1  Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location.

For more details see, **Overview: Opening a Configuration File**.

Step 2  Select the configuration file and click **Edit**.

The Editor window appears.

Step 3  Click **Tools**.

The Select Tool dialog box appears with the following tools:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compare Config</td>
<td>Compares the current file with any earlier version in the configuration archive.</td>
</tr>
<tr>
<td>View Changes</td>
<td>Displays the changes made in the opened file.</td>
</tr>
</tbody>
</table>
| External Syntax Checker | 1. Select this option to check the configuration file using an external syntax checker that is registered with Cisco Management Integration Center (CMIC).  
2. Click **Submit**.  
Config Editor launches the URL, displaying the configuration commands and sysobject ID of the device as input to the external syntax checker.  
3. View the output displayed by the external syntax checker.  
4. Modify the commands in Config Editor. |

Step 4  Select a tool.

Step 5  Click either:  
• **Submit** to launch the tool.  
Or  
• **Cancel** to close the window.
Comparing Versions of Configuration Files

You can use this feature to compare the current file with any earlier version in the configuration archive. The Compare option is enabled only if a file is open.

To compare versions of configuration files:

**Step 1** Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.
The List of Private Configs window appears.
Or
Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.
The Public Configs window appears.
You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location.
For more details see, [Overview: Opening a Configuration File](#).

**Step 2** Select the configuration file and click **Edit**.
The Editor window appears.

**Step 3** Click **Tools**.
The Select Tool dialog box appears.

**Step 4** Select **Compare Config**.

**Step 5** Click either:
- **Submit** to view the Version Selector dialog box and proceed to the next step.
  Or
- **Cancel** to close the window without making any changes.

**Step 6** Select a version with which you want to compare the current open file, from the list of other versions.
The Configuration Compare Report appears.

**Step 7** Select the View mode.

**Step 8** Click **Processed** to display files in Processed mode. This is the default option.
Files appear at the configlet level (a set of related configuration commands).

**Step 9** Click **Raw** to display the files in Raw mode.
The entire file appears.
If you want to print the report, click **Print**.
You can select Diff only option to view the differences, or All to view the entire configurations and compare the differences.
Displaying Your Changes

You can use this feature to display the changes made in the opened file. The text file in archive is compared with the opened version.

The View Changes option is enabled only if a file is open.

To display the changes in the open file:

Step 1
Select Configuration > Tools > Config Editor > Private Configs to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select Configuration > Tools > Config Editor > Public Configs to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2
Select the configuration file and click Edit.

The Editor window appears.

Step 3
Click Tools.

The Select Tool dialog box appears.

Step 4
Select View Changes option.

Step 5
Click either:

- Submit to view the differences in a new window.

Or

- Cancel to close the window without making any changes.

Overview: Syntax Checker

Config Editor provides ways to check the syntax of config commands using syntax checker. Config Editor checks syntax using the Interface to External Syntax Checker.

Interface to External Syntax Checker

The external syntax checker has to be registered with Cisco Management Integration Center (CMIC) using Link Registration.

For details see, Registering an External Syntax Checker Application With CMIC. Config Editor queries CMIC to check if the application is registered with the name “Config Syntax Checker”.
Overview: Syntax Checker

If the application is registered, Config Editor knows the External Syntax Checker URL to be launched and parameters to be passed to the syntax checker.

Config Editor launches the URL with two parameters, deviceSysObjID and cfgCmds:

- **deviceSysObjID**—sysObjectID of the device. External Syntax Checker uses deviceSysObjID to identify the device type.
- **cfgCmds**—List of commands for which the syntax has been checked.

ConfigEditor launches the External Syntax Checker URL in POST method. When the URL is launched you can view the configuration commands for which the syntax has been checked.

To validate the results and correct the commands in Config Editor:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select <strong>Configuration &gt; Tools &gt; Config Editor &gt; Config Editor</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select <strong>Device and Version</strong> in the Selection Area page.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Go</strong>.</td>
</tr>
<tr>
<td></td>
<td>The Device and Version dialog box appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select the required device using Device Selector.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select the information required to open a configuration file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
<td></td>
</tr>
<tr>
<td>Latest</td>
<td>Select the latest version of the configuration file.</td>
</tr>
<tr>
<td>Earlier</td>
<td>Select an earlier version of the configuration file.</td>
</tr>
<tr>
<td><strong>Version Number</strong></td>
<td>Version number of the configuration file. This option is enabled when you select <strong>Earlier</strong> in the version field. This field is not editable.</td>
</tr>
<tr>
<td></td>
<td>To enter the version number:</td>
</tr>
<tr>
<td></td>
<td>1. Click <strong>Select</strong> to open the Version Tree dialog box.</td>
</tr>
<tr>
<td></td>
<td>2. Select the desired version.</td>
</tr>
<tr>
<td></td>
<td>3. Either:</td>
</tr>
<tr>
<td></td>
<td>– Click <strong>OK</strong> to select the version</td>
</tr>
<tr>
<td></td>
<td>– Click <strong>Cancel</strong> to close the window.</td>
</tr>
</tbody>
</table>

| Step 6 | Click **Edit** to edit a configuration file |
| | The Configuration Editor dialog box appears. |
| Step 7 | Click **Tools**. |
| | The Select Tool dialog box appears with the tools. |
Step 8 Select **External Syntax Checker**.

Step 9 Click **Submit** to launch the tool.

Config Editor launches the External Syntax Checker URL.

---

**Registering an External Syntax Checker Application With CMIC**

To register an external syntax checker application with CMIC (Cisco Management Integration Center):

**Step 1** Select **Link Registration**.

The Registered Links window appears.

**Step 2** Click **Registration** in the Links Registrations Status page.

The Enter Link Attributes window appears.

**Step 3** Enter the inputs for the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>User Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter Config Syntax Checker.</td>
</tr>
<tr>
<td>URL</td>
<td>Enter the External Syntax Checker URL.</td>
</tr>
<tr>
<td>Display Location</td>
<td>Select Third Party.</td>
</tr>
</tbody>
</table>

The Registered Links window appears with the list of registered links.

---

**Viewing the List of Modified Configs**

You can use this feature to display a list of configuration files modified by any user in a private work area (select **Private Configs**) or a public work area (select **Public Configs**).

To list out all the modified files:

**Step 1** Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location.

For more details see, **Overview: Opening a Configuration File**.
Step 2  Do any of the following:

- Select the file and click **Edit** to edit an opened configuration file.
  The Configuration Editor dialog box appears.
- Select the file and click **Deploy** to deploy a job.
  The Select Configs dialog box appears.
- Select the file and click **Delete** to remove an opened configuration file.
  The screen is refreshed and the file is removed.

You can open a raw config in processed format. However, you cannot open a processed config in raw format.

---

**Overview: Opening a Configuration File**

You can use this feature to open a configuration file for editing.

You can open a configuration file by:

- **Device and Version**—Opens a configuration file from the archive.
- **Pattern Search**—Opens a configuration file by searching for a pattern.
- **Baseline**—Opens a configuration file using a baseline template stored in the device configuration management repository.
- **External Location**—Opens a configuration file stored in an external location

If another user has opened the configuration file, config editor opens another copy of the file.

To open a configuration file:

---

**Step 1**  Select **Configuration > Tools > Config Editor > Config Editor**.

**Step 2**  Select an option in the Selection Area page.

**Step 3**  Click **Go**.

The Option dialog box opens in a new window.

---

**Opening a Configuration File - By Device and Version**

You can use this feature to open a configuration file from the archive. The file opens in read-write mode depending on your edit permissions.

The file appears in either the Raw or Processed mode, based on your preferences.

To open a configuration file from the archive:

---

**Step 1**  Select **Configuration > Tools > Config Editor > Config Editor**.

**Step 2**  Select **Device and Version** in the Selection Area page.
Step 3  Click **Go**.
The Device and Version dialog box appears.

Step 4  Select the required device using the Device Selector.

Step 5  Select the information required to open a configuration file.

### Field | Description
--- | ---
**Version** |  
Latest | Select the latest version of the configuration file.
Other | Select an earlier version of the configuration file.
**Version Number** |  
Version number of the configuration file. This option is enabled when you select **Other** in the version field.
This field is not editable.
To enter the version number:
1. Click **Select** to open the Version Tree dialog box.
2. Select the version you need.
3. Either:
   - Click **OK** to select the version
   - Click **Cancel** to close the window.

**Format** |  
Raw | Displays the entire configuration file. After you open a file in a specific mode, you can view it only in that mode.
Processed | Displays only the commands.

Step 6  Click either:
- **Edit** to edit a configuration file
  The configuration editor dialog box appears.

Or
- **Reset** to clear all fields and get to the default setting.

---

### Opening a Configuration File - By Pattern Search

You can use this feature to open a configuration file by
- Selecting a label set in Config Archive
- Selecting a custom query of default patterns
- Searching for a pattern.
A pattern can be any text string. The file is displayed in either the Raw or Processed mode, based on your preferences.

To open a configuration file:

Step 1  
Select Configuration > Tools > Config Editor > Config Editor.

Step 2  
Select Pattern Search in the Selection Area page.

Step 3  
Click Go.

The Pattern Search dialog box appears.

Step 4  
Do any of the following:

- Open a configuration file by selecting a label set in Config Archive. See Configuring Labels for more information.
- Open a configuration file by selecting a custom query of default pattern
- Open a configuration file by searching for a pattern

Open a configuration file by selecting a label set in Config Archive. See Configuring Labels for more information.

a. Select Label to enable the Select a Config Label drop-down list box
b. Select the required label from the Select a Config Label drop-down list box

If you select a label and some devices from the Device Selector, and click Search, the search results will only be for the devices that are part of the selected label.

Open a configuration file by selecting a custom query of default pattern

Select the required Custom Query from the Select Custom Query drop-down list box. To create a custom query, select Configuration > Configuration Archive > Views > Custom Queries.

Open a configuration file by searching for a pattern

a. Enter a pattern in the editable Pattern Column. For example, http server.

   To search for more than one pattern, enter the second and third patterns in the Pattern 2 and Pattern 3 fields and so on. You cannot search for special characters. For example, control-C.

b. Click the corresponding Contains/Does not contain row to view the selection drop-down list box.

c. Select Include if you wish to search for configurations that match the patterns you entered and select Exclude if you wish to search for configurations that do not match the patterns you entered. Select the required devices using the Device Selector.

Step 5  
Select the required options:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting</td>
<td></td>
</tr>
<tr>
<td>Match Any</td>
<td>Searches for configurations that have at least one of the patterns you entered.</td>
</tr>
<tr>
<td>Match All</td>
<td>Searches for configurations that include all patterns you entered.</td>
</tr>
<tr>
<td>Match Case</td>
<td>Searches for configurations that are identical to the pattern entered.</td>
</tr>
<tr>
<td>Search Versions</td>
<td></td>
</tr>
<tr>
<td>Latest</td>
<td>Searches in the latest version of the configuration file</td>
</tr>
<tr>
<td>All</td>
<td>Searches in all the versions of the configuration file</td>
</tr>
</tbody>
</table>
Step 6  Click Search.

The Search Archive Result window appears in the Pattern Search Results page with the search results. The columns in this window are:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the configuration file</td>
</tr>
<tr>
<td>Created On</td>
<td>Date on which the configuration file was created</td>
</tr>
<tr>
<td>Change Description</td>
<td>Modification comments</td>
</tr>
</tbody>
</table>

Step 7  Select any of the following:

- **Edit** to open the selected configuration file in a pop up window for editing. The search result page will be retained. You can select another configuration from the search result page and open that file too for editing.
- **Back** to return to the Pattern Search page.
- **Finish** to complete the search.
- **Cancel** to return to the Selection Criteria page.

---

### Opening a Configuration File - By Baseline

You can use this feature to open a baseline configuration template maintained in the configuration archive. You can create a baseline configuration from the baseline template by replacing all the variables that appear in the configuration.

Config Editor does not check whether you have changed the template variables.

**Note**  The baseline template will be opened only in Raw format.

To open a baseline configuration template:

**Step 1**  Select Configuration > Tools > Config Editor > Config Editor.

**Step 2**  Select Baseline in the Selection Area page.

**Step 3**  Click Go.

The Baseline Config dialog box appears.

**Step 4**  Select the required devices using the Device Selector.

**Step 5**  Click Next

The Baseline Template window appears with the following details:
Baseline Configuration Editor

You can use this feature to edit the Baseline template of the configuration file. To do this:

**Step 1** Select **Configuration > Tools > Config Editor > Config Editor**.

**Step 2** Select **Baseline** in the Selection Area page.

**Step 3** Click **Go**.

The Baseline Config dialog box appears.

**Step 4** Select the required devices using the Device Selector.

**Step 5** Click **Next**.

The Baseline Template window appears with the following details:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline Name</td>
<td>Name of the Baseline template.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description about the template.</td>
</tr>
<tr>
<td>Created On</td>
<td>Date on which the template was created.</td>
</tr>
</tbody>
</table>

**Step 6** Select a Baseline template based on the device type.

**Step 7** Click **Finish**.

The Baseline Configuration Editor dialog box appears.

**Step 8** Edit the text area. (The upper section contains only non-credential commands and is called the text area.)

While editing a baseline template, you are required to replace variables that appear in the template with actual values.

For example, in the following line `[msg]` is the variable.

```
banner motd [msg]
```

You should replace `[msg]` with actual value.
Opening an External Configuration File

You can use this feature to associate a device with the selected configuration file from an external location (other than archive) in the server. The file appears in either a Raw or Processed mode, based on your preferences.

For example, if you associate the selected configuration to an IOS device in the Processed mode, then the given configuration is processed based on the IOS rules defined in LMS.

The file in the archive can be opened with a specified format from the temp directory on the local server, from another file system mapped drive or any mount. The file opened is validated for format with DCMA.

To open a configuration file from an external location:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select Configuration &gt; Tools &gt; Config Editor &gt; Config Editor.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select External Location in the Selection Area page.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Go.</td>
</tr>
<tr>
<td></td>
<td>The External File Selection dialog box appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Browse to select the external file location.</td>
</tr>
<tr>
<td></td>
<td>The External Config Selector dialog box appears with the following fields:</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>File</td>
<td>Location of the file</td>
</tr>
<tr>
<td>Directory content</td>
<td>Name of the directory</td>
</tr>
<tr>
<td>Drive</td>
<td>Name of the drive</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click either:</td>
</tr>
<tr>
<td></td>
<td>• OK to enter the external location.</td>
</tr>
<tr>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>• Cancel to return to the External File Selection page.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Select the required devices using the Device Selector.</td>
</tr>
</tbody>
</table>
Step 7  Either:

• Click **Edit** to edit a configuration file

  The configuration editor dialog box appears.

  Or

• Click **Reset** to clear all fields and get to the default setting.

You can control the access to directories/folders present on the server. There is a property file for this purpose located at:

- \( \text{NMSROOT} \)/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/config/cfgedit/ConfigEditor.properties (On Solaris and Soft Appliance)
- \( \text{NMSROOT} \)/MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\config\cfgedit\ConfigEditor.properties (On Windows)

\( \text{NMSROOT} \) is the LMS install directory.

This file has two variables:

• **DIR_LIST**—You can mention all the directories or files separated by pipe symbol (|).

• **ALLOW**—You can set as true or false. If you set the value as true, you can access only those directories or files given as values for the variable **DIR_LIST**. If you set the value as false, you cannot access those directories or files given as values for the variable **DIR_LIST**.

The default values for the variables are:

• **DIR_LIST**—etc/passwd

• **ALLOW**—false

## Configuration Deployment in Overwrite and Merge Modes

### Overwrite Mode

Config Editor assumes that the latest archived version is the same as the running configuration on the device.

Before Config Editor downloads the archived configuration on the device, it compares the archived version (which you have modified) with the latest version. The application then overwrites the running configuration on the device with the archived version. This means, after the configuration is successfully deployed, the selected configuration and the running configuration on the device are the same.

For example, assume that the archived version contains commands a, b, c, and d; and that the latest running version contains commands a, b, e, f, and g. After the archived configuration has been restored, the running configuration on the device, will contain commands a, b, c, and d.

Ensure that all the required commands are in the archived version. You can review the work order and make necessary changes by editing the archived version, if required.

This is the default mode for the configuration deployment.
Overview: Downloading a Configuration File

To download a configuration file to the device and to the archive, you must:

- Create a download job.
- Select the configuration file on which the job will run.
- Configure the job properties.
- Set the job approvers.
- Review the job work order.

When a job starts to download, the users on the job approver list are notified by e-mail. At least one approver must approve the job before it can run. Make sure that an approver list with the approvers you want exists.

If there is no approver list but you have the correct access privileges, you must modify or create approver lists, using the Job Approval option. Otherwise, contact your system administrator. See Administration of Cisco Prime LAN Management Solution 4.2 for more information.

Starting a New Download Job

You can use the Create Config Download Job wizard to define and schedule a download job.

Step 1
Select Configuration > Job Browsers > Config Editor.
The Config Deploy Job Browser window appears.

Step 2
Click Create.
The Create Config Download Job wizard appears.
All dialog boxes of the wizard contain the following buttons:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back</td>
<td>Returns to the previous page.</td>
</tr>
<tr>
<td>Next</td>
<td>Returns to the next page.</td>
</tr>
<tr>
<td>Finish</td>
<td>Completes creation of jobs.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels creation of job.</td>
</tr>
</tbody>
</table>
Selecting Configs

You can use the Select Configs dialog box to select configuration files of devices on which the download job will run.

You must start a new download job before you start selecting configuration files. To do this:

---

### Step 1
Select a configuration file on which to run the job using device selector on the left pane.

The select configuration file dialog has two panes.

- **Left Pane**—The Device Selector appears.
- **Right Pane**—The list of selected configuration files appear.

### Step 2
Click either:

- **Add Latest** to move the latest version of the selected configuration file to the Selected Configuration Files pane
  
  Or

- **Add Other Version** to move any version of the selected configuration file to the Selected Configuration Files pane

### Step 3
Do any of the following:

- Click **Next** to proceed to the Job Schedule and Options dialog box.
- Click **Cancel** to stop creating a download job.
- Select a configuration file from the Selected Configuration Files pane and click **Delete** to remove a configuration file.
## Scheduling a Job

This feature allows you to assign a job name, schedule the job and set job options.

Before scheduling a job you must:
1. Start a new download job.
2. Select Configs.

To schedule a job:

---

### Step 1
Enter the following information in the Job Schedule and Options dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description/Action</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>Schedules the job to run immediately or in the future. Select either <strong>Once</strong> or <strong>Immediately</strong>.</td>
<td>You can specify when you want to run the job. To define this, select an option from the drop down menu:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Once</strong>—Job will run once in the future. You can specify the Starting Date and Time for the job to be run</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Immediately</strong>—Job will run immediately. This option is not available if Job Approval is enabled.</td>
</tr>
<tr>
<td>Date</td>
<td>Date on which you want to run the job.</td>
<td>Select date for the job to run. If Run Type is Immediate, the system date is automatically selected.</td>
</tr>
<tr>
<td>At</td>
<td>Time when you want to run the job in the future.</td>
<td>Select time for the job to run. If Run Type is Immediate, the system time is automatically selected.</td>
</tr>
<tr>
<td><strong>Job Info</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter job description.</td>
<td>Make each description unique so you can easily identify jobs.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Allows you to enter the e-mail addresses to which the job will send status notices. Separate multiple addresses with commas.</td>
<td>E-mail notification is sent when job is created, started, deleted, canceled, and completed.</td>
</tr>
<tr>
<td>Comments</td>
<td>Allows you to enter comments.</td>
<td></td>
</tr>
<tr>
<td>Approval Comment</td>
<td>Allows you to enter approval comments.</td>
<td>This field is not active if approval comments were not set using administration approval. Select Configuration &gt; Config Jobs &gt; Job Approval to set approval comments. For more information, see <em>Administration of Cisco Prime LAN Management Solution 4.2</em>.</td>
</tr>
</tbody>
</table>
## Field: Maker E-mail
- **Description/Action:** Mail ID of the person who created the job.
- **Usage Notes:** This field is not active if approvers were not set using administration approval. Select Configuration > Config Jobs > Job Approval to set approval comments. For more information, see *Administration of Cisco Prime LAN Management Solution 4.2*.

### Job Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description/Action</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail on mismatch of Configuration Version</td>
<td>Select this option, if you want to cause the job to be considered Failed, if there is a version mismatch.</td>
<td>A job is considered Failed when the most recent configuration version in the configuration archive is not identical to the configuration that was running when you created the job.</td>
</tr>
<tr>
<td>Sync archive before running a job</td>
<td>Select this option if you want to archive the running configuration before making configuration changes.</td>
<td>Synchronize archive before running a job policy gets selected when Fail on mismatch of Configuration Version policy is selected.</td>
</tr>
<tr>
<td>Delete Config after Download</td>
<td>Select this option if you want to delete the configuration file after download.</td>
<td>Applicable only to private configuration files.</td>
</tr>
<tr>
<td>Copy running to Startup</td>
<td>Select this option if you want to copy the running configuration to the startup configuration on each device after configuration changes are made successfully.</td>
<td>This does not apply to Catalyst OS devices.</td>
</tr>
<tr>
<td>Enable Job Password</td>
<td>Select this option to enable username and password.</td>
<td></td>
</tr>
<tr>
<td>Login User Name</td>
<td>Enter the username configured on the device.</td>
<td>This field is editable only when you select the Enable Job Password option. LMS ignores the username in the database and uses the newly entered username instead.</td>
</tr>
<tr>
<td>Login Password</td>
<td>Enter the password for the device.</td>
<td>This field is editable only when you select the Enable Job Password option. LMS ignores the password in the database and uses the newly entered password instead.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the enable password configured on the device.</td>
<td>This field is editable only when you select the Enable Job Password option. LMS ignores the password in the database and uses the newly entered password instead.</td>
</tr>
</tbody>
</table>
## Scheduling a Job

### Failure Policy
Specify what the job should do if it fails to run on the device.

- Select **Ignore Failure and Continue** from the drop-down list box to continue the job and make configuration changes to the remaining devices, configured by the job.
- Select **Stop on Failure** to stop making changes to the remaining devices.

### Execution
Mode in which the job is executed. There are two options, Parallel and Sequential.

1. Select **Parallel** to run the job on multiple devices at same time
   
   Or
   
   Select **Sequential** to run the job one device at a time.

2. Click **Device Order**.
   
   The Set Device Order dialog box appears.

3. Use the Up and Down arrows to move a device up or down.

4. Click **Done**.

### Deploy Mode
Mode in which the configuration file is downloaded. The two modes are Overwrite and Merge.

Do either of the following:

- Select the **Overwrite** option, if you want to replace the existing running configuration on the device, with the selected configuration.

  This is the default option for the configuration deployment.

  The configuration that you have selected is compared with the latest running configuration in the Configuration Archive. (LMS assumes that the latest running configuration in the archive is the same as the configuration currently running on the device.)

  The Overwrite mode ensures that the running configuration on the device is overwritten with the selected configuration. This means, after the configuration is successfully deployed, the selected configuration and the running configuration on the device are the same.

  Overwrite mode supports only Write2Run of the configuration.

  Or

  - Select the **Merge** option, if you want to add incremental configuration to the device.

    The configuration that you have selected is deployed on to the device as is. This means, the existing running configuration of the device is updated incrementally with the commands in the selected configuration.

    The selected running configuration is not compared with the running configuration in the Configuration Archive.

    We recommend that you use this option on newly deployed devices. This is because, the Merge option effectively deploys the entire configuration from the archive, on to the device.

    Merge mode supports both Write2Run and Write2Start of the configuration.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description/Action</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Policy</td>
<td>Specify what the job should do if it fails to run on the device.</td>
<td>- Select <strong>Ignore Failure and Continue</strong> from the drop-down list box to continue the job and make configuration changes to the remaining devices, configured by the job. Or - Select <strong>Stop on Failure</strong> to stop making changes to the remaining devices.</td>
</tr>
<tr>
<td>Execution</td>
<td>Mode in which the job is executed. There are two options, Parallel and Sequential.</td>
<td>1. Select <strong>Parallel</strong> to run the job on multiple devices at same time Or - Select <strong>Sequential</strong> to run the job one device at a time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click <strong>Device Order</strong>. The Set Device Order dialog box appears.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Use the Up and Down arrows to move a device up or down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>Done</strong>.</td>
</tr>
</tbody>
</table>
| Deploy Mode | Mode in which the configuration file is downloaded. The two modes are Overwrite and Merge. | Do either of the following:  
- Select the **Overwrite** option, if you want to replace the existing running configuration on the device, with the selected configuration.  
  This is the default option for the configuration deployment.  
  The configuration that you have selected is compared with the latest running configuration in the Configuration Archive. (LMS assumes that the latest running configuration in the archive is the same as the configuration currently running on the device.)  
  The Overwrite mode ensures that the running configuration on the device is overwritten with the selected configuration. This means, after the configuration is successfully deployed, the selected configuration and the running configuration on the device are the same.  
  Overwrite mode supports only Write2Run of the configuration.  
  Or  
- Select the **Merge** option, if you want to add incremental configuration to the device.  
  The configuration that you have selected is deployed on to the device as is. This means, the existing running configuration of the device is updated incrementally with the commands in the selected configuration.  
  The selected running configuration is not compared with the running configuration in the Configuration Archive.  
  We recommend that you use this option on newly deployed devices. This is because, the Merge option effectively deploys the entire configuration from the archive, on to the device.  
  Merge mode supports both Write2Run and Write2Start of the configuration. |
## Reviewing the Work Order

The work order summarizes the job you created. If you find any changes missing when you review the work order you can go back and change the options.

Complete the following prerequisite steps of the job definition process:

1. Start a new download job
2. Select configs
3. Configure job properties
4. Set job approvers, if Job Approval is enabled

### Step 2

Select any of the following:

- **Back** to return to the Select Configs dialog box.
- **Next** to proceed to the Job Summary dialog box.
- **Cancel** to stop creating a Download job.

### Write To

<table>
<thead>
<tr>
<th>Field</th>
<th>Description/Action</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write To</td>
<td>The method in which the Configuration is pushed. The two methods are Running and Startup</td>
<td>Do either of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Select the Running option, if you want to replace the existing running configuration on the device, with the selected configuration file. This is also referred to as Write2Run. Or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Select the Startup option, if you want to erase the contents of the device's startup configuration and write the contents of the given file as the device's new startup configuration. This is also referred to as Write2Start.</td>
</tr>
</tbody>
</table>

Configurations edited from Raw mode (.RAW) can be downloaded to both Startup or Running configuration of the device.

Configurations edited from Processed mode (.PROC) can only be downloaded to the Running configuration of the device.

### Update credentials after deploy

<table>
<thead>
<tr>
<th>Field</th>
<th>Description/Action</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update credentials after deploy</td>
<td>Update the credentials in DCR after deployment, if the deployed commands include any credentials commands.</td>
<td>Choose this option if you want to update the DCR with the deployed credentials commands such as SNMP community strings, Telnet username/password etc. Write2Start does not support changing the credentials after deployment.</td>
</tr>
</tbody>
</table>
To review the work order:

**Step 1** Review the information in the Work Order dialog box. The fields in this dialog box are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Info</td>
<td>Detailed information about the job, such as owner, description and schedule.</td>
</tr>
<tr>
<td>Job Approval Info</td>
<td>Status of approval.</td>
</tr>
<tr>
<td>Devices</td>
<td>Devices on which the job will run. Edit in Device Selector dialog box.</td>
</tr>
<tr>
<td>Device Commands</td>
<td>Commands that the job will run.</td>
</tr>
<tr>
<td>Username</td>
<td>Username of the job owner.</td>
</tr>
</tbody>
</table>

- To modify the job, return to any previous dialog box and change the information.
- To return to a previous dialog box, click **Back** until the dialog box appears.

**Step 2** Click **Finish** in the Work Order dialog box to register the job.

---

**Viewing the Status of all Deployed Jobs**

You can use this feature to view the status of all pending, running, and completed jobs. You can create a new job or edit, copy, stop and delete a job that you have opened.

You can only Edit one job at a time while you can Stop or Delete multiple jobs at a time.
To view all the downloaded jobs:

**Step 1** Select **Configuration > Job Browsers > Config Editor**.

The List of Deploy Jobs window appears with the list of all the jobs.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique number assigned to job at creation. Never reused.</td>
</tr>
<tr>
<td>Run Status</td>
<td>Job states:</td>
</tr>
<tr>
<td></td>
<td>• Canceled</td>
</tr>
<tr>
<td></td>
<td>• Suspended</td>
</tr>
<tr>
<td></td>
<td>• Missed start</td>
</tr>
<tr>
<td></td>
<td>• Rejected</td>
</tr>
<tr>
<td></td>
<td>• Succeeded</td>
</tr>
<tr>
<td></td>
<td>• Succeeded with info</td>
</tr>
<tr>
<td></td>
<td>• Failed, Crashed</td>
</tr>
<tr>
<td></td>
<td>• Failed at start</td>
</tr>
<tr>
<td></td>
<td>• Running.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the job, as entered during job definition.</td>
</tr>
<tr>
<td>Owner</td>
<td>Name of the user who owns the configuration file.</td>
</tr>
<tr>
<td>Scheduled On</td>
<td>Date and time the job is scheduled to run.</td>
</tr>
<tr>
<td>Completed At</td>
<td>Date and time at which the job is completed.</td>
</tr>
<tr>
<td>Schedule Type</td>
<td>Job schedule types:</td>
</tr>
<tr>
<td></td>
<td>• Suspended</td>
</tr>
<tr>
<td></td>
<td>• Scheduled</td>
</tr>
<tr>
<td></td>
<td>• Waiting for approval</td>
</tr>
<tr>
<td></td>
<td>• Rejected</td>
</tr>
<tr>
<td></td>
<td>• Canceled.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of running or completed jobs: Job Started, Progress, Job Cancelled,</td>
</tr>
<tr>
<td></td>
<td>Job Failed, Job Successful.</td>
</tr>
<tr>
<td></td>
<td>Pending jobs have no status.</td>
</tr>
</tbody>
</table>
**Step 2**  Click one of the following buttons:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>
| Create | Creates a new job.                               | 1. Click **Create**.  
The Create Config Deploy Job wizard appears.  
2. Use the wizard to define and schedule a download job. |
| Edit   | Edits pending job.                               | Click **Edit** to edit only jobs you own.  
If the job start time occurs during editing, it will run without the edits.  
In such a case, you can complete your edits, reschedule the job, and re-edit it.  
To prevent job from running unedited:  
1. Complete edits before job start time.  
2. Cancel job and create new one. |
| Copy   | Copies job.                                      | Click **Copy**.  
The Job definition opens with the current information and the new ID except job schedule details filled in. |
| Stop   | Stops a running job.                             | 1. Click **Stop**.  
You are prompted to confirm stopping a job.  
2. Click **OK**.  
You can stop only the jobs that you own. Admin level users can stop all jobs. |
| Delete | Removes the job from the Job Scheduler.          | 1. Click **Delete**.  
You are prompted to confirm stopping a job.  
2. Click **OK** or **Cancel**.  
You can remove only the jobs that you own. Admin level users can remove all jobs. |
Managing Software Images Using Software Management

Manually upgrading your devices to the latest software version can be an error-prone, and time-consuming process. To ensure rapid, reliable software upgrades, Software Management automates the steps associated with upgrade planning, scheduling, downloading, and monitoring.

This chapter contains:

• Setting Up Your Environment
• Software Repository
• Software Distribution
• Using Software Management Job Browser
• Understanding User-supplied Scripts
• Locating Software Management Files

Using Software Management, you can:

• Set up your Software Management preferences.
  
  You can specify information such as the directory where images are stored, and the pathname of the user-supplied script to run before and after each device software upgrade.

  You can enable and define the protocol order for Software Management tasks. You can also enable the Job Based Password option for Software Management tasks.

  You can specify if the images on Cisco.com should be included during image recommendation of the device. Also specify the Cisco.com filters so that only the images that match the filter criteria are selected.

• Analyze software upgrades

  You can generate Upgrade Analysis reports that help you determine prerequisites for a new software deployment.

  These reports analyze the proposed images to determine the hardware upgrades (device access, boot ROM, Flash memory, RAM, and NVRAM and boot Flash, if applicable) required before you can perform the software upgrade.

  See Upgrade Analysis for further details.
• Perform In Service Software Upgrade (ISSU)
  LMS supports the In Service Software Upgrade (ISSU) process that allows Cisco IOS software images to be updated without rebooting the device. This process increases network availability and reduces downtime caused by planned software upgrades.
  See Support for In Service Software Upgrade for further details.

• Import images into the software repository
  You can determine the images missing from your repository and import them into the software repository.
  You can also keep the repository up-to-date and periodically synchronize the repository with the images running on your network devices.
  You can also schedule an image import for a later, more convenient time.
  See Adding Images to the Software Repository for further details.

• Distribute software images to groups of devices
  Depending on system complexity, you can configure upgrades for groups of devices to the same software image or to different software images.
  You can specify these groups manually, using your groups and search criteria. You can also use some other selection criterion, such as the current software version or hardware type to specify the groups.
  You can run the device upgrades job sequentially or in parallel. After upgrading the devices, you can also specify the reboot order.
  See Software Distribution for further details.

• Distribute images as patches to group of devices
  Depending on system complexity, you can configure upgrades for groups of devices to the patch software images.
  You can specify these groups manually, using your groups and search criteria. You can also use some selection criterion, such as the current software version or hardware type.
  You can run the device upgrades job sequentially or in parallel. After upgrading the devices, you can also specify the reboot order.
  See Patch Distribution for further details.

• Reduce errors by using a recommended image
  Software Management checks the current software version, Flash device size, DRAM size, boot ROM version. Software Management also checks any device type specific software and hardware requirements for compatibility. Software Management checks and recommends a best-fit image for a device.
  See Understanding Upgrade Recommendations for further details.

• Schedule image upgrade jobs
  You can schedule image upgrades to occur immediately or at a later, more convenient time. Optionally, you can integrate software upgrade scheduling into your internal change approval process.
After an upgrade, you can:

- Undo the upgrade and roll back to the previous image

  Software Management tracks the image history of each device so that if you upgrade to a new image, you have a record of what has been installed on the device. This information allows you to undo the upgrade and roll back to the previous image, if necessary.

  A Change Audit record is logged for this task. You can generate the Standard Change Audit report. See Reports Management with Cisco Prime LAN Management Solution 4.2 for more information.

  See Undo a Successful Distribution Job for further details.

- Retry the upgrade on devices that failed in a previous job

  You can also retry a job for devices that failed the upgrade process. For example, you may need to do this because of a configuration error or a bad network connection.

  You can retry the job and include only those devices that were not upgraded previously.

  See Retry a Failed Distribution Job for further details.

• Track job progress and job history information

  Software Management generates detailed job reports. These reports display the status of each software upgrade and a detailed job log. They also keep track of job and device operations and job history information.

  See Using Software Management Job Browser for further details.

• Track software bugs

  You can view the known catastrophic or severe bugs in the software running on the devices supported by Software Management using Locate Device Report (Reports > Cisco.com > Locate Device Report).

  See Reports Management with Cisco Prime LAN Management Solution 4.2 for further details.

• Set the debug mode for Software Management application

  You can set the debug mode for Software Management application in the Log Level Settings dialog box (Admin > System > Debug Settings > Config and Image Management Debugging settings).

  See Administration of Cisco Prime LAN Management Solution 4.2 for further details.

• The supported IOS image version is 11.x and later.

For list of supported devices in the Software Management application, see:

• Supported Image Import Features for Software Management

• Supported Image Distribution Features for Software Management
Setting Up Your Environment

This section lists all prerequisites for using the Software Management in LMS.

- **Requirements on LMS Server**
- **Logging Into Cisco.com**
- **Configuring Devices for Upgrades**
- **Using Job Approval for Software Management**

### Requirements on LMS Server

The following are the prerequisites:

- Make sure you have a directory or file system location with enough space to store the software images.
- Verify that you have the appropriate privilege level to access Software Management options. You can view the Permission Report (Reports > System > Users > Permission) to know the various privilege levels.
- If you do not have a user account and password on Cisco.com, contact your channel partner or enter a request on the main Cisco web site.
- If your system is behind a firewall, configure the proxy URL to access the Internet from the installed system. You can do this using Admin > System > Cisco.com Settings > Proxy Server Setup.
  
  You can enter Cisco.com credentials when you use the Software Management tasks.
  
  See Logging Into Cisco.com for further details.

### Mandatory Setup Tasks

- Add the device passwords to the Device and Credentials database. You can add these credentials using Inventory > Device Administration > Add / Import / Manage Devices. Also, see Configuring Telnet and SSH Access for further details.
- Use the Admin > System > System Preferences option to enter the name of your SMTP server. You have to configure the SMTP server to send e-mails.
  
  We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
- If you plan to enable a remote file copy (RCP) or secure copy server as the active file transfer server, see Configuring RCP or Configuring SCP for further details.
- Set or change your Software Management preferences. See Administration of Cisco Prime LAN Management Solution 4.2 for further details.
Optional Setup Tasks

- Make a baseline of your network images by importing images from the Software Management-supported devices in your network into your software image repository.
  
  To do this, go to Configuration > Tools > Software Image Management > Software Repository and click Add and select Device.

- Schedule the Synchronization report to run periodically. This is used to determine whether any images running on Software Management-supported devices are not in the software image repository.
  
  To generate the report, go to Configuration > Tools > Software Image Management > Repository Synchronization.

- If you use the Job Approval option to approve or reject jobs, you must create one or more approver lists and enable Job Approval. See Administration of Cisco Prime LAN Management Solution 4.2 to enable Job Approval.

Logging Into Cisco.com

Login privileges are required for all Software Management tasks that access Cisco.com.

If you do not have a user account and password on Cisco.com, contact your channel partner or enter a request on the main Cisco web site.

To download the cryptographic images on Cisco.com through Software Management tasks, you must have a Cisco.com account with cryptographic access.

To get the access you must have a Cisco.com account. You can register by going to the following URL: http://tools.cisco.com/RPF/register/register.do

After getting the Cisco.com account:

Step 1
Go to the following URL: http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y

Step 2
Log in with your Cisco.com account.

Step 3
Select your software from the list box and click Submit.

Step 4
Review and complete the Encryption Software Export Distribution Authorization form and click Submit.

After completing the steps, you will receive the Cisco Encryption Software: Crypto Access Granted message.

Note
It takes approximately 4 hours to process your application. You cannot download the software until the entitlement process is complete. You will not receive any notification for this.

On LMS Server, you can enter Cisco.com credentials for Individual user Cisco.com credentials.

You can enter your individual Cisco.com credentials when you perform any Software Management tasks that need access to the Cisco.com server.
If your Cisco.com username and password have not been added to the LMS database, enter your Cisco.com username and password. If you enter Cisco.com credentials in this workflow, the credentials are valid only for that session.

If your Cisco.com username and password have been added to the LMS database, then Cisco.com login dialog box appears with the information that is available in the LMS database.

If you are accessing Cisco.com over a proxy server, you must enter the proxy server details in the Proxy Server Setup dialog box (Admin > System > Cisco.com Settings > Proxy Server Setup).

**Using Job Approval for Software Management**

You can enable Job Approval for Software Management tasks, (Configuration > Job Browsers > Job Approval), which means all jobs require approval before they can run.

Only users with Approver permissions can approve Software Management jobs. Jobs must be approved before they can run if Job Approval is enabled on the system.

The following Software Management tasks require approval if you have enabled Job Approval:

- Adding images to Software Repository (Configuration > Tools > Software Image Management > Software Repository > Add) using:
  - Cisco.com
  - Device
  - URL
  - Network (Use Out-of-sync Report)

- Distributing software images (Configuration > Tools > Software Image Management > Software Distribution) using any one of these methods:
  - Distributing by Devices [Basic]
  - Distributing by Devices [Advanced]
  - Distributing by Images
  - Remote Staging and Distribution

If you have enabled Approval for Software Management tasks, then in the Job Schedule and Options dialog box, you get these two options:

- Maker Comments—Approval comments for the job approver.
- Maker E-Mail—E-mail ID of the job creator.

See *Administration of Cisco Prime LAN Management Solution 4.2* for more details on creating and editing approver lists, assigning approver lists, setting up Job Approval, and approving and rejecting jobs.
Software Repository

The Software Repository Management window displays the images that are available in the Software Management repository.

This section contains:
- Software Repository Synchronization
- Scheduling a Synchronization Report
- Viewing a Synchronization Report
- Removing a Synchronization Report Job
- Adding Images to the Software Repository
- Synchronizing Software Image Status With Cisco.com
- Deleting Images From the Software Repository
- Exporting Images from Software Repository
- Searching for Images from Software Repository
- Software Image Attributes

The Software Repository Management window contains the following fields, buttons, and the entry in the TOC:
- Software Repository Management Window Fields
- Software Repository Management Window Buttons and TOC Entry

Table 9-1 Software Repository Management Window Fields

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>File name of the software image. Click on the File Name to edit the image attributes. See Editing and Viewing the Image Attributes.</td>
</tr>
<tr>
<td>Image Family</td>
<td>Name of the image family.</td>
</tr>
<tr>
<td>Image Type</td>
<td>Type of the images (SYSTEM_SW, SUPERVISOR, SUPERVISOR2_6000, SUPERVISOR6000, BOOT_LOADER, ATM_WBPVC, etc.).</td>
</tr>
<tr>
<td>Version</td>
<td>Software version number.</td>
</tr>
<tr>
<td>Size</td>
<td>Image size in megabytes.</td>
</tr>
<tr>
<td>Updated at</td>
<td>Date and time the image was checked into the repository.</td>
</tr>
<tr>
<td>Comments</td>
<td>Comments, typically used to track the reason for adding the image to the repository.</td>
</tr>
</tbody>
</table>
Table 9-2 lists and describes the buttons and TOC entries in the Software Repository Management Window.

Table 9-2  

<table>
<thead>
<tr>
<th>Buttons and TOC Entry</th>
<th>Description</th>
</tr>
</thead>
</table>
| Software Repository Synchronization (TOC entry) | Keep the software repository up to date. See:  
  • Software Repository Synchronization  
  • Scheduling a Synchronization Report  
  • Viewing a Synchronization Report  
  • Removing a Synchronization Report Job |
| Filter (Button) | Filter and search images. See Searching for Images from Software Repository. |
| Add (Button) | Add images to the repository. See Adding Images to the Software Repository. |
| Delete (Button) | Delete images from the repository. See Deleting Images From the Software Repository. |
| Export (Button) | Export images from Repository. See Exporting Images from Software Repository. |
| Update Status (Button) | Update the status of the images. See Synchronizing Software Image Status With Cisco.com. |

**Software Repository Synchronization**

The Synchronization report shows the Software Management-supported devices that are running software images not available in the software image repository.

Using this option you can view and schedule the synchronization report.

*Note* View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

Select *Configuration > Tools > Software Image Management > Software Repository Synchronization*.

The Software Repository Synchronization dialog box that appears contains the following:

Table 9-3  

<table>
<thead>
<tr>
<th>Fields/Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Id</td>
<td>Unique number assigned to the job when it is created.</td>
</tr>
<tr>
<td>Next Run</td>
<td>Time and date of the next instance of Synchronization Report job.</td>
</tr>
</tbody>
</table>
### Table 9-3  Software Repository Synchronization Dialog Box (continued)

<table>
<thead>
<tr>
<th>Fields/Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Report</td>
<td>You can view the synchronization report. This report displays the Software Management-supported devices that are running software images not available in the software image repository. See <a href="#">Viewing a Synchronization Report</a> for further details.</td>
</tr>
<tr>
<td>Schedule</td>
<td>You can schedule a Synchronization report. You can also reschedule an existing Synchronization report. See <a href="#">Scheduling a Synchronization Report</a> for further details.</td>
</tr>
<tr>
<td>Remove Job</td>
<td>You can remove the scheduled synchronization report job. See <a href="#">Removing a Synchronization Report Job</a> for further details.</td>
</tr>
</tbody>
</table>
Scheduling a Synchronization Report

To schedule or reschedule a Synchronization report:

**Step 1** Go to **Configuration > Tools > Software Image Management > Software Repository Synchronization**. The Software Repository Synchronization dialog box appears.

**Step 2** Click **Schedule**. The Job Schedule for Out-of-sync Report dialog box appears.

**Step 3** Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Time</td>
<td>You can specify when you want to run the Image Out-of-Sync Report job. To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>• Daily—Runs daily at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly—Runs weekly on the day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Monthly—Runs monthly on the day of the month and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete.</td>
</tr>
<tr>
<td></td>
<td>For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed.</td>
</tr>
<tr>
<td></td>
<td>If the 10.00 a.m. November 1 job has not been completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the date and time (hours and minutes) to schedule the job.</td>
</tr>
<tr>
<td>Job Info</td>
<td>The system default job description, SoftwareImages Out Of Synch Report is displayed. You cannot change this description.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender’s address.</td>
</tr>
</tbody>
</table>

**Step 4** Click **Submit**.

If the job was scheduled successfully, the notification dialog box is displayed with the Job ID. You can check the status of your scheduled synchronization job by selecting **Configuration > Tools > Software Image Management > Jobs**.
Viewing a Synchronization Report

To view a synchronization report:

**Step 1** Select Configuration > Tools > Software Image Management > Software Repository Synchronization.

The Software Repository Synchronization dialog box appears.

**Step 2** Click View Report.

The Image Out-of-sync Report window appears.

Removing a Synchronization Report Job

To remove a Synchronization Report job:

**Step 1** Select Configuration > Tools > Software Image Management > Software Repository Synchronization.

The Software Repository Synchronization dialog box appears.

**Step 2** Click Remove Job.

A confirmation dialog box shows that the synchronization report job is removed successfully.

**Step 3** Click OK.

Adding Images to the Software Repository

Your software image repository should contain copies of software images running on all Software Management-supported devices in your network. Use the following options to populate and maintain your software repository:

- Add Image to Software Repository using the Cisco.com option downloads images for devices in LMS from Cisco.com to the software repository.
  
  See Adding Images to the Software Repository From Cisco.com.

- Add Image to Software Repository using the Device option
  – Imports images from selected Cisco devices to the software repository.
  – Imports software from Flash cards on a live device to the software repository.
  
  See Adding Images to the Software Repository From Devices.

- Add Image to Software Repository using the File System option imports an image from a directory accessible from the LMS server.
  
  See Adding Images to the Software Repository From a File System.
Software Repository

- Add Image to Software Repository using the URL option downloads images from the URL you specify.
  See Adding Images to the Software Repository From a URL.
- Add Image to Software Repository using the Network option creates a baseline of all Software Management-supported devices in your network, and imports these images into your software repository.
  See Adding Images to the Software Repository From the Network.

Adding Images to the Software Repository From Cisco.com

Use this option to download software images from Cisco.com into the software image repository.
- Contact your channel partner or enter a request on the main Cisco web site. If you do not have a user account and password on Cisco.com.
  See Logging Into Cisco.com.
- Access the Cisco.com web site to make sure that the releases for the images you plan to download are stable.
- Determine the approximate number and size of the images you want to download. The number of images you can download at a time can vary depending on Cisco.com load, image sizes, network load, and LMS server load.

Note View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To add images from Cisco.com:

Step 1 Select Configuration > Tools > Software Image Management > Software Repository.
The Software Repository Management dialog box appears.
Step 2 Click Add. Do not select any images from Software Repository Management window.
The Image Source dialog box appears.
Step 3 Select Cisco.com.
The Cisco.com and Proxy Server Credential Profile dialog box appears.
  - Enter your Cisco.com username and password. If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.
  - You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:
    Admin > System > Cisco.com Settings > Proxy Server Setup
  - After entering the credential information, Click OK.
Step 4 Click Next.
The Device Selection dialog box appears.
Step 5  Select the device from the Device Selection dialog box, and click Next.
If you do not want to select any devices, click Next.
If you select devices from this list, they identify a subset of device software images. This helps you
narrow your options on subsequent screens.
The Add Images from Cisco.com dialog box appears. This dialog box has several sections from which
you select combinations of device platforms, software release versions, and software subset images.
See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to
use the Device Selector.

Step 6  Select the images to download. Work from left to right and from top to bottom:
  a. From the Select a Device/Platform section, select a device or device family.
     If you select an individual device, the device family, Cisco IOS release, and required Flash and RAM
     sizes appear.
     For IPX/IGX/BPX/MGX devices, the system software release appears.
     A list of available software versions for that device appears in the top middle section.
  b. From the Software Versions section, select a software version.
     If you are unsure of the subset image you need, see the Release Notes on Cisco.com.
     – For IPX/IGX/BPX platforms, both switch software and all applicable module firmware images
       appear.
     – For MGX platforms, system releases appear.
     A list of available subset images for the selected software version appear in the top right frame.
  c. From the Software Subset Images section, select a subset image.
     The subset image is added to the Images to be Added table in the bottom section.
     For IPX/IGX/BPX/MGX devices, there are no subset images. Select the item that appears in this
     section to complete image selection.

Step 7  Continue adding images to the list.
The images that you have added appear in the Images to be Added table. This table contains the
following information:
• Devices/Platforms—Name of the device or platform.
• Version—Software version that you have selected.
• Subset—Subset image information.

Step 8  Click Next when the list contains all image combinations to download.
Software Management verifies that the images in the Image list run in the selected devices and displays
the status in the Add Images from Cisco.com dialog box. The Add Images from Cisco.com dialog box
contains:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device/Platform</td>
<td>Lists the device details that you have selected.</td>
</tr>
<tr>
<td>Selected Version and Subset</td>
<td>Displays the image details.</td>
</tr>
<tr>
<td>Image Requirements</td>
<td>Displays the required hardware (RAM and Flash) details.</td>
</tr>
</tbody>
</table>
Step 9

Select the images to add to the image repository in the Add Images from Cisco.com dialog box and click Next.

The Job Control Information dialog box appears.

Step 10

Enter the following in the Job Control Information dialog box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Download</strong></td>
<td>Select the image you want to download. By default, the check boxes are selected for the images that have passed the verification. You can choose not to add an image by deselecting that check box.</td>
</tr>
<tr>
<td><strong>Pass/Fail</strong></td>
<td>Results of image verification.</td>
</tr>
<tr>
<td></td>
<td>• Pass—Device has the minimum required memory and Flash memory.</td>
</tr>
<tr>
<td></td>
<td>• Fail—Device does not have enough memory or Flash memory.</td>
</tr>
<tr>
<td></td>
<td>Images that fail verification on one device could work on another. Therefore, you can download a failed image by selecting the Download check box.</td>
</tr>
</tbody>
</table>

**Field Description**

**Scheduling**

Run Type

You can specify when you want to run the Image Import (from Cisco.com) job. To do this, select one of these options from the drop-down menu:

- **Immediate**—Runs this job immediately.
- **Once**—Runs this job once at the specified date and time.

Date

If you have selected **Once** for Run Type, select the date and time (hours and minutes) to schedule.

**Job Info**

Job Description

Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.

E-mail

Enter the e-mail address to which the job sends messages at the beginning and at the end of the job.

You can enter multiple e-mail addresses separated by commas.

Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences).

We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.

Comments

Enter additional information about this job.
Adding Images to the Software Repository From Devices

Use this procedure to add software images from Cisco devices to the software repository.

Software Management downloads images from more than one device in parallel. You must ensure that software repository has enough free space to accommodate at least 20 images.

The image import from device option is not available for all the devices. Find the devices from which you can download images in the Supported Image Import Features for the Software Management table on Cisco.com.


**Note** View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To add images from devices:

**Step 1** Select Configuration > Tools > Software Image Management > Software Repository.

The Software Repository Management dialog box appears.

**Step 2** Click Add.

Do not select any images from Software Repository Management window.

The Image Source dialog box appears.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maker E-Mail</td>
<td>Enter the e-mail ID of the job creator. This is a mandatory field.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed only if you have enabled Job Approval for Software Management.</td>
</tr>
<tr>
<td>Maker Comments</td>
<td>Enter comments for the job approver.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed only if you have enabled Job Approval for Software Management.</td>
</tr>
</tbody>
</table>

**Field**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Description</td>
<td>Displays the job description. This is what you entered while scheduling the job.</td>
</tr>
<tr>
<td>Work Order</td>
<td>Displays the details of the device name and image name that you have selected. It also displays the file size of the image.</td>
</tr>
</tbody>
</table>

**Step 11** Click Next.

The Image Import Work Order dialog box appears with the following information:

**Step 12** Click Finish.

If the job was scheduled successfully, the notification dialog box appears with the Job ID.

To check the status of your scheduled synchronization job, select Configuration > Tools > Software Image Management > Jobs.
**Step 3** Select **Device**, and click **Next**.

The Device Selection dialog box appears in the Add Images from Device window.

See *Inventory Management with Cisco Prime LAN Management Solution 4.2* for information on how to use the Device Selector.

**Step 4** Select the devices that contain the images to add to the software repository.

**Step 5** Click **Next**.

Software Management retrieves the images, analyzes them according to the selected image type, and displays a report that contains:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image</td>
<td>Images available on your device.</td>
</tr>
<tr>
<td>Available At</td>
<td>Location where the image is available on your device.</td>
</tr>
<tr>
<td>Device</td>
<td>Name of the device as managed by LMS.</td>
</tr>
<tr>
<td>Size</td>
<td>Image size in bytes.</td>
</tr>
<tr>
<td>Errors</td>
<td>Click on the link for details.</td>
</tr>
</tbody>
</table>

By default, the check boxes of the images that are not in the software repository are selected. You can choose not to add an image by deselecting the corresponding check box.

**Step 6** Click **Next**.

The Job Control Information dialog box appears.

**Step 7** Enter the following in the Job Control Information dialog box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>You can specify when you want to run the Image Import (from Device) job.</td>
</tr>
<tr>
<td></td>
<td>To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs this job immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs this job once at the specified date and time.</td>
</tr>
<tr>
<td>Date</td>
<td>If you have selected <strong>Once</strong> for Run Type, select the date and time (hours and minutes) to schedule.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Job Info</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Description</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job.</td>
</tr>
<tr>
<td></td>
<td>You can enter multiple e-mail addresses separated by commas.</td>
</tr>
<tr>
<td></td>
<td>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences).</td>
</tr>
<tr>
<td></td>
<td>We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.</td>
</tr>
</tbody>
</table>
Adding Images to the Software Repository From a File System

Use the following procedure to add software images from a file system to the software repository.

You have to know the directory name in which the image files are stored before importing the images from the File System to the software repository.

**Note**

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To add images from file system:

**Step 1**  Select Configuration > Tools > Software Image Management > Software Repository.

The Software Repository Management dialog box appears.

**Step 2**  Click Add..

Do not select any images from the Software Repository Management window.

The Image Source dialog box appears in the Add Images window.

**Step 3**  Click File System, and click Next.

The Add Image From Local File System dialog box appears.
Step 4  Enter the full pathname of the source file or directory.

Or

a. Click **Browse** to search for the directory name.
   The Server Side File Browser dialog box appears.

b. Select either the file or the directory on the LMS server.

c. Click **OK**.

Step 5  Click **Next**.

The Image Attributes dialog box appears with this information:

- **Filename**—Filename as it appears in filesystem directory.
  You cannot add an image if a file with the same name already exists in the software repository or if the minimum required attributes cannot be retrieved.

- **Image Type**—Image type, determined from the filename. If the image type is not correct, select the correct type from the drop-down list box.

  Software Management tries to determine the image type from the filename. If it cannot determine the image type (for example, if the image has been renamed using a nonstandard name), it labels the image type as **Unknown**.

By default, the check boxes of the images that are not in the software repository are selected. You can choose not to add an image by deselecting the corresponding check box.

Step 6  Click **Next**.

The Image Attributes window appears with the following information for verification:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>Filename as it appears in filesystem directory</td>
<td>You cannot add images if a file with the same name already exists in the software repository or if the minimum required attributes cannot be retrieved.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of file in bytes.</td>
<td>None.</td>
</tr>
<tr>
<td>Image Family</td>
<td>Device family name.</td>
<td>None.</td>
</tr>
<tr>
<td>Image Type</td>
<td>Image type, determined from the filename.</td>
<td>Software Management tries to determine the image type from the filename. If it cannot determine the image type (for example, if the image has been renamed to a nonstandard name), it labels the image type as <strong>Unknown</strong>. You must select an image type from an available option before you can add the file to the repository.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the image</td>
<td>None.</td>
</tr>
<tr>
<td>Errors</td>
<td>Click on the link for details.</td>
<td>None.</td>
</tr>
</tbody>
</table>

Step 7  Click **Finish**.

A pop up window appears for you to enter a description.
Step 8  Either:
   • Click **OK**.

   The Software Repository Management window appears with the newly added images. The
description that you have entered appears in the Comments column in the Software Repository
Management window.

   Or

   • Click **Cancel**.

   The Software Repository Management window appears with the newly added images. The
Comments column in the Software Repository Management window will be blank for this task.

---

**Note**
The import from File System may take more time if you have selected many images.

---

**Adding Images to the Software Repository From a URL**

Use the following procedure to add software images from a URL to the software repository.

**Note**
View Permission Report (**Reports > System > Users > Permission**) to check if you have the required
privileges to perform this task.

To add images from URL:

**Step 1**  Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management window appears.

**Step 2**  Click **Add**.

Do not select any images from the Software Repository Management window.

The Image Source dialog box appears in the Add Images window.

**Step 3**  Click **URL**, and click **Next**.

The Add Image From URL dialog box appears.

**Step 4**  Enter the URL details.

For example: http://servername:portnumber/file_location/

Where,

• **servername** is the name of the server where the image resides.

• **portnumber** is the http port number.

• **file_location** is the image location on the server. The file_location can be swimtemp or htdocs folder.

For example,

   If the image is in swimtemp, then the URL is http://servername:portnumber/swimtemp/image_file

   If the image is in the htdocs, then the URL is http://servername:portnumber/image_file

The web server must be running on the destination machine. You can use only HTTP URLs. The remote
server should not have any authentication.
Step 5  Click Next.

The Job Control Information dialog box appears.

Step 6  Enter the following information in the Job Control Information dialog box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>You can specify when you want to run the Image Import (from URL) job.</td>
</tr>
<tr>
<td></td>
<td>To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs this job immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs this job once at the specified date and time.</td>
</tr>
<tr>
<td>Date</td>
<td>If you have selected Once for Run Type, select the date and time (hours and minutes) to schedule the job.</td>
</tr>
<tr>
<td><strong>Job Info</strong></td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You cannot enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter the additional information about this job.</td>
</tr>
<tr>
<td>Maker E-Mail</td>
<td>Enter the e-mail ID of the job creator. This is a mandatory field.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed only if you have enabled Job Approval for Software Management.</td>
</tr>
<tr>
<td>Maker Comments</td>
<td>Enter comments for the job approver.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed only if you have enabled Job Approval for Software Management.</td>
</tr>
</tbody>
</table>

Step 7  Click Next.

The Image Import Work Order dialog box appears with the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Description</td>
<td>Displays the job description. This description is what you entered while scheduling the job.</td>
</tr>
<tr>
<td>Work Order</td>
<td>Displays the details of the device name and image name that you have selected. It also displays the file size of the image.</td>
</tr>
</tbody>
</table>
Step 8  
Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select Configuration > Tools > Software Image Management > Jobs.

---

**Adding Images to the Software Repository From the Network**

This option allows you to import running images from all Software Management-supported devices in your network into the software image repository.

Use this option to create a baseline of the image in your network and populate the software image repository. Use the Synchronize report option to review the Software Management supported devices are running images that are not in the Software Repository.

**Note**  
View **Permission Report (Reports > System > Users > Permission)** to check if you have the required privileges to perform this task.

You must locate your device in the Supported Image Import Features for Software Management table on Cisco.com. This is because the image baseline capabilities might not be available yet for all devices.


To add images from network:

**Step 1**  
Select Configuration > Tools > Software Image Management > Software Repository.  
The Software Repository Management dialog box appears.

**Step 2**  
Click **Add**. Do not select any images from the Software Repository Management window.  
The Image Source dialog box appears.

**Step 3**  
Select **Network**, and click **Next**.  
Software Management checks the devices on your network and the software images running on those devices.

To run this check faster, select **Use generated Out-of-sync Report** to find the images that are not in the Software Images repository.

You should generate an Out-of-sync Report before selecting this option. The running images in the network that are not in the Software Repository, appear in the Network Baselining dialog box.

If you have not selected the Use generated Out-of-sync Report option, all running images that are not in the Software Repository appear in the Network Baselining dialog box.
The Network Baselining dialog box contains the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>Filename as it appears in filesystem directory. You cannot add an image if a file with the same name already exists in the software repository or if the minimum required attributes cannot be retrieved.</td>
</tr>
<tr>
<td>Size</td>
<td>Image size in bytes.</td>
</tr>
<tr>
<td>Available at</td>
<td>Location where the image is available on your device.</td>
</tr>
<tr>
<td>Error</td>
<td>Click on the link to review the details.</td>
</tr>
</tbody>
</table>

By default, the check boxes of the images that are not in the Software Repository are selected. You can choose not to add an image by deselecting the corresponding check box.

**Step 4** Select/deselect the images and click **Next**.

The Job Control Information dialog box appears.

**Step 5** Enter the following information in the Job Control Information dialog box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>You can specify when you want to run the Image Import (from Network) job.</td>
</tr>
<tr>
<td>Date</td>
<td>If you have selected <strong>Once</strong> for Run Type, select the date and time (hours and minutes) to schedule the job.</td>
</tr>
<tr>
<td>Job Info</td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter additional information about this job.</td>
</tr>
<tr>
<td>Maker E-Mail</td>
<td>Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.</td>
</tr>
<tr>
<td>Maker Comments</td>
<td>Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.</td>
</tr>
</tbody>
</table>
Step 6 Click Next.
The Image Import Work Order dialog box appears with the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Description</td>
<td>Displays the job description. This description is what you entered while</td>
</tr>
<tr>
<td></td>
<td>scheduling the job.</td>
</tr>
<tr>
<td>Work Order</td>
<td>Displays the details of the device name and image name that you have</td>
</tr>
<tr>
<td></td>
<td>selected. It also displays the file size of the image.</td>
</tr>
</tbody>
</table>

Step 7 Click Finish.
If the job was scheduled successfully, the notification dialog box appears with the Job ID.
To check the status of your scheduled synchronization job, select Configuration > Tools > Software Image Management > Jobs.

Synchronizing Software Image Status With Cisco.com

You can check if the software images that are in your software repository are valid images using the Update Status button in the Software Repository Management window.
The Status table column is updated with the following status:
- Not Deferred—Displayed when this image is a valid image.
- Deferred—Displayed when this image is not supported and not available to be downloaded from Cisco.com.
  This image is not recommended by Software Management.
- Software Advisory Notice—Displayed when this image has some issues. You can download this image from Cisco.com.
  This image may be recommended by Software Management. However, you have to read the Software Advisory Notice before importing or upgrading your device.
- Unknown—Displayed when you have added images to the repository for the first time, using any one of these methods:
  - Add Images by Devices
  - Add Images by File system
  - Add Images by URL
  - Add Images from Network
  Use the Update Status button to update the status field.
- Not available—Displayed when information is not available on Cisco.com.
Read the software release notes on Cisco.com for more details.

Note View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.
To synchronize Software Image Status with Cisco.com:

### Step 1
Select **Configuration > Tools > Software Image Management > Software Repository**.
The Software Repository Management dialog box appears.

### Step 2
Select the images for which you want to know the status and click **Update Status**.
The Cisco.com login dialog box appears.
- If your Cisco.com username and password have not been added to the LMS database, enter your Cisco.com username and password, click **OK**. If you enter Cisco.com credentials in this workflow then the credentials are valid only for that session.
- If your Cisco.com username and password have been added to the LMS database, the Cisco.com login dialog box appears with the information that is available in the LMS database. Click **OK**.
A confirmation message appears that Image Status was retrieved from Cisco.com successfully.

### Step 3
Click **OK**.
Review the Status table column in the Software Repository Management window.

### Deleting Images From the Software Repository

To delete software images from the software repository:

#### Note
View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

### Step 1
Select **Configuration > Tools > Software Image Management > Software Repository**.
The Software Repository Management dialog box appears.

### Step 2
Select the images that you want to delete, then click **Delete**.
A confirmation message appears, **The selected images will be deleted.**

### Step 3
Click **OK**.
The Software Repository Management window reappears with the selected images deleted.
Exporting Images from Software Repository

To export software images from the Software Repository:

---

**Step 1** Select **Configuration > Tools > Software Image Management > Software Repository**.
The Software Repository Management dialog box appears.

**Step 2** Select images that you want to export, then click **Export**.
A confirmation message appears, **The selected images will be exported.**

**Step 3** Click **OK**.
The Select directory to export window appears.

**Step 4** Click on **Browse** to select a directory to which you want to export the selected images.
The Server Side File Browser dialog box appears.

**Step 5** Choose the required directory and click **OK**.
The Image Directory field in the Select directory to export window displays the directory location that you had selected.

**Step 6** Click **Next**
A progress bar appears indicating the progress of the export of images.
The Export Images Summary Report appears, after the image export is completed with the following details:
- Number of Selected Images
- Target Directory
- Summary

**Step 7** Click **Finish**.
You have successfully exported the images to the selected directory.
Searching for Images from Software Repository

To search software images from the software repository:

Note View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

Step 1 Select Configuration > Tools > Software Image Management > Software Repository. The Software Repository Management dialog box appears.

Step 2 Select one of the following from the Filter by drop-down list:
- File Name
- Image Family
- Image Type
- Version
- Size
- Updated At

You cannot use wildcard characters. However, you can filter based on the first character.

For example: If you have images with file names `c3640-i-mz.112-24.P.bin`, `c3640-i-mz.112-25.P.bin`, `cat5000-sup.5-5-18.bin`, and `cat5000-supg.6-4-10.bin`.

If you select File Name as the Filter by option and enter the value as `c3`. The filter result displays only `c3640-i-mz.112-24.P.bin` and `c3640-i-mz.112-25.P.bin` images.

Step 3 Click Filter. The Software Repository Management window appears with the filtered image details.

Software Image Attributes

To ensure that Software Management is using the most current information about an image, you should keep the image attributes up to date. Software Management uses image attribute information to:

- Recommend the appropriate image for a given device
  When you distribute an image from the software repository to a device, Software Management uses the image attributes to recommend an image.
- Notify you when a Flash memory or DRAM upgrade is required (upgrade analysis)
  When you distribute an image from the Software Repository to a device, Software Management compares the current Flash memory and DRAM attributes with the Flash memory and DRAM requirements for the new image.
The following sections contain:

- Understanding Software Image Attributes
- Understanding Default Attribute Values
- Finding Missing Attribute Information
- Editing and Viewing the Image Attributes

### Understanding Software Image Attributes

To ensure that Software Management is using the most current information about an image, keep the image attributes updated.

If you do not have all the image attribute information when you add the image to the Software Repository, you must edit the attributes when the information becomes available.

**Note**
The auto fill of the Minimum NVRAM, Minimum RAM and Minimum Bootflash image attributes is applicable only for IOS.

The attributes for software images are:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum RAM</td>
<td>Minimum RAM required.</td>
<td>Select it from the list of options.</td>
</tr>
<tr>
<td>Minimum Flash</td>
<td>Minimum Flash memory required.</td>
<td>Select it from the list of options.</td>
</tr>
<tr>
<td>Minimum Boot ROM</td>
<td>Minimum bootstrap version required.</td>
<td>Enter text in standard Cisco IOS format: a.b(c).</td>
</tr>
<tr>
<td>Minimum system software version</td>
<td>Minimum system software version required on the device to upgrade the microcode image (MICA portware, Microcom firmware, CIP microcode only)</td>
<td>Enter text in standard Cisco IOS format: a.b(c).</td>
</tr>
<tr>
<td>Minimum supervisor version</td>
<td>Minimum software image version required on supervisor engine module. Cisco Switches can contain any number of modules such as, ATM, FDDI/CDDI, etc. These modules can run different images. There are some interdependencies among the software images that can run on the supervisor engine module and the ATM, FDDI/CDDI, and Token Ring modules residing on the same device chassis.</td>
<td>Enter text in standard Cisco IOS format: a.b(c).</td>
</tr>
<tr>
<td>Minimum NVRAM</td>
<td>Minimum NVRAM required to run image on Supervisor Engine III.</td>
<td>Select from list of options.</td>
</tr>
</tbody>
</table>
Understanding Default Attribute Values

The Unknown attribute option has different meanings for different image attributes.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>If you select <strong>Unknown</strong>, Software Management computes the RAM value.</td>
</tr>
<tr>
<td>Flash Size</td>
<td>If Min.Flash is unknown, it is ignored. If the image size is unknown, the required Flash size to copy the image cannot be determined and the image cannot be used for upgrade.</td>
</tr>
<tr>
<td>Boot ROM Version</td>
<td>If you select <strong>Unknown</strong>, no value is stored in this field and the image can run with any boot ROM image version.</td>
</tr>
</tbody>
</table>

Finding Missing Attribute Information

When you import an image from another filesystem, the image might not contain all the attribute information that Software Management requires.

You can find the missing attribute information in the following ways:

- Read the Release Notes on Cisco.com or the documentation CD-ROM.
- Review the image attribute information that is available along with the images, when you download the images from Cisco.com.

You can update the missing attribute information in the Edit/View Image Attributes dialog box.

See Editing and Viewing the Image Attributes for further details.

Editing and Viewing the Image Attributes

LMS allows you to edit and view image attributes.

**Note**

View Permission Report ([Reports > System > Users > Permission](#)) to check if you have the required privileges to perform this task.

To edit the software images attributes:

**Step 1** Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

**Step 2** Click the **File Name**.

The Edit/View Image Attributes dialog box displays attributes for the selected image type.

**Step 3** Make your changes in the available editable fields.

For editable image attributes, you will get either a drop-down list or text fields that you can edit.
Step 4  Either:
- Click **Update**, if you have updated the image attributes.
  The Software Repository Management dialog box appears after updating the attributes.
  Or
- Click **OK**, if you have not updated the image attributes.
  The Software Repository Management dialog box appears without updating the attributes.

Software Distribution

Software Distribution allows you to distribute images in your network and to analyze and determine the
impact and prerequisites for new software images before distribution.

This section contains:
- Upgrade Analysis
- Software Distribution Methods
- Patch Distribution
- Remote Staging and Distribution
- Understanding Upgrade Recommendations

Upgrade Analysis

Before planning a software image upgrade, you must determine the prerequisites of the new software
images. You can analyze these by using,
- Cisco.com (See **Planning an Upgrade From Cisco.com**.)
- Repository (See **Planning an Upgrade From Repository**.)

This section contains:
- Understanding the Upgrade Analysis Report
- Support for In Service Software Upgrade
- Planning the Upgrade
- Configuring Devices for Upgrades
- Scheduling the Upgrade
Planning an Upgrade From Cisco.com

Use the Cisco.com Upgrade Analysis option to determine the impact to and prerequisites for a new software deployment using images that reside in Cisco.com.

This option allows you to identify only images that meet certain criteria. It then analyzes the images to determine the required hardware upgrades (boot ROM, Flash memory, RAM, and access).

This option helps you answer questions such as:

- Does the device have sufficient RAM to hold the new software?
- Have the minimum ROM version requirements been met?
- Is the Flash memory large enough to hold the new software?
- Do I need to add Telnet access information for the device to the Device and Credential Repository?
- Have I performed an upgrade path and NVRAM analysis on my Catalyst devices?
- Does the module firmware on my IPX/IGX/BPX devices need to be upgraded?

**Note** View Permission Report ([Reports > System > Users > Permission](#)) to check if you have the required privileges to perform this task.

To upgrade from Cisco.com:

**Step 1**
Select [Configuration > Tools > Software Image Management > Upgrade Analysis](#).
The Select Upgrade Source dialog box appears.

**Step 2**
Select [Cisco.com](#) and click [Go](#).
The Device Selection dialog box appears.

**Step 3**
Select the devices to analyze, then click [Next](#).

See [Administration of Cisco Prime LAN Management Solution 4.2](#) for information on how to use the Device Selector.

The Cisco.com and Proxy Server Credential Profile dialog box appears.

a. Enter your Cisco.com username and password.

   If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.

   You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:

   - [Admin > System > Cisco.com Settings > Proxy Server Setup](#)

b. Click [OK](#) after entering the credential information.

The Cisco.com Upgrade Analysis dialog box appears with the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device</td>
</tr>
<tr>
<td>Running Image</td>
<td>Running image of the device</td>
</tr>
</tbody>
</table>
Step 4  Click **Finish** to update the upgrade path information.

The Upgrade Analysis Report appears in a new browser window.
See [Understanding the Upgrade Analysis Report](#) for details.

### Planning an Upgrade From Repository

Use the Repository Upgrade Analysis option to analyze images in your software repository and determine the impact to and prerequisites for a new software deployment. The option produces the Upgrade Analysis report, which shows the required boot ROM, Flash memory, RAM, and access.

This option helps you answer such questions as:

- Does the device have sufficient RAM to hold the new software?
- Have the minimum ROM version requirements been met?
- Is the Flash memory large enough to hold the new software?
- Do I need to add Telnet access information for the device to the Device and Credential Repository?
- Does the module firmware on my IPX/IGX/BPX devices need to be upgraded?

**Note**

View Permission Report ([Reports > System > Users > Permission](#)) to check if you have the required privileges to perform this task.

To upgrade from repository:

**Step 1**  Select **Configuration > Tools > Software Image Management > Upgrade Analysis**.

The Select Upgrade Source dialog box appears.

**Step 2**  Select **Repository**, then click **Go**.

The Repository Upgrade Analysis dialog box appears.

**Step 3**  From the list, select the image to analyze, then select the devices to upgrade, then click **Run Report**.

The Upgrade Analysis Report window appears.
See [Understanding the Upgrade Analysis Report](#) for details.
Understanding the Upgrade Analysis Report

The Upgrade Analysis report summarizes the impact to and prerequisites for a new software deployment for the selected devices. It is generated by the Cisco.com Upgrade Analysis (Planning an Upgrade From Cisco.com) and Repository Upgrade Analysis (Planning an Upgrade From Repository) options.

The information that is shown in this report depends on the device type you have selected. See these tables to understand the Upgrade Analysis Report, Table 9-5 and Table 9-6.

Locate your device in the Supported Image Import Features for Software Management table on Cisco.com. For some devices the upgrade analysis option may not be available yet.

<table>
<thead>
<tr>
<th>Table 9-5 Upgrade Analysis Report Columns</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column</strong></td>
</tr>
<tr>
<td>Device Information</td>
</tr>
<tr>
<td>Boot ROM Upgrade</td>
</tr>
<tr>
<td>Flash Upgrade</td>
</tr>
<tr>
<td>RAM Upgrade</td>
</tr>
<tr>
<td>Telnet Access</td>
</tr>
<tr>
<td>Boot Flash Upgrade</td>
</tr>
<tr>
<td>NVRAM Upgrade</td>
</tr>
<tr>
<td>Module Firmware Upgrade</td>
</tr>
<tr>
<td>Firmware Compatibility</td>
</tr>
</tbody>
</table>

The following table (Table 9-6) maps the Upgrade Analysis Report to the supported device types:

- Optical Networking
- Routers and Switches
- Storage Networking

The Upgrade Analysis from Cisco.com and Repository are not supported for these device types because the required information for the upgrade analysis is not provided by the device:

- Universal Gateways and Access Servers
- Content Networking
- DSL and Long Reach Ethernet (LRE)
- Optical Networking
- Security and VPN
- Broadband Cable
- Voice and Telephony
- Network Management
- Wireless
- Cisco Interfaces and Modules
### Table 9-6  Upgrade Analysis Report Based on Device Type

<table>
<thead>
<tr>
<th>Upgrade Analysis Report Columns</th>
<th>Device Type: Routers and Optical Networking</th>
<th>Device Type: Switches</th>
<th>Device Type: Storage Networking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot ROM Upgrade</td>
<td>Supported</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Flash Upgrade</td>
<td>Supported</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>RAM Upgrade</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Telnet Access</td>
<td>Supported</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Boot Flash Upgrade</td>
<td>Not supported</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>NVRAM Upgrade</td>
<td>Not supported</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Module Firmware Upgrade</td>
<td>Supported.</td>
<td>Supported.</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>See the Supported Image Distribution Features for Software Management table on Cisco.com for the router’s device list that supports Module Firmware Upgrade. <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html">http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html</a></td>
<td>Supported. This is applicable for the following devices: • IPX/IGX/BPX device switch • MGX system</td>
<td></td>
</tr>
<tr>
<td>Firmware Compatibility</td>
<td>Not supported</td>
<td>Supported.</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is applicable for the following devices: IPX/IGX/BPX device firmware</td>
<td></td>
</tr>
</tbody>
</table>

In addition to this information, you can use the Go To drop-down list to navigate to particular device analysis report.

### Button Description

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export to File (Icon)</td>
<td>Exports the analysis report in CSV or PDF format.</td>
</tr>
<tr>
<td>Print (Icon)</td>
<td>Generates a format that can be printed.</td>
</tr>
</tbody>
</table>
Support for In Service Software Upgrade

LMS supports In Service Software Upgrade (ISSU) process. This process allows Cisco IOS software images to be updated without rebooting the device. This increases network availability and reduces downtime caused by planned software upgrades.

To perform the image upgrade using this ISSU process, the running image and the upgrade image must be ISSU capable and should be available in the flash memory.

The ISSU image upgrade process may fail if:

- The running or the upgrade image is not available in the flash memory
- The running image is deleted because of flash cleanup operation performed while the job is running.

ISSU support is available only for the following devices:

- Cisco Catalyst 6000 Series IOS Dual Chassis (VSS) Switches
- Cisco Catalyst 6000 Series Dual Supervisor Switches

ISSU process can be applied to the following distribution methods:

- By devices [Basic]
- By image
- Use remote staging

To perform this ISSU image upgrade process:

- Select **Reboot immediately after downloading** in the Job Schedule and Options page of the Device Distribution flow.
- You can also customize the configurations available in the Issuconf.properties file located at:
  - `NMSROOT/MDC/tomcat/webapps/rme/WEB-INF/conf/swim` (On Solaris and Soft Appliance)
  - `NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\conf\swim` (On Windows)

`NMSROOT` is the LMS install directory.
You can configure the following properties in the Issuconf.properties file:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RBTCongfig</td>
<td>Configure the rollback timer. By default, the value of this variable is set as NO. If you configure the value as <strong>Yes</strong>, then rollback will happen for the value set in the variable <strong>RollBackTime</strong>.</td>
</tr>
<tr>
<td>RollBackTime</td>
<td>Enter the rollback timer (value in minutes). By default, the rollback time is set as 45. To consider the value for rollback timer you must set the RBTCongfig value as <strong>Yes</strong>.</td>
</tr>
<tr>
<td>IssuSupImgVer</td>
<td>The ISSU supported version of the running image. For ISSU upgrade support, the value for this variable must be an ISSU capable image version such as <strong>SXI</strong>. This value can either match the version of the running image completely, or partially. For example, 12.2(33)SXI, or SXI.</td>
</tr>
</tbody>
</table>

The running software image version in the device must match the version configured in the Issuconf.properties.

If the running image or the upgrade image is not an ISSU capable image, or the version of the image is wrongly configured for the variable “IssuSupImgVer” in the Issuconf.properties file, then ISSU upgrade process will not happen and LMS proceeds with the normal upgrade process.

For example, if the running image version is 12.2(33)SXI, which is ISSU capable, and the version entered for the variable “IssuSupImgVer” is 12.2(33)SXH, then ISSU upgrade will not happen and LMS proceeds with normal upgrade process.

To fix this issue, you must provide the proper version for the variable “IssuSupImgVer” that is ISSU capable. For example, 12.2(33)SXI, or SXI.

**Software Distribution Methods**

You can distribute images to the devices in your network, using any of these options:

- **Distribute by Devices [Basic]:**
  
  This option enables you to select devices and perform software image upgrades to those devices. Software Management checks the current image on the device and recommends a suitable image and the appropriate image storage for distribution.

  See **Distributing by Devices [Basic]**

- **Distribute by Devices [Advanced]:**
  
  This option enables you to enter the software image and storage media for the device that you want to upgrade.

  The selected image and storage media is validated and verified for dependencies and requirements based on the device information that you entered when you added devices to the Device Credentials Repository.

  See **Distributing by Devices [Advanced]**
Software Distribution

- Distribute by Images:
  This option enables you to select a software image from the software image repository and use it to perform an image upgrade on suitable devices in your network. This option is useful when you have to distribute the same image to multiple devices.
  See Distributing by Images.

- Remote Staging and Distribution:
  This option enables you to select a software image, store it temporarily on a device and then use this stored image to upgrade suitable devices in your network. This option is helpful when the LMS server and the devices (including the remote stage device) are distributed across a WAN.
  See Remote Staging and Distribution.

You can run the device upgrades job sequentially or in parallel. After the devices upgrade, you can also specify the reboot order. You can specify these options in the Job Schedule and Options dialog box.

During the image upgrade, Software Management:

- Checks the amount of Flash memory on the device. If Flash memory needs to be erased before the new system image is loaded and erasing is allowed, it erases the Flash memory. Before erasing the Flash, a warning message appears Flash memory will be erased.
- Performs MD5 Checksum check of the image when it is downloaded from Cisco.com directly. It also performs image size check once the image is copied to a device, to check if there was any network transfer issue. These are the image consistency checks performed by Software Management.
- Provides a running log of the upgrade job.
- E-mails a report on the results to the specified addresses after completing the upgrade.
- Inserts boot commands to activate the upgraded image.
- Reboots the device if the Reboot Schedule option has been set to Reboot Immediately.
- RAM value is not checked. Hence, distribution proceeds without any errors even if the RAM value is unknown.
- Min.Flash is ignored, if Min.Flash is unknown.
- Image cannot be used for upgrade, if Flash size is unknown.

After you schedule an image upgrade, you can use Software Management Job Browser (Configuration > Job Browsers > Software Image Management) to review, retry, or cancel a job.

After a successful distribution job, Software Management triggers

- An inventory and a configuration collection.
This section contains:

- Planning the Upgrade
- Configuring Devices for Upgrades
- Scheduling the Upgrade
- Authorizing a Distribution Job
- Distributing by Devices [Basic]
- Distributing by Devices [Advanced]
- Distributing by Images

Planning the Upgrade

Planning the upgrade typically involves these phases:

- Identifying Possible Changes
- Satisfying the Prerequisites
- Maintaining Your Software Image Repository
- Testing the New Images

Identifying Possible Changes

Identifying which devices at your site might require software upgrades consists of these phases:

- Determine whether an upgrade is required
  
  You can learn about new features or fixes in different ways.
  
  You use the Browse Bugs option (Reports > Cisco.com > Bug Summary) to summarize the software image bugs for the devices in your network.
  
  You can schedule a Browse Bugs job to run at regular intervals. This will help you determine any bugs related to current running images on the devices.
  
  If you find a bug in your software, call the Technical Assistance Center (TAC) to know the status of the bug.
  
  Your sales engineer or channel partner notifies you of new features that might be appropriate for your site.
  
  You check Cisco.com periodically to review new release notes, bug-fix documentation, and marketing bulletins.

- Retrieve information about the upgrade
  
  Go to Cisco.com to read the most recent product Release Notes or bug-fix documentation. This information will help you determine the software image version you need.

- Determine whether the upgrade is really necessary
  
  After you determine the version you need, you can list the current software version numbers for your managed devices.
  
  You can generate this using (Reports > Inventory > Software)

Satisfying the Prerequisites

Run Cisco.com Upgrade Analysis or Repository Upgrade Analysis to determine the prerequisites for a new software deployment. See Upgrade Analysis for further details.
In addition, you need to answer questions such as:

- Have you supplied the minimum requirements such as the minimum device configuration requirements for each device? See Meeting Minimum Device Requirements for further details.
- Is the device running from Flash (RFF)?
- Does the device have multiple Flash partitions?
- Does the Supervisor board require a new software image?
- Have you satisfied the additional requirements for the devices? See Configuring Devices for Upgrades for further details.

**Maintaining Your Software Image Repository**

- Use the Adding Images to the Repository > Network option to import running images from all Software Management-supported devices in your network into the repository.
  
  See Adding Images to the Software Repository From the Network for further details.
- Since you can download new images to a device without using Software Management, eventually the software image repository might not reflect the images that are running on your network devices.
  
  To keep the repository current:
  - Review all software images in the repository.
    
    See Software Repository for further details.
  - Schedule the Synchronization report to run periodically.
    
    See Scheduling a Synchronization Report for further details.
  - Retrieve additional images from Cisco.com, another device, or a file system on your server.
    
    See Adding Images to the Software Repository for further details.
- Download Cisco images from Cisco.com during a scheduled distribution job.

**Testing the New Images**

To confirm the stability of your network after upgrades, test the new software images before you perform a full-scale deployment.

You cannot roll back software upgrades for supervisor modules on Catalyst 5000 series switches. Therefore, test the new images for these devices thoroughly before deploying them on your network.

**Configuring Devices for Upgrades**

This section lists all the required tasks that have to be performed on Cisco devices. This section also captures the following information:

- Meeting Minimum Device Requirements
- Meeting Additional Device Requirements
- Additional SFB Checks
- Configuring Telnet and SSH Access
- Configuring SCP
Meeting Minimum Device Requirements

Before you can upgrade software images, you must meet the following requirements:

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device configuration</td>
<td>Device must be configured with SNMP read-write community string.</td>
</tr>
<tr>
<td></td>
<td>There should not be any access list on the device that will disable TFTP</td>
</tr>
<tr>
<td></td>
<td>transfers from the workstation.</td>
</tr>
<tr>
<td>IOS and ONS devices</td>
<td>For the device to be rebooted using the SNMP protocol, you must configure</td>
</tr>
<tr>
<td></td>
<td>the <code>snmp-server system-shutdown</code> command on the device.</td>
</tr>
<tr>
<td>SFB devices</td>
<td>See Additional SFB Checks for further details.</td>
</tr>
<tr>
<td>RSP 7000 or 7500 devices</td>
<td>See Additional SFB Checks for further details.</td>
</tr>
<tr>
<td>running Cisco IOS version</td>
<td></td>
</tr>
<tr>
<td>11.x or later</td>
<td></td>
</tr>
<tr>
<td>Microcode images</td>
<td>See Meeting Microcode and Modem Firmware Requirements for further details.</td>
</tr>
<tr>
<td>Inventory</td>
<td>SNMP read-write community string must be in Device and Credentials database</td>
</tr>
<tr>
<td></td>
<td>(Inventory &gt; Device Administration &gt; Add / Import / Manage Devices).</td>
</tr>
<tr>
<td>tftpboot directory space</td>
<td>Must have enough space for all concurrent jobs, which could include image</td>
</tr>
<tr>
<td></td>
<td>distribution, image import, config file scan, and so on.</td>
</tr>
</tbody>
</table>

Meeting Additional Device Requirements

Before you upgrade, you must meet the following additional device requirements:

- Make sure you have Telnet access to upgrade the devices. Before you upgrade, add the Enable mode password (see Configuring Telnet and SSH Access) and access information for each device to the Device and Credential Repository.

  See the Software Management Functional Supported Device tables on Cisco.com for the devices list that requires Telnet access.


- To perform the upgrade, the device must be rebooted to RxBoot mode using SNMP. Do this even if you have selected the Do not reboot option when scheduling the upgrade. This procedure is applicable only to RFF devices.
• Configure PIX Firewall for SNMP and telnet access. For LMS to manage these devices, you must enter these commands on the device, in the config mode:
  1. `config terminal`
  2. `snmp -server host hostname`
  3. `snmp -server community community name`
  4. `telnet ip 255.255.253.255 inside interface`
  5. `write mem`

Additional SFB Checks

Software Management validates the image upgrades at the time the job is scheduled. For SFB devices, Software Management also verifies that:

• IP routing is enabled on the device.
• The ethernet interface that connects LMS to the device has an IP address assigned to it and is routing IP protocol.
• If the device is configured with Frame Relay subinterfaces, the device software version is 11.1 or higher.
• The ROM monitor code version is 5.2 or higher.

Configuring Telnet and SSH Access

Before you schedule the upgrade, use the Device and Credentials (Inventory > Device Administration > Add / Import / Manage Devices) option to add or change passwords and access information.

When you select the SSH protocol for the Software Management, the underlying transport mechanism checks whether the device is running SSHv2.

If so, it tries to connect to the device using SSHv2.

If the device does not run SSHv2 and runs only SSHv1 then it connects to the device through SSHv1.

If the device runs both SSHv2 and SSHv1, then it connects to the device using SSHv2.

If a problem occurs while connecting to the device using SSHv2, then it does not fall back to SSHv1 for the device that is being accessed.

See the Software Management Functional Supported Device tables on Cisco.com for the devices list that requires Telnet and SSH access.


• Telnet password

  If the Telnet password is configured on your device, you might need this password for basic login access.

  Enter the Telnet password in the Primary Credential Password field in the Add Credential Template dialog box (Inventory > Device Administration > Add / Import / Manage Devices).

• Local user name

  If the device is configured with the local username and password, you must enter this information when you log in. In Telnet mode, for catalyst devices, the local user name is not applicable, so you must leave this field blank. In secure shell (SSH) mode, for catalyst devices, you must enter this information.
Enter the Local User name in the Primary Credential Username field in the Add Credential Template dialog box (Inventory > Device Administration > Add / Import / Manage Devices).

- Local user password
  If the device is configured with the local username and password, you must enter this information when you log in.
  
  If TACACS is configured, the application uses the TACACS information.
  
  If the parent TACACS server is down and the local username and password are present, the application uses this information instead.
  
  Enter the Local user password in the Primary Credential Password field in the Add Credential Template dialog box (Inventory > Device Administration > Add / Import / Manage Devices).

- TACACS username and password
  If the device is configured for TACACS, you must enter the TACACS username and password. The application will try to use this information first for login access.
  
  Enter the TACACS username and password in the Primary Credential Username and Primary Credential Password fields in the Add Credential Template dialog box (Inventory > Device Administration > Add / Import / Manage Devices).

- Enable secret password
  The enable secret password takes precedence over the enable password in Cisco IOS Release 11.x and later. Use this password to make changes when running in regular Cisco IOS mode. If the service password-encryption is enabled, enable secret passwords are more secure than enable passwords.
  
  Enter the Enable password in the Primary Credential Enable Password field in the Add Credential Template dialog box (Inventory > Device Administration > Add / Import / Manage Devices).

- Enable password
  Since some versions of BOOT ROM mode do not recognize the enable secret password or if enable secret is not configured on the device, you must use the enable password to load Flash memory.
  
  Enter the Enable password in the Primary Credential Enable Password field in the Add Credential Template dialog box (Inventory > Device Administration > Add / Import / Manage Devices).

- Enable TACACS
  Sometimes the device is configured for enable TACACS. In this case, you must provide the TACACS user name and password information for enable access.

Note  The TACACS user name and password must be same as the Local user name and password. You cannot configure different user names and passwords for user mode and enable mode for the device.
Some useful URLs on configuring SSHv2 are:

- Configuring Secure Shell on Routers and Switches Running Cisco IOS:
  

- How to Configure SSH on Catalyst Switches Running Catalyst OS:


- Configuring the Secure Shell Daemon Protocol on CSS:


- Configuration Examples and TechNotes:


### Configuring SCP

You can use the SCP protocol to transfer the software images. While using SCP protocol, the LMS server acts like a client and the device acts like a server.

To configure the LMS server as an SCP client, you must enter the SSH credentials. See Configuring Telnet and SSH Access for further details.

For Cisco Catalyst 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches, if you are upgrading the .tar images using SCP protocol, you must configure the SCP username and password.

The minimum supported version of the running image should be 12.2(25) SEC and should have the SCP protocol support.

In this case, LMS server acts like a SCP server and the device acts like a client.
To configure SCP username and password:

**Step 1**
Go to **Admin > System > System Preferences**.
The System Preferences dialog box appears.

**Step 2**
Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP User</td>
<td>Enter the user name.</td>
</tr>
<tr>
<td></td>
<td>For Solaris and Soft Appliance:</td>
</tr>
<tr>
<td></td>
<td>• You must specify a user name that has SSH authorization. SCP uses this authorization for transferring the images.</td>
</tr>
<tr>
<td></td>
<td>For Windows:</td>
</tr>
<tr>
<td></td>
<td>• The username you have entered here is taken for transferring images using SCP protocol.</td>
</tr>
<tr>
<td>SCP Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td></td>
<td>For Solaris and Soft Appliance:</td>
</tr>
<tr>
<td></td>
<td>• You must specify a password that has SSH authentication. SCP uses this authentication for transferring the images.</td>
</tr>
<tr>
<td></td>
<td>For Windows:</td>
</tr>
<tr>
<td></td>
<td>• The password you have entered here is used for authentication while transferring images using SCP protocol.</td>
</tr>
<tr>
<td>SCP Verify Password</td>
<td>Re-enter the password to verify.</td>
</tr>
</tbody>
</table>

**Step 3**
Click **Apply** after making the changes.

**Step 4**
To cancel the changes, click **Cancel**.

**Configuring RCP**

You can use the RCP protocol to transfer the software images. The LMS server acts like a RCP server and the device acts like a client.

Configuring RCP involves the following:

- Configuring RCP on Solaris and Soft Appliance
- Configuring RCP on Windows
- Selecting RCP as the Active File Transfer Method on Solaris and Soft Appliance and Windows
- Configuring Cisco IOS Software Devices to Allow RCP Transactions

**Configuring RCP on Solaris and Soft Appliance**

Configuring RCP on Solaris and Soft Appliance, involves the following:

- Creating the RCP Remote User Account
- Enabling the RCP Daemon
Creating the RCP Remote User Account

To use RCP, you must create a user account on the system to act as the remote user to authenticate the RCP commands issued by devices. This user account must own an empty .rhosts file in its home directory to which the user, casuser has write access.

You can choose the name of this user account because you can configure the LMS server to use any user account.

The default user account name is `cwuser`. The examples in this procedure use the default name `cwuser`. If you choose to use a different name, substitute that name for `cwuser`.

To create and configure the RCP remote user account, follow these steps while logged in as root:

---

**Step 1** To add a user account named `cwuser` to the system, enter:

```
# useradd -m -c "user account to authenticate remote copy operations" cwuser
```

**Step 2** Navigate to the `cwuser` home directory.

**Step 3** Create the .rhosts file, by entering:

```
# touch .rhosts
```

**Step 4** Change the owner of the .rhosts file, by entering:

```
# chown cwuser:casusers .rhosts
```

**Step 5** Change the permissions of the .rhosts file, by entering:

```
# chmod 0664 .rhosts
```

If you did not use the default user name `cwuser`, use the user account that you created as the RCP remote user account.

a. Login to the server as `admin`.

b. Select **Admin > System > System Preferences**.

   The View / Edit System Preferences dialog box appears.

c. Enter the name of the user account that you created in the RCP User field, then click **Apply**.

---

Enabling the RCP Daemon

To add and configure standard Solaris and Soft Appliance RCP server software:

---

**Step 1** Log in as superuser.

**Step 2** Edit the `/etc/inetd.conf` file using a text editor.

- Look in the file `/etc/inetd.conf` for the line that invokes rshd. If the line begins with a pound sign (#), remove the pound sign with a text editor. Depending on your system, the line that invokes the rshd server might look similar to:

  ```
  shell stream tcp nowait root /usr/sbin/in.rshd in.rshd
  ```

- Save the changes to the edited file and exit the text editor.
Step 3 Go to the UNIX prompt, enter the following to display the process identification number for the *inetd* configuration:

```
# /usr/bin/ps -ef | grep -v grep | grep inetd
```

The system response is similar to:

```
root 119  1  0 12:56:14 ? 0:00 /usr/bin/inetd -s
```

The first number in the output (119) is the process identification number of the *inetd* configuration.

Step 4 Enable your system to read the edited */etc/inetd.conf* file, enter:

```
# kill -HUP 119
```

where 119 is the process identification number identified in Step 3.

Step 5 Verify that rshd is enabled by entering:

```
# netstat -a | grep shell
```

which should return output similar to:

```
*.shell *.* 0 0 0 0 LISTEN
```

---

**Configuring RCP on Windows**

During LMS installation, the RCP server is configured.

**Selecting RCP as the Active File Transfer Method on Solaris and Soft Appliance and Windows**

Step 1 Select Admin > Network > Software Image Management > View/Edit Preferences.
The View/Edit Preferences dialog box appears.

Step 2 Select the Protocol Order.

Step 3 Click Apply.

---

**Configuring Cisco IOS Software Devices to Allow RCP Transactions**

Given here is a basic configuration in a router that can handle RCP transactions from the LMS server.

```
calvi# show running configuration
Building configuration...

Current configuration:
!
version 11.3 service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname calvi
!
boot system c2500-is-1.113-11a.T1.bin 255.255.255.255
enable password 7 1106170043130700
!
username cwuser password 7 000C1C0A05
```
ip rcmd rcp-enable
ip rcmd remote-host cwuser 172.17.246.221 cwuser enable
ip rcmd remote-username cwuser
!
!
process-max-time 200
!
interface Loopback0
  ip address 5.5.5.5 255.255.255.255
  no ip directed-broadcast
!
interface Ethernet0
  description Connection to Backbone
  ip address 172.17.246.4 255.255.255.0
  no ip mroute-cache
!
interface Serial0
  no ip address
  no ip mroute-cache shutdown
  no cdp enable
!
interface Serial1
  no ip address
  no ip mroute-cache shutdown
  no cdp enable
!
interface Async1
  no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.17.246.1
!
logging monitor informational
snmp-server community private RW
snmp-server community public RO
snmp-server enable traps snmp
snmp-server host 172.17.246.117 traps public
!
line con 0
  exec-timeout 0 0
  password 7 0504080A754D4205
  login
line 1 8
  exec-timeout 0 0
Chapter 9      Managing Software Images Using Software Management

Software Distribution

login
transport input all
line aux 0
   password 7 06090124184F0515
login
line vty 0 4
   exec-timeout 0 0
   password 7 06090124184F0515
login
!
end

where:

• username cwuser password 7 000C1C0A05 creates the username cwuser on the router. You must choose a password for this user.

• ip rcmd rcp-enable enables RCP service on the device.

• ip remote-host cwuser 172.17.246.221 cwuser enable The remote system where you install LMS has the IP address 172.17.246.221 and the local definition of the user, cwuser. This command allows cwuser to issue the copy command on the network device.

• ip rcmd remote-username cwuser configures use of the remote user name at the request of a remote copy. At the initiation of the remote copy operation in the network device, for example, in Add Images to Library, the device uses the cwuser name to authenticate against the LMS server.

Configuring TFTP

You can use the Trivial File Transfer Protocol (TFTP) protocol to transfer the software images. The LMS server acts like a TFTP server and the device acts like a client.

Configuring TFTP on Windows

During LMS installation, the tftpboot directory is created under the directory in which LMS is installed (the default is SystemDrive:\Program Files\CSCOPx).

Configuring TFTP on Solaris and Soft Appliance

A file transfer server must be installed on your system. You must enable a TFTP server because it is the default file transfer server type.

During Software Management installation, if the installation tool cannot find a TFTP server, it tries to add one. If the installation tool cannot find or create a TFTP server, you must install and enable the TFTP server. Verify that a /tftpboot directory exists, as explained in the following sections.

• Enabling the TFTP Daemon

• Creating the /tftpboot Directory
**Enabling the TFTP Daemon**

If you are using standard Solaris and Soft Appliance software, you can add and configure the TFTP server (TFTPD).

---

**Step 1** Log in as superuser.

**Step 2** Edit the `/etc/inetd.conf` file using a text editor.

- Look in the file `/etc/inetd.conf` for the line that invokes TFTPD. If the line begins with a pound sign (#), remove the pound sign with your text editor. Depending on your system, the line that invokes the TFTP server might look similar to:
  
  tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot

- Save the changes to the edited file and exit your text editor.

**Step 3** Go to the UNIX prompt, enter the following command to display the process identification number for the inetd configuration:

```bash
# /usr/bin/ps -ef | grep -v grep | grep inetd
```

The system response is similar to:

```
root 119 1 0 12:56:14 ? 0:00 /usr/bin/inetd -s
```

The first number in the output (119) is the process identification number of the inetd configuration.

**Step 4** Enable your system to read the edited `/etc/inetd.conf` file, enter:

```bash
# kill -HUP 119
```

where 119 is the process identification number identified in Step 3.

**Step 5** Verify that TFTP is enabled by entering either:

```bash
# netstat -a
```

or

```bash
# grep tftp
```

which should return output similar to:

```
*tftp Idle
```

or enter:

```bash
# /opt/CSCOpx/bin/mping -s tftp localhost_machine_name
```

which returns the number of modules sent and received, for example:

```
sent:5 recvd:5 ...
```

If the output shows that zero modules were received, TFTP is not enabled. Repeat these steps, beginning with Step 1, to make sure you have enabled TFTP.

---

**Creating the `/tftpboot` Directory**

LMS uses the `/tftpboot` directory when transferring files between the LMS server and network devices. The files are removed after the transfer is complete. However, multiple jobs (for example, image distribution, image import, or config file scan) could be running at the same time.

Each of these jobs requires its own space. Software image sizes, for example, can be up to 20 MB. To ensure that jobs run successfully, make sure there is sufficient space available in the `/tftpboot` directory.
If the /tftpboot directory does not exist on your system, you must create it:

**Step 1** Enter:
```
# mkdir /tftpboot
```

**Step 2** Make sure all users have read, write, and execute permissions to the /tftpboot directory by entering:
```
# chmod 777 /tftpboot
```

The /tftpboot directory now exists and has the correct permissions.

**Configuring HTTP**

No configuration on device is required for this protocol.

**Meeting Microcode and Modem Firmware Requirements**

The following minimum system software versions are required to support microcode and modem firmware upgrades. However, different versions of these image types might require different versions of system software.

Software Management does not check for compatibility and dependence between each microcode version and system software version. It merely warns the user to check this information by consulting a technical representative or the compatibility matrix published on Cisco.com.

**MICA Portware Image Types**

<table>
<thead>
<tr>
<th>Device</th>
<th>Minimum System Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS5200</td>
<td>Cisco IOS version 11.3(2)T</td>
</tr>
<tr>
<td></td>
<td>Bootloader version 11.2(11)P</td>
</tr>
<tr>
<td>AS5300</td>
<td>Cisco IOS version 11.2(9)XA</td>
</tr>
<tr>
<td>3640</td>
<td>Cisco IOS version 11.2(12)P</td>
</tr>
</tbody>
</table>

**Microcom Firmware Image Types**

<table>
<thead>
<tr>
<th>Device</th>
<th>Minimum System Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS5200</td>
<td>Cisco IOS version 11.2(10a)P</td>
</tr>
<tr>
<td></td>
<td>Bootloader version 11.2(11)P</td>
</tr>
<tr>
<td>AS5300</td>
<td>Cisco IOS version 11.1(14)AA</td>
</tr>
</tbody>
</table>

**CIP Microcode Image Types**

Supported for Cisco IOS versions 11.x and later.
Chapter 9     Managing Software Images Using Software Management

Scheduling the Upgrade

Scheduling an upgrade consists of:

• Selecting the devices to upgrade
  Use Software Management's scheduling features to schedule the upgrade for one device or a series
  of devices.

  Software Management downloads images from more than one device in parallel. You must ensure
  that the tftpboot directory (NMSROOT/tftpboot (On Solaris and Soft Appliance), and
  NMSROOT\tftpboot (On Windows)) has enough free space to accommodate at least 20 images.

• Determining any limitations or requirements for the selected devices
  For example, SFB devices have several upgrade requirements and limitations.

• Updating the inventory
  Since Software Management uses the inventory to make image and Flash memory
  recommendations, be sure that your current inventory reflects the correct device information.

  For some devices such as 6400 NRP1, 801, and 802, etc., Software Management contacts devices to
  get the Flash information.

• Configuring file transfer protocol order
  Before scheduling a software upgrade job, set the protocol order for configuration file transfer.

  For fetching configuration from device, the protocol settings of Configuration Management are
  used. Software Management uses the same protocol for fetch and download of configurations. You
  can set the Configuration Management protocol order using Admin > Collection Settings > Config
  > Config Collection Settings.

  For better performance, set tftp as the first protocol.

• Determining the upgrade and execution order
  Based on your network topology and to minimize the impact on your network, you can schedule the
  upgrades job either sequentially or in parallel.

  For example, if devices A, B, and C are networked sequentially, then you must upgrade device C
  first, then device B, then device A. If you upgrade device B first, you might no longer have access
  to device C.

• Determining the upgrade schedule
  For most devices, you can schedule the software to:
  – Distribute the software to the device and reload the device immediately.
  – Distribute the software only. You will perform the reloads manually.

  The following devices are always rebooted immediately after the software is downloaded:
  – Single Flash bank devices
  – FDDI/CDDI, ATM, and Token Ring modules on Catalyst switches

• Checking the Work Order report
  The Work Order report contains such information as the state of the software running on the device
  and the new software, the operations that will be performed during the upgrade procedure, and any
  important notes that you should be aware of before the upgrade begins.
Authorizing a Distribution Job

The Job Approval approval option allows you to require job upgrade approvals before running a scheduled job. It enforces the approval process by sending job requests through e-mail to people on the approver list.

To set up the authorization process:

- Select the appropriate Job Approval options.
- Make sure one or more approver lists exist.
- Make sure the upgrade job identifies an approver list.
- Make sure the approver is a member of that approver list.

See Administration of Cisco Prime LAN Management Solution 4.2 for more details on creating and editing approver lists, assigning approver lists, setting up Job Approval, and approving and rejecting jobs.

Distributing by Devices [Basic]

You can use the Distribute by Devices option to schedule device-centric upgrade jobs.

Software Management recommends any software images available on LMS server and Cisco.com, if this option is selected by you (Admin > Network > Software Image Management > View/Edit Preferences).

To do this, select the devices first and distribute suitable images to them. After the distribution job is complete, you can use the Software Management Job Browser window to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade

**Note** View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

Before You Begin

Before you begin distributing the images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device and also verified whether the necessary software images are present in the software image repository.
  
  You can also download the images from Cisco.com. You must ensure that you have the access to download the images from Cisco.com.
  
- Considered the effect of the upgrade on your network and your network users.
  
- Supplied the information required by Software Management for each device.

To distribute the images by device in Basic mode:

**Step 1** Select Configuration > Tools > Software Image Management > Software Distribution.

The Distribution Method dialog box appears.

**Step 2** Select By device [Basic] and click Go. The Select Devices dialog box appears.
Step 3  Select the devices, then click Next.

The Cisco.com and Proxy Server Credential Profile dialog box appears.

a. Enter your Cisco.com username and password.

   If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.

   You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:

   **Admin > System > Cisco.com Settings > Proxy Server Setup**

   • Click OK after entering the credential information.

   The software management analyzes the required images that are available in your software repository and on Cisco.com. It then recommends the appropriate image for distribution.

   See **Understanding Upgrade Recommendations** for details on how Software Management recommends image for various Cisco device types.

   The Distribute By Devices dialog box appears with the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td>Name of the device.</td>
</tr>
<tr>
<td></td>
<td>Click on the device name to launch the Troubleshooting page.</td>
</tr>
<tr>
<td>Module Information</td>
<td>Image type, chassis model, and software version on device.</td>
</tr>
<tr>
<td>Image Options</td>
<td>Details of the recommended image.</td>
</tr>
<tr>
<td>Storage Options</td>
<td>Details of recommended image storage information.</td>
</tr>
<tr>
<td>Errors</td>
<td>Click on the underlined Error message to review the details.</td>
</tr>
</tbody>
</table>

**Notation Descriptions**

• An asterisk (*) at the beginning of the field indicates the recommended image or partition by Software Management. If there is no asterisk at the beginning of the field, it indicates that an appropriate image or partition could not be found but the displayed selections might work.

• A `^` means that the image resides in Cisco.com but not in your software image repository. When you select an image in Cisco.com to distribute to a network device, the image is first added to the image repository, then downloaded to the device.

• A superscript ‘1’ refers to read-only Flash memory.

• A superscript ‘2’ refers to the Flash partition that holds the running image when a device is running from Flash (RFF).

Step 4  Select the devices to which you want to distribute images and click Next.

The Distribute By Devices window appears with these details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device</td>
</tr>
<tr>
<td>Selected Module</td>
<td>Module information that you have selected.</td>
</tr>
<tr>
<td>Selected Image</td>
<td>Image information that you have selected.</td>
</tr>
</tbody>
</table>
### Step 5

Click **Next**.

The Job Schedule and Options dialog box appears.

### Step 6

Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>You can specify when you want to run the Image Distribution (by device [Basic]) job.</td>
</tr>
<tr>
<td></td>
<td>To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs this job immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs this job once at the specified date and time.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the date and time (hours and minutes) to schedule the job.</td>
</tr>
<tr>
<td>Job Info</td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job.</td>
</tr>
<tr>
<td></td>
<td>You can enter multiple e-mail addresses separated by commas.</td>
</tr>
<tr>
<td></td>
<td>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences).</td>
</tr>
<tr>
<td></td>
<td>We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter additional information about this job.</td>
</tr>
<tr>
<td>Maker E-Mail</td>
<td>Enter the e-mail ID of the job creator. This is a mandatory field.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed only if you have enabled Job Approval for Software Management.</td>
</tr>
<tr>
<td>Maker Comments</td>
<td>Enter comments for the job approver.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed only if you have enabled Job Approval for Software Management.</td>
</tr>
<tr>
<td>Job Options</td>
<td></td>
</tr>
<tr>
<td>Reboot immediately after download</td>
<td>Choose not to reboot (and reboot manually later) or to reboot immediately after download.</td>
</tr>
<tr>
<td></td>
<td>You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option.</td>
</tr>
<tr>
<td></td>
<td>Note the following about this option:</td>
</tr>
<tr>
<td></td>
<td>• Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately.</td>
</tr>
<tr>
<td></td>
<td>• Line cards reboot automatically.</td>
</tr>
<tr>
<td></td>
<td>• Does not apply to PIX devices managed through Auto Update Server (AUS).</td>
</tr>
</tbody>
</table>
Software Distribution

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform distribution in Non-Installed mode</td>
<td>This option is available only if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.</td>
</tr>
<tr>
<td>Do not insert new boot commands into configuration file</td>
<td>Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.</td>
</tr>
</tbody>
</table>
| Use current running image as tftp fallback image | If the running image is in the repository, select this option to place a copy in the TFTP server directory. Uses this copy of image if reboot with new image fails. Note the following about this option:  
  • Option is subject to your platform restrictions to boot over connection to server. Check your platform documentation.  
  • Backup image is not deleted after upgrade. It remains in TFTP server directory so that the device can find it any time it reboots |
| Backup current running image                   | Select to back up the running image in software image repository before upgrading. Line cards do not support upload.                                                                                                               |
| On error, halt processing of subsequent devices | Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do not select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details. |
| Enable Job Password                             | Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices) are ignored. |
| Execution                                       | Select the job execution order for the devices. This can be either Parallel or Sequential:  
  • Sequential—Job runs on the devices, sequentially. You can define this sequence.  
  • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential:  
    1. Click **Execution Order**. The Execution Order dialog box appears.  
    2. Use the Up and Down arrows to order your device list.  
    3. Click **Done**. |
Chapter 9      Managing Software Images Using Software Management

Step 7  Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verification warnings generated during image distribution (if applicable).

Step 8  Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

---

### Distributing by Devices [Advanced]

You can use the Distribute by Devices option to schedule device-centric upgrade jobs.

The selected image and storage media is validated and verified for dependencies and requirements based on the device information that you have provided at the time of adding devices to the Device and Credential Repository and the device data that is collected by the inventory.

The images that you want to distribute must be available in the Software repository.

You can use this method to upgrade the System software on all Software Management supported devices.

You can also upgrade module software on those modules which have a management IP address.

The modules/interfaces that do not have a management IP address cannot be upgraded using this method.
Chapter 9  Managing Software Images Using Software Management

Software Distribution

The input file that contains the details of the device and image must be available at this location:

On Solaris and Soft Appliance:
/var/adm/CSCOpx/files/rme/swim/advdistinput

On Windows:
NMSROOT\files\rme\swim\advdistinput

Where NMSROOT is the LMS installed directory.

After the distribution job is complete, you can use the Software Management Job Browser window to:

• Undo an upgrade and roll back to the previous image
• Retry devices that failed a previous upgrade

Note  View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

Before You Begin

Before you begin distributing the images, you should have:

• Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device. You should have verified whether the necessary software images are present in the image repository.
• Considered the effect of the upgrade on your network and your network users.
• Supplied the information required by Software Management for each device.

To distribute the images by device in Advance mode:

Step 1  Select Configuration > Tools > Software Image Management > Software Distribution. The Distribution Method dialog box appears.

Step 2  Select By device [Advanced], then click Go. The Expert Distribution dialog box appears.

Step 3  Click Browse. The Server Side File Browser dialog box appears.

Step 4  Select the file and click OK.
The input file that contains the details must be available at this location:
On Solaris and Soft Appliance:
/var/adm/CSCOpx/files/rme/swim/advdistinput
On Windows:
NMSROOT\files\rme\swim\advdistinput
Where NMSROOT is the LMS installed directory.
The selected file must contain the information in CSV format and all the fields are mandatory:
device-display-name,image-in-repository,storagedestination,moduleidentifier
• device-display-name—Name of the device as entered in Device and Credential Repository.
• image-in-repository—Image name as in the software image repository.
• `storagedestination`—Image storage destination
• `moduleidentifier`—Module identifier number. This is applicable only for Catalyst devices. For other devices, you must enter 0.

You can identify the device module number using Inventory Detailed Device Report (Reports > Inventory > Detailed Device). In the Detailed Device Report, the Slot Number column in the Module Information table provides you the Module Identifier Number.

For example, for a Cisco Router:

```
Rtr1750,c1700-sy56i-mz.121-24.bin,flash:1,0
```

For a Cisco Catalyst device:

```
cat5500-10.100.38.17,cat5000-supg.6-4-10.bin,bootflash:,1
```

**Step 5**
Do either of the following:

• Check the Skip Verification checkbox if you want to postpone the verification to the job execution stage.

  If you have checked the Skip Verification checkbox, go to **Step 7**.

Or

• Click **Verify** if you want the verification to take place during the job scheduling stage itself.

  If you have clicked **Verify**, go to **Step 6**.

**Step 6**
When you click Verify, the Expert Distribution window is updated with the following device details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device as specified in the input file.</td>
</tr>
<tr>
<td>Image</td>
<td>Name of the image as specified in the input file.</td>
</tr>
<tr>
<td>Storage Destination</td>
<td>Image storage information as specified in the input file.</td>
</tr>
<tr>
<td>Module Number</td>
<td>Module identifier number as specified in the input file.</td>
</tr>
<tr>
<td>Result</td>
<td>Click on the link to review the details.</td>
</tr>
</tbody>
</table>

**Step 7**
Click **Next**.
The Job Schedule and Options dialog box appears.

**Step 8**
Enter the following information in the Job Schedule and Options dialog box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td>You can specify when you want to run the Image Distribution (by device [Advanced]) job.</td>
</tr>
<tr>
<td>Run Type</td>
<td>To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs this job immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs this job once at the specified date and time.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the date and time (hours and minutes) to schedule the job.</td>
</tr>
</tbody>
</table>
## Software Distribution

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job Info</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Job Description</strong></td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td><strong>E-mail</strong></td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender’s address.</td>
</tr>
<tr>
<td><strong>Comments</strong></td>
<td>Enter additional information about this job.</td>
</tr>
<tr>
<td><strong>Maker E-Mail</strong></td>
<td>Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.</td>
</tr>
<tr>
<td><strong>Maker Comments</strong></td>
<td>Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.</td>
</tr>
<tr>
<td><strong>Job Options</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Reboot immediately after download** | Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option:
  • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately.
  • Applies to Supervisor Engine I, II, and III only. Line cards reboot automatically.
  • Does not apply to PIX devices managed through Auto Update Server (AUS). |
| **Perform distribution in Non-Installed mode** | This option is available only if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode. |
| **Do not insert new boot commands into configuration file** | Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Note the following about this option:
  • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
  • Applies to Supervisor Engine III only. |
| **Use current running image as tftp fallback image** | If the running image is in the repository, select this option to place a copy in the TFTP server directory. Uses this copy of image if reboot with new image fails. Note the following about this option:
  • Applies to Supervisor Engine I, II, and III only.
  • Option is subject to your platform restrictions to boot over connection to server. Check your platform documentation.
  • Backup image is not deleted after upgrade. It remains in TFTP server directory so that the device can find it any time it reboots. |
Step 9  Click Next after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
Software Distribution

• Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
• Verification warnings generated during image distribution (if applicable).

Step 10 Click Finish.
The notification window appears with the Job ID.
To check the status of your scheduled job, select Configuration > Tools > Software Image Management > Jobs.

Distributing by Images

You can use the Distribute by Images option to schedule image-centric upgrade jobs. To do this, you must first select an image and then distribute it to applicable devices.

After the distribution job is complete, you can use the Job Details report to:
• Undo an upgrade and roll back to the previous image
• Retry devices that failed a previous upgrade

Note View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

You cannot use this procedure to upgrade:
• MICA portware
• Microcom firmware
• CIP microcode
• Bootloader for IOS
• Catalyst modules other than the Supervisor module

Before You Begin

Before you begin distributing the images, you should have:
• Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device. You should have verified whether the necessary software images are in the image repository.
  See Planning the Upgrade for further details.
• Considered the effect of the upgrade on your network and your network users.
  See Scheduling the Upgrade for further details.
• Supplied the information required by Software Management for each device.
  See Configuring Devices for Upgrades for further details.
To distribute images by image:

**Step 1** Select **Configuration > Tools > Software Image Management > Software Distribution**.
The Distribution Method dialog box appears.

**Step 2** Select **By image**, then click **Go**.
The Select Image And Devices dialog box appears.

**Step 3** Select:
- a. An image from the software image repository.
- b. Devices that need upgrading

**Step 4** Click **Next**.
The Device Recommendation dialog box appears with the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td>Name of the device. Click on the device name to launch the Troubleshooting page.</td>
</tr>
<tr>
<td>Module Information</td>
<td>Image type, chassis model, and software version on device.</td>
</tr>
<tr>
<td>Recommended Storage</td>
<td>Details of recommended image storage information.</td>
</tr>
<tr>
<td>Error</td>
<td>Click on the link to review the details.</td>
</tr>
</tbody>
</table>

**Notation Descriptions**
- An asterisk (*) at the beginning of the field indicates the recommended partition by Software Management. If there is no asterisk at the beginning of the field indicates, an appropriate partition could not be found but the displayed selections might work.
- A superscript ‘1’ refers to read-only Flash memory.

**Step 5** Select the devices you want to upgrade, then click **Next**.
The Image Centric Distribution Verification window appears. This window displays the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device</td>
</tr>
<tr>
<td>Selected Module</td>
<td>Module information that you have selected.</td>
</tr>
<tr>
<td>Selected Slot</td>
<td>Image storage information that you have selected.</td>
</tr>
<tr>
<td>Verification Result</td>
<td>Click on the link to review the details.</td>
</tr>
</tbody>
</table>

Software management recommends the Flash partition with the maximum free space in each device. You can override the recommendation and select another partition from the drop-down box.

**Step 6** Click **Next**.
The Job Schedule and Options dialog box appears.
Step 7  Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
</tbody>
</table>
| Run Type | You can specify when you want to run the Image Distribution (by image) job. To do this, select one of these options from the drop-down menu:  
  • Immediate—Runs this job immediately.  
  • Once—Runs this job once at the specified date and time. |
| Date | Select the date and time (hours and minutes) to schedule the job. |
### Field | Description
---|---
**Job Info**  
Job Description | Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.  
E-mail | Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.  
Comments | Enter additional information about this job.  
Maker E-Mail | Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.  
Maker Comments | Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.  
**Job Options**  
Reboot immediately after download | Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option:  
• Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately.  
• Line cards reboot automatically.  
• Does not apply to PIX devices managed through Auto Update Server (AUS).  
Perform distribution in Non-Installed mode | This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.  
Do not insert new boot commands into configuration file | Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.  
Use current running image as tftp fallback image | If running image is in repository, select option to place a copy in the TFTP server directory. Uses this copy if reboot with new image fails. Note the following:  
• This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation.  
• Backup image is not deleted after upgrade. It remains in TFTP server directory so that device can find it any time it reboots  
Back up current running image | Select to back up running image in software image repository before upgrading. Line cards do not support upload.
Chapter 9  Managing Software Images Using Software Management

### Software Distribution

#### Step 8
Click Next after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:
- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| On error, halt processing of subsequent devices | Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device.  
For sequential execution, if you do not select this option, upgrade for next device begins.  
For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed.  
See the Job Summary page for details. |
| Enable Job Password | Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution.  
The credentials that you enter here are used for this particular Software Management job.  
The credentials that you have entered in the Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices) are ignored. |
| Execution | Select the job execution order for the devices. This can be either Parallel or Sequential:  
- Sequential—Job runs on the devices, sequentially. You can define this sequence.  
- Parallel—Job runs on a batch of 15 devices at the same time.  
If you have selected Sequential:  
1. Click Execution Order.  
   The Execution Order dialog box appears.  
2. Use the Up and Down arrows to order your the device list.  
3. Click Done. |
| Reboot | Select the reboot order for the devices. This can be either Parallel or Sequential.  
If you have selected Sequential:  
1. Click Boot Order.  
   The Boot Order dialog box appears.  
2. Use the Up and Down arrows to order your devices list.  
3. Click Done. |
• Whether the bootloader will be upgraded. (For a bootloader upgrade.)
• Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
• Verification warnings generated during image distribution (if applicable).

Step 9  Click Finish.
The notification window appears with the Job ID.
To check the status of your job, select Configuration > Tools > Software Image Management > Jobs.

Support for IOS Software Modularity

Software Management provides support for Cisco IOS Software Modularity Images. The Cisco IOS Software Modularity Images combine subsystems into individual processes and enhances the memory architecture in order to provide the process level fault isolation and subsystem In-Service Software Upgrade (ISSU) capability.

Traditionally, IOS Software images are distributed by:
• Copying the image to disk.
• Updating boot commands and rebooted.

The IOS Software Modularity images can be run in this mode as well. This is called Cisco IOS Software Modular non-install mode (also known as binary mode).

Software Management supports distribution of Patches and Maintenance Packs. This distribution is accomplished by the use of Cisco IOS Software Modularity Images. Software Modularity enhances the IOS infrastructure to allow selective system maintenance through individual patch upgrades. See Patch Distribution for more details.

Patches
A patch is a single fix that may affect one or more subsystems. Patches can only be installed to a search root, where a base image exists. Patches are released for a particular base image version and device platform.

Maintenance Pack
A Maintenance Pack includes one or more patches. This pack is applied like a Patch. Maintenance Packs are released for a particular base image version and device platform.

Note
Software Management does not support downloading Patches/Maintenance Packs from Cisco.com. The reason is that these images are available in an external URL. You have to manually download patches from the external URL and add the same to Software Repository.
Modes of Distribution

There are two modes of distribution of Software Modularity images to devices:

- **Non Installed Mode**
  
  This process involves the distribution of images by copying of the IOS Software Modularity images to the hard disk of the device, updating the boot commands and rebooting the OS on the device. You can run the Cisco IOS Software Modularity Images in this mode and so it is also called IOS Software Modularity non-install mode. It is also known as binary mode.

- **Installed Mode**
  
  According to this mode the IOS Software Modularity image is extracted/uncompressed to a compact Flash with a well defined directory structure. The installed mode provides the advantage of accommodating the point fix capabilities of Software Modularity.

**Note**

Software Management checks the current image on the device and recommends a suitable image and the appropriate image storage for distribution. Software Management only recommends Maintenance Pack Images for devices. It does not recommend patches for devices.

Cisco IOS Software Modularity base images support:

- Import of Image from Cisco.com
- Import of Image from device
- Import of Image from File System
- Import of Image from Network
- Cisco.com Upgrade Analysis
- Distribution of Images
- Software Repository Synchronization

Support for Import of Image from device, Import of Image from Network and Software Repository Synchronization is applicable only for devices running IOS Software Modularity images in non-installed mode.

The population of Flash files on Cisco-Flash-MIB is not done on the devices running IOS Software Modularity image versions 12.2(18)SXF4 and 12.2(18)SXF5 and so these image versions are not supported by Software Management. The minimum IOS Software Modularity image version supported by Software Management is 12.2(18)SXF6.
Patch Distribution

You can distribute patches simultaneously to applicable devices. Patch distribution does not require reboot of the entire OS on a device. You can install a patches only to a search root where a base image exists. Patches, once installed, must be activated to come to effect on the running system.

Note

You can apply Patches or Maintenance Packs to a device only if the device is running IOS Software Modularity Images in installed mode.

Software Management verifies:

- Patches against the base image and device platform to ensure compatibility. If the patches are incompatible then those patches are rejected.
- Whether the target patch already exists on the device.

Patch Distribution Methods

You can distribute patch images to the devices in your network, using any of these methods:

- Distribute by Devices
  
  This method enables you to select devices and perform patch upgrades to those devices. 
  
  See Patch Distribution - by Devices.

- Distribute by Patch
  
  This method enables you to select a patch image from the Software Repository and use it to perform a patch upgrade on suitable devices in your network. This option is useful when you have to distribute the same patch image to multiple devices. 
  
  See Patch Distribution - by Patch.

Patch Distribution - by Devices

You can use the Distribute by Devices option to schedule device-centric patch upgrade jobs.

Software Management recommends any Maintenance Pack software images available in the Repository.

Note

Currently Software Management does not support importing of patch images from Cisco.com. You need to import patch images into local filesystem and then import into repository by using Import from file system. See Adding Images to the Software Repository From a File System for more details.

Before You Begin

Before you begin distributing the patch images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device and also verified whether the necessary software images are present in the software image repository.
- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.
To distribute the patch images by device:

**Step 1** Select **Configuration > Tools > Software Image Management > Patch Distribution**.
The Patch Distribution Method dialog box appears.

**Step 2** Select **By devices** and click **Proceed**.
The Patch Distribute by Devices dialog box appears. The Device Selector lists all the available devices.

**Step 3** Select the devices, then click **Next**.
If any of the selected device is not in install mode, an error message is displayed:

- **Device is not in installed mode or not patchable**
- Unselect the device that is not in installed mode and continue.

The software management analyzes the required patch images that are available in your software repository and lists the applicable patch images for each device selected. You can select one or more required patches from the list for each device by using the Ctrl key.

You should select at least one patch for each selected device. If you do not select a patch for a device, an error message is displayed:

- **You should select at least one patch image for each selected device.**

Ensure that you select at least one patch for each selected device and continue.

The Patch Distribute By Devices dialog box appears with the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Module Information</td>
<td>Patch type, chassis model, and software version on device.</td>
</tr>
<tr>
<td>Patches Options</td>
<td>Details of the patch.</td>
</tr>
<tr>
<td>Storage Location</td>
<td>Details of the storage location of the selected patch image.</td>
</tr>
<tr>
<td>Errors</td>
<td>Click on the underlined Error message to review the details.</td>
</tr>
</tbody>
</table>

**Step 4** Select the devices as well as the patch images you wish to distribute to the selected devices and click **Next**.
The Patch Distribute By Devices window appears with these details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device</td>
</tr>
<tr>
<td>Selected Module</td>
<td>Module information that you have selected.</td>
</tr>
<tr>
<td>Selected Patch</td>
<td>Patch information that you have selected.</td>
</tr>
<tr>
<td>Selected Slot</td>
<td>Image storage information from where the current base image is running.</td>
</tr>
<tr>
<td>Verification Result</td>
<td>Click on the link to review the details.</td>
</tr>
</tbody>
</table>

**Step 5** Click **Next**. The Job Schedule and Options dialog box appears.
Step 6 Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td>You can specify when you want to run the Patch Distribution (by device [Basic]) job. To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td>Run Type</td>
<td>• Immediate—Runs this job immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs this job once at the specified date and time.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the date and time (hours and minutes) to schedule the job.</td>
</tr>
</tbody>
</table>
## Software Distribution

### Job Info

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Description</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter additional information about this job.</td>
</tr>
</tbody>
</table>

### Job Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate Patches</td>
<td>Select if you want to activate the patches immediately after download.</td>
</tr>
<tr>
<td>Reboot if it needs</td>
<td>Select if the patch activation requires a reboot. Unselect if the patch activation does not require a reboot.</td>
</tr>
<tr>
<td>On error, stop</td>
<td>Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do not select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.</td>
</tr>
<tr>
<td>processing subsequent</td>
<td></td>
</tr>
<tr>
<td>devices</td>
<td></td>
</tr>
<tr>
<td>Enable Job Password</td>
<td>This option is checked, when the user name, password and enable password are provided for the job.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the username for the distribution job. The credentials that you enter here are used for this particular Software Management job.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the distribution job. The credentials that you enter here are used for this particular Software Management job.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Re-enter the password for confirmation purpose.</td>
</tr>
<tr>
<td>Execution</td>
<td>Select the job execution order for the devices. This can be either Parallel or Sequential:</td>
</tr>
<tr>
<td></td>
<td>• Sequential—Job runs on the devices, sequentially. You can define this sequence.</td>
</tr>
<tr>
<td></td>
<td>• Parallel—Job runs on a batch of 15 devices at the same time.</td>
</tr>
<tr>
<td></td>
<td>If you have selected Sequential:</td>
</tr>
<tr>
<td></td>
<td>1. Click Execution Order.</td>
</tr>
<tr>
<td></td>
<td>The Execution Order dialog box appears.</td>
</tr>
<tr>
<td></td>
<td>2. Use the Up and Down arrows to order your the device list.</td>
</tr>
<tr>
<td></td>
<td>3. Click Done.</td>
</tr>
</tbody>
</table>
Step 7  Click Next after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Patches selected for the upgrade.
- Job Approval information.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verify warnings generated during patch distribution (if applicable).

Step 8  Click Finish.

The notification window appears with the Job ID.

To check the status of your scheduled job, select Configuration > Tools > Software Image Management > Jobs.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot</td>
<td>Select the reboot order for the devices. This can be either Parallel or Sequential.</td>
</tr>
<tr>
<td></td>
<td>If you have selected Sequential:</td>
</tr>
<tr>
<td></td>
<td>1. Click Boot Order.</td>
</tr>
<tr>
<td></td>
<td>The Boot Order dialog box appears.</td>
</tr>
<tr>
<td></td>
<td>2. Use the Up and Down arrows to order your devices list.</td>
</tr>
<tr>
<td></td>
<td>3. Click Done.</td>
</tr>
</tbody>
</table>

**Patch Distribution - by Patch**

You can use the Distribute by Patch option to schedule patch upgrade jobs.

**Note**  Currently Software Management does not support importing of patch images from Cisco.com. You need to import patch images into local filesystem and then import into repository by using Import from file system. See Adding Images to the Software Repository From a File System for more details.
Before You Begin

Before you begin distributing the patch images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device and also verified whether the necessary software images are present in the software image repository.
- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the patch images by device:

Step 1 Select **Configuration > Tools > Software Image Management > Patch Distribution**.

The Patch Distribution Method dialog box appears.

Step 2 Select **By Patch** and click **Proceed**.

The Distribute by Patch dialog box appears.

Step 3 Select a patch from the Image Selection pane and devices from the Device Selection pane, and click **Next**.

The Distribute By Patch - Recommendations dialog box appears with the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td>Name of the device.</td>
</tr>
<tr>
<td></td>
<td>Click on the device name to launch the Troubleshooting page.</td>
</tr>
<tr>
<td>Module Information</td>
<td>Image type, chassis model, and software version on device.</td>
</tr>
<tr>
<td>Storage Options</td>
<td>Details of the storage location of the selected patch image.</td>
</tr>
<tr>
<td>Errors</td>
<td>Click on the underlined Error message to review the details.</td>
</tr>
</tbody>
</table>

Step 4 Select the devices as well as the patch images you wish to distribute to the selected devices and click **Next**.

The Distribute By Patch - Verification window appears with these details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device</td>
</tr>
<tr>
<td>Selected Module</td>
<td>Module information that you have selected.</td>
</tr>
<tr>
<td>Selected Slot</td>
<td>Image storage information from where the current base image is running.</td>
</tr>
<tr>
<td>Verification Result</td>
<td>Click on the link to review the details.</td>
</tr>
</tbody>
</table>

Step 5 Click **Next**.

The Job Schedule and Options dialog box appears.
**Step 6** Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td>You can specify when you want to run the Patch Distribution (by device [Basic]) job. To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td>Run Type</td>
<td>• Immediate—Runs this job immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs this job once at the specified date and time.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the date and time (hours and minutes) to schedule the job.</td>
</tr>
<tr>
<td><strong>Job Info</strong></td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job.</td>
</tr>
<tr>
<td>E-mail</td>
<td>You can enter multiple e-mail addresses separated by commas.</td>
</tr>
<tr>
<td></td>
<td>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences).</td>
</tr>
<tr>
<td></td>
<td>We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter the additional information about this job.</td>
</tr>
<tr>
<td><strong>Job Options</strong></td>
<td>Select if you want to activate the patches immediately after download.</td>
</tr>
<tr>
<td>Activate Patches</td>
<td>Select if the patch activation requires a reboot. Unselect if the patch activation does not require a reboot.</td>
</tr>
<tr>
<td>Reboot if it needs</td>
<td>Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device.</td>
</tr>
<tr>
<td>On error, stop</td>
<td>For sequential execution, if you do not select this option, upgrade for the next device begins.</td>
</tr>
<tr>
<td>processing subsequent</td>
<td>For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed.</td>
</tr>
<tr>
<td>devices</td>
<td>See the Job Summary page for details.</td>
</tr>
<tr>
<td>Enable Job Password</td>
<td>This option is checked, when the user name, password and enable password are provided for the job.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the username for the distribution job. The credentials that you enter here are used for this particular Software Management job.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the distribution job. The credentials that you enter here are used for this particular Software Management job.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Re-enter the password for confirmation purpose.</td>
</tr>
</tbody>
</table>
Step 7  Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Patches selected for the upgrade.
- Job Approval information.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verify warnings generated during patch distribution (if applicable).

**Step 8**  Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.
Remote Staging and Distribution

The Remote Staging and Distribution option helps you to upgrade multiple devices over a WAN. You can perform remote staging and distribution by any one of the methods:

- External FTP server
- External TFTP server
- Remote Staging Device

In this workflow, a managed device or external TFTP server or FTP server is used to stage an image temporarily. The staged image is then used to upgrade devices that are connected by LAN to the Remote Stage device or external TFTP server or FTP server. If you use this method, you do not have to copy a similar image, multiple times across the WAN.

After the image distribution job is completed using a managed device as a remote stage device, the configuration changes made to the Remote Stage device are automatically reversed and the staged image is deleted from the Remote Stage device.

After the distribution job is complete, you can use the Software Image Management Job Browser to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade

This section contains:

- Using External FTP Server
- Using External TFTP Server
- Using Remote Stage Device

**Note**

View Permission Report ([Reports > System > Users > Permission](#)) to check if you have the required privileges to perform this task.

**Supported Remote Stage Devices**

The device that is used as the Remote Stage must have enough free Flash space to copy the selected image.

See the Supported Image Distribution Features for Software Management table on Cisco.com for Remote Staging devices list.

**Before You Begin**

Before you begin distributing the images, you should:

- Prepare for this upgrade. You should have met all of the prerequisites for loading the software on the device or external TFTP server or FTP server. You should also verified whether the necessary software images are in the image repository.
- Manually copy the software image to the External TFTP server or FTP server. This is if you are using the External TFTP/FTP server as the Staging Server.
- Consider the effect of the upgrade on your network and your network users.
- Supply the necessary information required by Software Management for each device.
- Decide on the device or external TFTP server or FTP server that you will use as the Remote Stage device or server.
• Ensure that the Telnet or SSH protocols are functioning properly if you are planning to distribute the images to devices using a External FTP server. The connection protocol for running FTP commands on the device can be either Telnet or SSH.

Note
For the devices that supports remote staging using external FTP Server, see Supported Devices for FTP.

To distribute images using Remote Staging:

Step 1
Select Configuration > Tools > Software Image Management > Software Distribution.
The Distribution Method dialog box appears.

Step 2
Select Use remote staging and click Go.
The Remote Staging and Distribution dialog box appears.

Step 3
Select any of the following:
• Using External FTP Server to use an external FTP server as the staging server.
  For more information, see Using External FTP Server.
• Using External TFTP Server to use an external TFTP server as the staging server.
  For more information, see Using External TFTP Server.
• Using Remote Stage Device to use a device as the remote staging device.
  For more information, see Using Remote Stage Device.

Using External FTP Server

LMS Software Management uses the External FTP server option to upgrade software images in one or more devices. When you select this option, you must enter the FTP credentials and image location.

The FTP copy command is arrived at based on the FTP credentials that you enter. Software Management uses Telnet or SSH protocol to connect to the devices and deploy the FTP copy command. This command gets the software images from the specified location in the FTP server.

Only WLSE and NAM devices support image distribution using External FTP server.

If you have selected Using External FTP server option:

Step 1
Enter the following FTP credentials in their applicable text boxes:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP Server Name</td>
<td>Name of the FTP server</td>
</tr>
<tr>
<td>FTP User Name</td>
<td>FTP Username to access the External FTP server.</td>
</tr>
<tr>
<td>FTP Password</td>
<td>FTP Password to access the External FTP server.</td>
</tr>
<tr>
<td>Image Location</td>
<td>Location of the image in the FTP server directory. These images will be used by Software Management to upgrade the software images on the selected devices.</td>
</tr>
</tbody>
</table>
Software Management will validate the FTP credentials and image location only while the job is running; not while the job is being scheduled.

If you have selected Using External TFTP server option, proceed to the TFTP Wizard.

Step 2 Click Next.
The Remote Staging and Distribution dialog box appears.

Step 3 Select:
- An image from the Image Selection pane.
- Click on Select Applicable Devices button to automatically select the applicable devices
  Or
  Manually select the devices that need an upgrade from the Devices to be Upgraded pane.

For more information on the unsupported images for Remote Staging and Distribution, see Unsupported Software Images.

Step 4 Click Next.
If you have selected Using External TFTP server option, proceed to the TFTP Wizard.
The External FTP Server Details dialog box appears with the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP Address of the External FTP server.</td>
</tr>
<tr>
<td>Selected Image</td>
<td>Image name that you have selected for distribution.</td>
</tr>
<tr>
<td>Errors</td>
<td>Error information.</td>
</tr>
</tbody>
</table>

Step 5 Click Next.
If you have selected Using External TFTP server option, proceed to the TFTP Wizard.
The Device Recommendation dialog box appears with the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Information | Name of the device.  
  Click on the device name to launch the Troubleshooting page. |
| Module Information | Image type, chassis model, and software version on device. |
| Storage Options  | Details of recommended image storage information.  |
| Errors          | Error information.                                 |

Step 6 Click Next.
If you have selected Using External TFTP server option, proceed to the TFTP Wizard.
The Remote Devices Verification dialog box appears with the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device</td>
</tr>
<tr>
<td>Selected Module</td>
<td>Module information that you have selected.</td>
</tr>
</tbody>
</table>
Step 7  Click **Next**. The Job Schedule and Options dialog box appears.

Step 8  Enter the following information. If you have selected Using External TFTP server option, proceed to the **TFTP Wizard**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Selected Slot</strong></td>
<td>Image storage information that you have selected.</td>
</tr>
<tr>
<td><strong>Verification Result</strong></td>
<td>Click on the link to review the details.</td>
</tr>
</tbody>
</table>

**Field**

**Description**

Run Type

You can specify when you want to run the Image Distribution (using remote staging) job.

To do this, select one of these options from the drop-down menu:
- **Immediate**—Runs this job immediately.
- **Once**—Runs this job once at the specified date and time.

Date

Select the date and time (hours and minutes) to schedule.

Job Info

Job Description

Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.

E-mail

Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas.

Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences).

We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.

Comments

Enter the additional information about this job.

Maker E-Mail

Enter the e-mail ID of the job creator. This is a mandatory field.

This field is displayed only if you have enabled Job Approval for Software Management.

Maker Comments

Enter comments for the job approver.

This field is displayed only if you have enabled Job Approval for Software Management.

Job Options

Reboot immediately after download

Choose not to reboot (and reboot manually later) or to reboot immediately after download.

You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option.

Note the following about this option:
- Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately.
- Line cards reboot automatically.
- Does not apply to PIX devices managed through Auto Update Server (AUS).
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform distribution in Non-Installed mode</td>
<td>This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.</td>
</tr>
<tr>
<td>Do not insert new boot commands into configuration file</td>
<td>Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.</td>
</tr>
<tr>
<td>Use current running image as tftp fallback image</td>
<td>If running image is in repository, select option to place a copy in the FTP server directory. Uses this copy if reboot with new image fails. Note the following: • This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. • Backup image is not deleted after upgrade. It remains in FTP server directory so that device can find it any time it reboots</td>
</tr>
<tr>
<td>Back up current running image</td>
<td>Select to back up running image in software image repository before upgrading. Line cards do not support upload.</td>
</tr>
<tr>
<td>On error, halt processing of subsequent devices</td>
<td>Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device. For sequential execution, if you do not select this option, upgrade for next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.</td>
</tr>
<tr>
<td>Enable Job Password</td>
<td>Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (Inventory &gt; Device Administration &gt; Add / Import / Manage Devices) are ignored. You are allowed to provide a password in this field only if you have selected the Enable Job Based Password in the View / Edit Preferences dialog box. See Administration of Cisco Prime LAN Management Solution 4.2 for more details.</td>
</tr>
</tbody>
</table>
**Chapter 9: Managing Software Images Using Software Management**

### Software Distribution

**Step 9** Click **Next** after you finish entering the job information details. If you have selected Using External TFTP server option, proceed to the **TFTP Wizard**.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Details of the Remote Stage device or the External FTP server.
- Verification warnings generated during image distribution (if applicable).

**Step 10** Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Execution | Select the job execution order for the devices. This can be either Parallel or Sequential:  
- Sequential—Job runs on the devices, sequentially. You can define this sequence.  
- Parallel—Job runs on a batch of 15 devices at the same time.  
If you have selected Sequential:  
1. Click **Execution Order**.  
   The Execution Order dialog box appears.  
2. Use the Up and Down arrows to order your the device list.  
3. Click **Done**. |
| Reboot | Select the reboot order for the devices. This can be either Parallel or Sequential.  
If you have selected Sequential:  
1. Click **Boot Order**.  
   The Boot Order dialog box appears.  
2. Use the Up and the Down arrows to order your devices list.  
3. Click **Done**. |
## Supported Devices for FTP

<table>
<thead>
<tr>
<th>Device Family</th>
<th>Device</th>
<th>SysObject ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAM</td>
<td>NAM X6380</td>
<td>1.3.6.1.4.1.9.5.1.3.1.1.2.223</td>
</tr>
<tr>
<td></td>
<td>NAM1</td>
<td>1.3.6.1.4.1.9.5.1.3.1.1.2.914</td>
</tr>
<tr>
<td></td>
<td>NAM2</td>
<td>1.3.6.1.4.1.9.5.1.3.1.1.2.291</td>
</tr>
<tr>
<td></td>
<td>NM NAM</td>
<td>1.3.6.1.4.1.9.1.562</td>
</tr>
<tr>
<td></td>
<td>NME NAM</td>
<td>1.3.6.1.4.1.9.1.826</td>
</tr>
<tr>
<td>WLSE</td>
<td>WLSE</td>
<td>1.3.6.1.4.1.9.1.459</td>
</tr>
<tr>
<td></td>
<td>WLSE</td>
<td>1.3.6.1.4.1.9.1.630</td>
</tr>
<tr>
<td></td>
<td>WLSE</td>
<td>1.3.6.1.4.1.9.1.631</td>
</tr>
<tr>
<td></td>
<td>WLSE 1153</td>
<td>1.3.6.1.4.1.9.1.752</td>
</tr>
<tr>
<td>Cisco Catalyst 3750 Series Switches</td>
<td>CatalystIOS37XXStack</td>
<td>1.3.6.1.4.1.9.1.516</td>
</tr>
<tr>
<td></td>
<td>Catalyst3750ME</td>
<td>1.3.6.1.4.1.9.1.574</td>
</tr>
<tr>
<td></td>
<td>WS.C3750G.12S.SD</td>
<td>1.3.6.1.4.1.9.1.688</td>
</tr>
<tr>
<td></td>
<td>WS.C3750E.24TD</td>
<td>1.3.6.1.4.1.9.1.789</td>
</tr>
<tr>
<td></td>
<td>WS.C3750E.48TD</td>
<td>1.3.6.1.4.1.9.1.790</td>
</tr>
<tr>
<td></td>
<td>WS.C3750E.48PD</td>
<td>1.3.6.1.4.1.9.1.791</td>
</tr>
<tr>
<td></td>
<td>WS.C3750E.24PD</td>
<td>1.3.6.1.4.1.9.1.792</td>
</tr>
<tr>
<td></td>
<td>catalyst375024</td>
<td>1.3.6.1.4.1.9.1.511</td>
</tr>
<tr>
<td></td>
<td>catalyst375048</td>
<td>1.3.6.1.4.1.9.1.512</td>
</tr>
<tr>
<td></td>
<td>catalyst375024TS</td>
<td>1.3.6.1.4.1.9.1.513</td>
</tr>
<tr>
<td></td>
<td>catalyst375024T</td>
<td>1.3.6.1.4.1.9.1.514</td>
</tr>
<tr>
<td></td>
<td>catalyst375048PS</td>
<td>1.3.6.1.4.1.9.1.535</td>
</tr>
<tr>
<td></td>
<td>catalyst3750G24PS</td>
<td>1.3.6.1.4.1.9.1.602</td>
</tr>
<tr>
<td></td>
<td>catalyst3750G48PS</td>
<td>1.3.6.1.4.1.9.1.603</td>
</tr>
<tr>
<td></td>
<td>catalyst3750G48TS</td>
<td>1.3.6.1.4.1.9.1.604</td>
</tr>
<tr>
<td></td>
<td>catalyst3750G24TS1U</td>
<td>1.3.6.1.4.1.9.1.624</td>
</tr>
<tr>
<td></td>
<td>catalyst375024FS</td>
<td>1.3.6.1.4.1.9.1.656</td>
</tr>
<tr>
<td>Cisco Intelligent Gigabit Ethernet Switch Module (IEGSM)</td>
<td>ciscoIGESM</td>
<td>1.3.6.1.4.1.9.1.592</td>
</tr>
<tr>
<td></td>
<td>ciscoIGESMSFP</td>
<td>1.3.6.1.4.1.9.1.660</td>
</tr>
</tbody>
</table>
### Table 9-7  Supported Devices for FTP

<table>
<thead>
<tr>
<th>Device Family</th>
<th>Device</th>
<th>SysObject ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 3560,C3560E Series</td>
<td>CatalystIOS3560G.24PS</td>
<td>1.3.6.1.4.1.9.1.614</td>
</tr>
<tr>
<td>Switches</td>
<td>CatalystIOS3560G.24TS</td>
<td>1.3.6.1.4.1.9.1.615</td>
</tr>
<tr>
<td></td>
<td>CatalystIOS3560G.48PS</td>
<td>1.3.6.1.4.1.9.1.616</td>
</tr>
<tr>
<td></td>
<td>CatalystIOS3560G.48TS</td>
<td>1.3.6.1.4.1.9.1.617</td>
</tr>
<tr>
<td></td>
<td>CatalystIOS3560.24PS.S</td>
<td>1.3.6.1.4.1.9.1.563</td>
</tr>
<tr>
<td></td>
<td>CatalystIOS3560.48PS</td>
<td>1.3.6.1.4.1.9.1.564</td>
</tr>
<tr>
<td></td>
<td>CatalystIOS3560.24TS</td>
<td>1.3.6.1.4.1.9.1.633</td>
</tr>
<tr>
<td></td>
<td>CatalystIOS3560.48TS</td>
<td>1.3.6.1.4.1.9.1.634</td>
</tr>
<tr>
<td></td>
<td>WS.C3560E.24TD</td>
<td>1.3.6.1.4.1.9.1.793</td>
</tr>
<tr>
<td></td>
<td>WS.C3560E.48TD</td>
<td>1.3.6.1.4.1.9.1.794</td>
</tr>
<tr>
<td></td>
<td>WS.C3560E.24PD</td>
<td>1.3.6.1.4.1.9.1.795</td>
</tr>
<tr>
<td></td>
<td>WS.C3560E.48PD</td>
<td>1.3.6.1.4.1.9.1.796</td>
</tr>
<tr>
<td></td>
<td>WS.C3560.8PC</td>
<td>1.3.6.1.4.1.9.1.797</td>
</tr>
<tr>
<td>CBS3030Del</td>
<td>CBS3030Del</td>
<td>1.3.6.1.4.1.9.1.749</td>
</tr>
<tr>
<td>Cisco Blade Switches (CBS)</td>
<td>CBS3020</td>
<td>1.3.6.1.4.1.9.1.748</td>
</tr>
<tr>
<td></td>
<td>CBS3040</td>
<td>1.3.6.1.4.1.9.1.784</td>
</tr>
<tr>
<td></td>
<td>CBS1100</td>
<td>1.3.6.1.4.1.9.1.946</td>
</tr>
<tr>
<td></td>
<td>CBS3110</td>
<td>1.3.6.1.4.1.9.1.947</td>
</tr>
<tr>
<td></td>
<td>CBS3120</td>
<td>1.3.6.1.4.1.9.1.948</td>
</tr>
<tr>
<td></td>
<td>CBS3130</td>
<td>1.3.6.1.4.1.9.1.949</td>
</tr>
<tr>
<td></td>
<td>CBS3012</td>
<td>1.3.6.1.4.1.9.1.999</td>
</tr>
<tr>
<td></td>
<td>CBS3012I</td>
<td>1.3.6.1.4.1.9.1.1000</td>
</tr>
<tr>
<td></td>
<td>CBS3132</td>
<td>1.3.6.1.4.1.9.1.920</td>
</tr>
<tr>
<td></td>
<td>CBS3110G-S</td>
<td>1.3.6.1.4.1.9.1.909</td>
</tr>
<tr>
<td></td>
<td>CBS3110X-S</td>
<td>1.3.6.1.4.1.9.1.910</td>
</tr>
<tr>
<td></td>
<td>CBS3110G-S-I</td>
<td>1.3.6.1.4.1.9.1.911</td>
</tr>
<tr>
<td></td>
<td>CBS3110X-S-I</td>
<td>1.3.6.1.4.1.9.1.912</td>
</tr>
<tr>
<td></td>
<td>CBS3125G-S</td>
<td>1.3.6.1.4.1.9.1.1001</td>
</tr>
<tr>
<td></td>
<td>CBS3120G-S</td>
<td>1.3.6.1.4.1.9.1.1018</td>
</tr>
<tr>
<td></td>
<td>CBS3125X-S</td>
<td>1.3.6.1.4.1.9.1.1002</td>
</tr>
<tr>
<td></td>
<td>CBS3120X-S</td>
<td>1.3.6.1.4.1.9.1.1919</td>
</tr>
<tr>
<td></td>
<td>CBS3130G-S</td>
<td>1.3.6.1.4.1.9.1.921</td>
</tr>
<tr>
<td></td>
<td>CBS3130X-S</td>
<td>1.3.6.1.4.1.9.1.922</td>
</tr>
</tbody>
</table>
### Supported Devices for FTP

<table>
<thead>
<tr>
<th>Device Family</th>
<th>Device</th>
<th>SysObject ID</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Catalyst 2960 Series Switches</strong></td>
<td>Catalyst296024</td>
<td>1.3.6.1.4.1.9.1.694</td>
</tr>
<tr>
<td></td>
<td>Catalyst296048</td>
<td>1.3.6.1.4.1.9.1.695</td>
</tr>
<tr>
<td></td>
<td>Catalyst2960G24</td>
<td>1.3.6.1.4.1.9.1.696</td>
</tr>
<tr>
<td></td>
<td>WS-C2960G-48TC-L</td>
<td>1.3.6.1.4.1.9.1.697</td>
</tr>
<tr>
<td></td>
<td>Catalyst296024TT</td>
<td>1.3.6.1.4.1.9.1.716</td>
</tr>
<tr>
<td></td>
<td>Catalyst296048TT</td>
<td>1.3.6.1.4.1.9.1.717</td>
</tr>
<tr>
<td></td>
<td>Catalyst29608TC</td>
<td>1.3.6.1.4.1.9.1.798</td>
</tr>
<tr>
<td></td>
<td>Catalyst2960G8TC</td>
<td>1.3.6.1.4.1.9.1.799</td>
</tr>
<tr>
<td></td>
<td>C2960-24-S</td>
<td>1.3.6.1.4.1.9.1.929</td>
</tr>
<tr>
<td></td>
<td>C2960-24TC-S</td>
<td>1.3.6.1.4.1.9.1.928</td>
</tr>
<tr>
<td></td>
<td>C2960-48TC-S</td>
<td>1.3.6.1.4.1.9.1.927</td>
</tr>
<tr>
<td></td>
<td>C2960-24PC-L</td>
<td>1.3.6.1.4.1.9.1.950</td>
</tr>
<tr>
<td></td>
<td>C2960-24LT-L</td>
<td>1.3.6.1.4.1.9.1.951</td>
</tr>
<tr>
<td></td>
<td>C2960PD-8TT-L</td>
<td>1.3.6.1.4.1.9.1.952</td>
</tr>
<tr>
<td></td>
<td>C2960P</td>
<td>1.3.6.1.4.1.9.1.1006</td>
</tr>
<tr>
<td></td>
<td>C2960</td>
<td>1.3.6.1.4.1.9.1.1005</td>
</tr>
<tr>
<td><strong>Cisco Catalyst 3550 Series Switches</strong></td>
<td>Catalyst355012T</td>
<td>1.3.6.1.4.1.9.1.368</td>
</tr>
<tr>
<td></td>
<td>Catalyst355024switch</td>
<td>1.3.6.1.4.1.9.1.366</td>
</tr>
<tr>
<td></td>
<td>Catalyst355048switch</td>
<td>1.3.6.1.4.1.9.1.367</td>
</tr>
<tr>
<td></td>
<td>Catalyst355012G</td>
<td>1.3.6.1.4.1.9.1.361</td>
</tr>
<tr>
<td></td>
<td>Catalyst355024DC</td>
<td>1.3.6.1.4.1.9.1.452</td>
</tr>
<tr>
<td></td>
<td>Catalyst355024FX</td>
<td>1.3.6.1.4.1.9.1.453</td>
</tr>
<tr>
<td></td>
<td>Catalyst355024PWR</td>
<td>1.3.6.1.4.1.9.1.485</td>
</tr>
<tr>
<td><strong>Cisco PIX Series Security Appliances</strong></td>
<td>PIX 535</td>
<td>1.3.6.1.4.1.9.1.675</td>
</tr>
<tr>
<td></td>
<td>PIX 525</td>
<td>1.3.6.1.4.1.9.1.676</td>
</tr>
<tr>
<td></td>
<td>PIX 515</td>
<td>1.3.6.1.4.1.9.1.678</td>
</tr>
<tr>
<td></td>
<td>PIX 515E</td>
<td>1.3.6.1.4.1.9.1.451</td>
</tr>
<tr>
<td></td>
<td>PIX 515EFirewall</td>
<td>1.3.6.1.4.1.9.1.677</td>
</tr>
</tbody>
</table>
Chapter 9 
Managing Software Images Using Software Management

Software Distribution

Table 9-7: Supported Devices for FTP

<table>
<thead>
<tr>
<th>Device Family</th>
<th>Device</th>
<th>SysObject ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Adaptive Security Appliances (ASA)</td>
<td>ASA5510</td>
<td>1.3.6.1.4.1.9.1.773</td>
</tr>
<tr>
<td></td>
<td>ASA5520</td>
<td>1.3.6.1.4.1.9.1.671</td>
</tr>
<tr>
<td></td>
<td>ASA5520</td>
<td>1.3.6.1.4.1.9.1.670</td>
</tr>
<tr>
<td></td>
<td>ASA5510</td>
<td>1.3.6.1.4.1.9.1.669</td>
</tr>
<tr>
<td></td>
<td>ASA5505</td>
<td>1.3.6.1.4.1.9.1.745</td>
</tr>
<tr>
<td></td>
<td>ASA5550</td>
<td>1.3.6.1.4.1.9.1.763</td>
</tr>
<tr>
<td></td>
<td>ASA5540</td>
<td>1.3.6.1.4.1.9.1.673</td>
</tr>
<tr>
<td></td>
<td>ASA5580</td>
<td>1.3.6.1.4.1.9.1.672</td>
</tr>
<tr>
<td></td>
<td>ASA5550</td>
<td>1.3.6.1.4.1.9.1.753</td>
</tr>
<tr>
<td></td>
<td>ASA5540</td>
<td>1.3.6.1.4.1.9.1.914</td>
</tr>
<tr>
<td></td>
<td>ASA5580</td>
<td>1.3.6.1.4.1.9.1.915</td>
</tr>
</tbody>
</table>

Using External TFTP Server

If you have selected Using External TFTP server option:

Step 1 Enter the external TFTP server IP address in the Enter TFTP IP Address text box.

Step 2 Click Next.

The Remote Staging and Distribution dialog box appears.

Step 3 Select:
   a. An image from the Image Selection pane.
   b. Click on Select Applicable Devices button to automatically select the applicable devices
      Or
      Manually select the devices that need an upgrade from the Devices to be Upgraded pane.

For more information on the unsupported images for Remote Staging and Distribution, see Unsupported Software Images.

Step 4 Click Next.

The External TFTP Server Details dialog box appears with the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP Address of the External TFTP server.</td>
</tr>
<tr>
<td>Selected Image</td>
<td>Image name that you have selected for distribution.</td>
</tr>
<tr>
<td>Errors</td>
<td>Error information.</td>
</tr>
</tbody>
</table>

Step 5 Click Next.

The Device Recommendation dialog box appears with the following details:
### Field | Description
---|---
Device Information | Name of the device.  Click on the device name to launch the Troubleshooting page.
Module Information | Image type, chassis model, and software version on device.
Storage Options | Details of recommended image storage information.
Errors | Error information.

**Step 6**  Click **Next**.

The Remote Devices Verification dialog box appears with the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device</td>
</tr>
<tr>
<td>Selected Module</td>
<td>Module information that you have selected.</td>
</tr>
<tr>
<td>Selected Slot</td>
<td>Image storage information that you have selected.</td>
</tr>
<tr>
<td>Verification Result</td>
<td>Click on the link to review the details.</td>
</tr>
</tbody>
</table>

**Step 7**  Click **Next**.

The Job Schedule and Options dialog box appears.

**Step 8**  Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Run Type | You can specify when you want to run the Image Distribution (using remote staging) job. To do this, select one of these options from the drop-down menu:  
  - Immediate—Runs this job immediately.  
  - Once—Runs this job once at the specified date and time. |
| Date | Select the date and time (hours and minutes) to schedule. |
| **Job Info** |  |
| Job Description | Enter a description for the job. This is mandatory. You can enter only alphanumeric characters. |
| E-mail | Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job.  
You can enter multiple e-mail addresses separated by commas.  
Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences).  
We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender’s address. |
| Comments | Enter the additional information about this job. |
### Software Distribution

**Field** | **Description**
--- | ---
Maker E-Mail | Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.

Maker Comments | Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

**Job Options**

| **Reboot immediately after download** | Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option:
• Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately.
• Line cards reboot automatically.
• Does not apply to PIX devices managed through Auto Update Server (AUS). |

| **Perform distribution in Non-Installed mode** | This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode. |

| **Do not insert new boot commands into configuration file** | Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated. |

| **Use current running image as tftp fallback image** | If running image is in repository, select option to place a copy in the TFTP server directory. Uses this copy if reboot with new image fails. Note the following:
• This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation.
• Backup image is not deleted after upgrade. It remains in TFTP server directory so that device can find it any time it reboots |

| **Back up current running image** | Select to back up running image in software image repository before upgrading. Line cards do not support upload. |

| **On error, halt processing of subsequent devices** | Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device. For sequential execution, if you do not select this option, upgrade for next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details. |
The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Details of the Remote Stage device or the External TFTP/FTP server.
- Verification warnings generated during image distribution (if applicable).

**Step 9** Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- **Enable Job Password**
  Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution.
  The credentials that you enter here are used for this particular Software Management job.
  The credentials that you have entered in the Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices) are ignored.
  You are allowed to provide a password in this field only if you have selected the Enable Job Based Password in the View / Edit Preferences dialog box. See *Administration of Cisco Prime LAN Management Solution 4.2* for more details.

- **Execution**
  Select the job execution order for the devices. This can be either Parallel or Sequential:
  - **Sequential**—Job runs on the devices, sequentially. You can define this sequence.
  - **Parallel**—Job runs on a batch of 15 devices at the same time.
  If you have selected Sequential:
    1. Click **Execution Order**.
       The Execution Order dialog box appears.
    2. Use the Up and Down arrows to order your device list.
    3. Click **Done**.

- **Reboot**
  Select the reboot order for the devices. This can be either Parallel or Sequential.
  If you have selected Sequential:
    1. Click **Boot Order**.
       The Boot Order dialog box appears.
    2. Use the Up and the Down arrows to order your devices list.
    3. Click **Done**.
Step 10 Click Finish.

The notification window appears with the Job ID.

To check the status of your scheduled job, select Configuration > Tools > Software Image Management > Jobs.

Using Remote Stage Device

If you have selected Remote Stage device option:

Step 1 Go to the Select Remote Stage Device pane, select a device that you want to use as the remote stage device. Ensure that you select a device that supports remote staging.

If you select a device that does not support remote staging, an error message is displayed.

Step 2 Click Next.

The Remote Staging and Distribution dialog box appears.

Step 3 Select:

a. An image from the Image Selection pane.

b. Click Select Applicable Devices to automatically select the applicable devices or

Manually select the devices that need an upgrade from the Devices to be Upgraded pane.

For more information on the unsupported images for Remote Staging and Distribution, see Unsupported Software Images.

Step 4 Click Next.

The Remote Stage and Image Upgrade Details dialog box appears with the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Stage Name</td>
<td>Name of the remote stage device that you want to use as a remote stage.</td>
</tr>
<tr>
<td>Selected Image</td>
<td>Image name that you have selected for distribution.</td>
</tr>
<tr>
<td>Storage Options</td>
<td>Image storage information</td>
</tr>
</tbody>
</table>

Step 5 Click Next.

If the Remote Stage verification fails, check if the Remote Stage device has enough free space and restart the software distribution from the beginning.
The Device Recommendation dialog box appears. This displays the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td>Name of the device.</td>
</tr>
<tr>
<td></td>
<td>Click on the device name to launch the Troubleshooting page.</td>
</tr>
<tr>
<td>Module Information</td>
<td>Image type, chassis model, and software version on device.</td>
</tr>
<tr>
<td>Storage Options</td>
<td>Details of recommended image storage information.</td>
</tr>
</tbody>
</table>

Step 6  Click Next.

The Remote Devices Verification dialog box appears with the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Selected Module</td>
<td>Module information that you have selected.</td>
</tr>
<tr>
<td>Selected Slot</td>
<td>Image storage information that you have selected.</td>
</tr>
<tr>
<td>Verification Result</td>
<td>Click on the link to review the details.</td>
</tr>
</tbody>
</table>

Step 7  Click Next.

The Job Schedule and Options dialog box appears.

Step 8  Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td>You can specify when you want to run the Image Distribution (using remote staging) job.</td>
</tr>
<tr>
<td>Run Type</td>
<td>You can specify when you want to run the Image Distribution (using remote staging) job.</td>
</tr>
<tr>
<td></td>
<td>To do this, select one of these options from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs this job immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs this job once at the specified date and time.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the date and time (hours and minutes) to schedule.</td>
</tr>
<tr>
<td>Job Info</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas.</td>
</tr>
<tr>
<td></td>
<td>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter the additional information about this job.</td>
</tr>
</tbody>
</table>
### Software Distribution

#### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maker E-Mail</td>
<td>Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.</td>
</tr>
<tr>
<td>Maker Comments</td>
<td>Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.</td>
</tr>
</tbody>
</table>

#### Job Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Reboot immediately after download          | Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option:  
• Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately.  
• Line cards reboot automatically.  
• Does not apply to PIX devices managed through Auto Update Server (AUS). |
| Perform distribution in Non-Installed mode | This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode. |
| Do not insert new boot commands into configuration file | Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated. |
| Use current running image as tftp fallback image | If running image is in repository, select option to place a copy in the TFTP server directory. Uses this copy if reboot with new image fails. Note the following:  
• This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation.  
• Backup image is not deleted after upgrade. It remains in TFTP server directory so that device can find it any time it reboots |
| Back up current running image             | Select to back up running image in software image repository before upgrading. Line cards do not support upload.                                      |
| On error, halt processing of subsequent devices | Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device.  
For sequential execution, if you do not select this option, upgrade for next device begins.  
For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed.  
See the Job Summary page for details. |
Chapter 9  Managing Software Images Using Software Management

Software Distribution

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Job Password</td>
<td>Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (Inventory &gt; Device Administration &gt; Add / Import / Manage Devices) are ignored. You are allowed to provide a password in this field only if you have selected the Enable Job Based Password in the View / Edit Preferences dialog box. See Administration of Cisco Prime LAN Management Solution 4.2 for more details.</td>
</tr>
</tbody>
</table>

**Execution**

Select the job execution order for the devices. This can be either Parallel or Sequential:
- Sequential—Job runs on the devices, sequentially. You can define this sequence.
- Parallel—Job runs on a batch of 15 devices at the same time.

If you have selected Sequential:
1. Click **Execution Order**.
   - The Execution Order dialog box appears.
2. Use the Up and Down arrows to order your device list.
3. Click **Done**.

**Reboot**

Select the reboot order for the devices. This can be either Parallel or Sequential.

If you have selected Sequential:
1. Click **Boot Order**.
   - The Boot Order dialog box appears.
2. Use the Up and the Down arrows to order your devices list.
3. Click **Done**.

---

**Step 9**  
Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:
- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Details of the Remote Stage device or the External TFTP server.
- Verification warnings generated during image distribution (if applicable).
Step 10  Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs.**

---

**Unsupported Software Images**

During remote staging, there may be software images running on the devices selected for remote staging, but some of them may not get listed as available images. This is because, some software images do not support Remote Staging and Distribution.

The following below lists the software images that do not support Remote Staging and Distribution:

- CSS_SW FDDI_CDDI
- ATM_WTALL
- ATM_WBPVC
- CIP
- CSS_11000_SW
- C6KMODULE_MWAM_SW
- PATCH_SW
- ONS15530
- TOKENRING
- ATM_WBLANE
- BOOT_LOADER
- C6KMODULE_MWAM_SW
- CSS_11500_SW
- CSS_11000_SW
- C2500
- C1600
- BLADERUNNER
- ATM_WTOKEN
- MICA MICROCOM
- NAM_APPL_SW
- SPA_FPD_SW
- CSS_11500_SW
- ONS15540
Understanding Upgrade Recommendations

This section describes how Software Management recommends image for the various Cisco device types:

- Upgrade Recommendation for Cisco IOS Devices
- Upgrade Recommendation for Catalyst Devices
- Upgrade Recommendation for VPN 3000 Series
- Upgrade Recommendation for Catalyst 1900/2820
- Upgrade Recommendation for Other Device Types

Upgrade Recommendation for Cisco IOS Devices

To determine the recommended software images for Cisco IOS devices, Software Management:

1. Lists all images in the software repository that can run on the device. For example, C7000 images run on 7000 and 7010 devices, IGS images run on 25xx devices, and so on.
2. Removes all listed images that require:
   - More RAM or Flash memory than is available on the device.
   - A newer boot ROM than the one on the device.
   If RAM is UNKNOWN, it is not considered in any comparison operation (image filtering). However, you are warned during the subsequent task.
3. Recommends an image whose feature subset matches the image running on the device.
   - Any images that support all current features and include some additional ones, take precedence over images that match exactly.
   - If more than one image is either a superset or an exact match of the running image, the latest version takes precedence over earlier versions.
4. Removes the images from recommendation if the images Min.Flash size requirement is not met by the device.
   If Min.Flash required is UNKNOWN, it is not considered in any comparison operation (image filtering).
   If Flash Size is UNKNOWN, the image cannot be used for upgrade.
   See the IOS Software Release documentation on Cisco.com to know the Min.Flash size.
5. Depending on the image feature list, Software Management recommends an image whose image version is lower than the current running image version.
6. Recommends to filter out the images that are larger in size than the flash available on the device.
7. Recommends Flash partitions on the device along with the storage details, if you are upgrading the Boot Loader image.

This algorithm might recommend images that are older than the one running on the device.

To ensure that only newer images are recommended, select Admin > Network > Software Image Management > View/Edit Preferences. In the View/Edit Preferences dialog box, select the Include images higher than running image checkbox, then click Apply.
Upgrade Recommendation for Catalyst Devices

For Catalyst device upgrades, Software Management typically recommends the latest version images in the software repository.

For default RAM requirements for Supervisor Engine I and Supervisor Engine III, however, Software Management uses:

<table>
<thead>
<tr>
<th>Module Type and Version</th>
<th>Default RAM (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor Engine III</td>
<td>32</td>
</tr>
<tr>
<td>Supervisor version 2.1 up to (but not including) 3.1</td>
<td>8</td>
</tr>
<tr>
<td>Supervisor version 3.1.1 and later</td>
<td>16</td>
</tr>
<tr>
<td>Maintenance release versions 3.1 and 3.2 with “Sup8M” in filename</td>
<td>8</td>
</tr>
</tbody>
</table>

For supervisor versions 3.1 to 3.2, when the image repository or Cisco.com has both 8 MB of RAM and regular images available, Software Management also checks the device RAM:

1. If the RAM can be determined and the available RAM is greater than 16 MB:
   a. Software Management recommends the latest regular supervisor image where the RAM requirement is less than the available RAM.
   b. If no regular image with matching RAM requirements is available, it recommends the latest version of the 8-MB images.
   c. If there is still no matching image, it recommends the latest image version that has no RAM requirements (where the RAM requirement is set to DEFAULT_SIZE).

2. If the RAM can be determined and the available RAM is less than 16 MB:
   a. Software Management recommends the highest image version for which the RAM requirement is less than 16 MB.
   b. If there is still no matching image, it recommends the latest image version that has no RAM requirements (where the RAM requirement is set to DEFAULT_SIZE).

3. If the RAM cannot be determined:
   a. Software Management recommends the latest regular image.
   b. If no regular image is available, it recommends the latest 8-MB image.
   c. If there is still no matching image, it recommends the latest image version that has no RAM requirements (where the RAM requirement is set to DEFAULT_SIZE).

The minimum RAM in the image attributes file supersedes these guidelines.

For example, if a supervisor engine module is running the version 3.1 maintenance release (8 MB RAM) but the RAM in the image attributes was changed to 16 MB, Software Management uses the value in the attributes file.
Upgrade Recommendation for VPN 3000 Series

Software Management recommends the latest version of the image in the software image repository. If the device is a VPN 3005 Concentrator, it recommends the VPN 3005 System software images in the repository.

Upgrade Recommendation for Catalyst 1900/2820

For Catalyst 1900/2820 Enterprise version device upgrades, Software Management typically recommends the latest version of images in the software repository.

Note

For Catalyst 1900/2820 Series devices, Software Management recommends images with version numbers greater than 8.0(0) because the older versions do not support the Command Line Interface. Non-Enterprise versions of the Catalyst 1900/2820 are not supported in Software Management.

Upgrade Recommendation for Other Device Types

For the following device types, Software Management recommends the latest version of the image in the software image repository:

- PIX Firewall Devices
  - If you are running PIX image version 7.0 or later, while recommending the image, Software Management will also recommend the storage details of the device.
- Content Service Switches
- Aironet AP Series
- Optical Switch Series
- Network Analysis Module Series
- Content Engines

Using Software Management Job Browser

Using this window you can view all your scheduled Software Management jobs. The Software Management Job Browser contains the following fields and buttons:

- Software Management Job Browser Fields
- Software Management Job Browser Buttons

This section contains:

- Changing the Schedule of a Job
- Retry a Failed Distribution Job
- Undo a Successful Distribution Job
- Stopping a Job
- Deleting Jobs
The Software Management Job Browser displays the following details for a job:

Table 9-8  Software Management Job Browser Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique number assigned to the job when it is created.</td>
</tr>
<tr>
<td></td>
<td>Click to display a summary of job details and schedule options.</td>
</tr>
<tr>
<td></td>
<td>See Understanding the Software Management Job Summary for further details.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Type of job such as Import Images, Distribute Images.</td>
</tr>
<tr>
<td>Status</td>
<td>Job states:</td>
</tr>
<tr>
<td></td>
<td>• Successful—Job completed successfully</td>
</tr>
<tr>
<td></td>
<td>• Failed—Failed job. Click on the Job ID to view the job details.</td>
</tr>
<tr>
<td></td>
<td>The number, within brackets, next to Failed status indicates the count of</td>
</tr>
<tr>
<td></td>
<td>the devices that had failed for that job. This count is displayed only</td>
</tr>
<tr>
<td></td>
<td>if the status is Failed.</td>
</tr>
<tr>
<td></td>
<td>For example, If the status displays Failed(5), then the count of devices</td>
</tr>
<tr>
<td></td>
<td>that had failed is 5.</td>
</tr>
<tr>
<td></td>
<td>• Running—Job still running.</td>
</tr>
<tr>
<td></td>
<td>• Pending—Job scheduled to run.</td>
</tr>
<tr>
<td></td>
<td>• Stopped—Running job stopped by you.</td>
</tr>
<tr>
<td></td>
<td>• Missed Start—Job could not run for some reason at the scheduled time.</td>
</tr>
<tr>
<td></td>
<td>For example, if the system was down when the job was scheduled to start,</td>
</tr>
<tr>
<td></td>
<td>when the system comes up again, the job does not run.</td>
</tr>
<tr>
<td></td>
<td>This is because the scheduled time for the job has elapsed. The status for</td>
</tr>
<tr>
<td></td>
<td>the specified job will be displayed as Missed Start.</td>
</tr>
<tr>
<td></td>
<td>• Approved—Job approved by an approver</td>
</tr>
<tr>
<td></td>
<td>• Rejected—Job rejected by an approver. Click on the Job ID to view the</td>
</tr>
<tr>
<td></td>
<td>rejection details.</td>
</tr>
<tr>
<td></td>
<td>• Waiting for Approval—Job waiting for approval.</td>
</tr>
<tr>
<td>Description</td>
<td>Job description as entered at the time of creation.</td>
</tr>
<tr>
<td>Owner</td>
<td>User who created the job.</td>
</tr>
<tr>
<td>Scheduled At</td>
<td>Start time of the scheduled job.</td>
</tr>
<tr>
<td>Completed At</td>
<td>End time of the scheduled job.</td>
</tr>
<tr>
<td>Schedule Type</td>
<td>Type of the scheduled job:</td>
</tr>
<tr>
<td></td>
<td>• Immediate</td>
</tr>
<tr>
<td></td>
<td>• Once</td>
</tr>
</tbody>
</table>
Changing the Schedule of a Job

You can change the schedule only for jobs that are either in the Pending, Waiting for Approval or the Approved status.

Note View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To change the schedule of a job:

Step 1 Select Configuration > Tools > Software Image Management > Jobs.

The Software Management Job Browser dialog box appears.

Step 2 Select either a pending or an approved job.

Step 3 Click Edit.

The Change Job Schedule dialog box appears.
Step 4  Change the schedule.
Step 5  Click Submit.

## Retry a Failed Distribution Job

You can retry only failed distribution jobs.

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To retry a Job:

**Step 1**  Select Configuration > Tools > Software Image Management > Jobs. The Software Management Job Browser dialog box appears.

**Step 2**  Select a failed distribution job.

**Step 3**  Click Retry. The Retry Upgrade dialog box appears with the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td>Name of the device</td>
</tr>
<tr>
<td>Module</td>
<td>Device module</td>
</tr>
<tr>
<td>Pre-upgrade Image</td>
<td>Image name that was running before the upgrade.</td>
</tr>
<tr>
<td>Selected Image</td>
<td>Image name that is selected for distribution.</td>
</tr>
<tr>
<td>Running Image</td>
<td>Image name that is currently running on the device.</td>
</tr>
<tr>
<td>Errors</td>
<td>Click on the underlined Error message to review the details.</td>
</tr>
</tbody>
</table>

**Step 4**  Click Next.

Continue entering the information for this job as you would for a new distribution depending on your previous distribution selection:

- Distributing by Devices [Basic]
- Distributing by Devices [Advanced]
- Distributing by Images
- Remote Staging and Distribution
Undo a Successful Distribution Job

You can undo only successful Distribution jobs.

Note View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To undo a job:

Step 1 Select Configuration > Tools > Software Image Management > Jobs.

The Software Management Job Browser dialog box appears.

Step 2 Select a successful distribution job.

Step 3 Click Undo.

The Undo Upgrade dialog box appears with the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device</td>
</tr>
<tr>
<td>Module</td>
<td>Device module</td>
</tr>
<tr>
<td>Pre-upgrade Image</td>
<td>Image name which was running before the upgrade.</td>
</tr>
<tr>
<td>Post-upgrade Image</td>
<td>Image name after completing the upgrade.</td>
</tr>
<tr>
<td>Running Image</td>
<td>Image name that is currently running on the image.</td>
</tr>
<tr>
<td>Errors</td>
<td>Click on the underlined Error message to review the details.</td>
</tr>
</tbody>
</table>

Step 4 Click Next.

Continue entering the information for this job as you would for a new distribution. This depend on what you selected earlier in the Distribution Method window:

- Distributing by Devices [Basic]
- Distributing by Devices [Advanced]
- Distributing by Images
- Remote Staging and Distribution
Stopping a Job

You can stop only jobs that are either in the Pending or the Running status.

The job stops only after the current task is complete. During this time, the Software Management Job Browser window displays the job status as Running.

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

To stop a job:

Step 1 Select Configuration > Tools > Software Image Management > Jobs.

The Software Management Job Browser dialog box appears.

Step 2 Select either a pending or a running job.

Step 3 Click Stop.

A confirmation box shows that the selected job will be stopped.

Step 4 Click OK.

A message appears that the selected job has been stopped.

After the job is stopped, the Pending job status changes to Stopped. The Running job status changes temporarily to Stop Initiated and then to Stopped.

Deleting Jobs

To delete jobs:

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

Step 1 Select Configuration > Tools > Software Image Management > Jobs.

The Software Management Job Browser dialog box appears.

Step 2 Select the jobs.

Step 3 Click Delete.

A confirmation box shows that the selected jobs will be deleted.

Step 4 Click OK.
Understanding the Software Management Job Summary

From the Software Management Job Browser, you can learn more about one job by viewing its details. You can view this details by clicking the Job ID on the Software Management Job Browser window.

Note

View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

The Software Management Job Details window contains the following information:

<table>
<thead>
<tr>
<th>Page/Folder</th>
<th>Description</th>
</tr>
</thead>
</table>
| Work Order       | Select a device to view the summary of the job:  
  • If there is more than one device, the software distribution order.  
  • The state of the running image on the device.  
  • The image selected for the upgrade.  
  • Whether Flash memory will be erased before the new image is loaded.  
  • Operations that will be performed during the upgrade procedure.  
  • For a bootloader upgrade, whether the bootloader will be upgraded.  
  • The Job Approval information.  
  • Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.  
  • Details of the Remote Stage device (if applicable).  
  • Verification warnings generated during image distribution (if applicable). |
| Job Results      | Select a device to view the complete job result. It displays information on:  
  • The job status, start time and end time.  
  • The job completion status on the devices you have selected. For example, number of successful devices where the job is executed successfully.  
  • The import/upgrade mode (parallel or sequential)  
  • The protocol order used for image transfer and configuration tasks.  
  • How the job was processed. |
| Summary[On Job Complete] | Displays the summary of the completed job  
For software distribution jobs, the summary contains details about the device, image type, running image name, upgrade image name, upgrade storage location, and image distribution status.  
For software import jobs, the summary contains details about device, image name, storage location, and import status of the image.
  
The Job Summary is not generated for Image Out-Of-Sync Report job. |
Understanding User-supplied Scripts

User-supplied scripts are run before and after each device upgrade, for example:

- The preupgrade script can check whether the device is accessible.
- The preupgrade script can check whether any users are connected to the access server. If the script finds that some users are connected, it can decide whether to disable the connections before upgrading.
- The post-upgrade script can check whether the upgrade was successful. Depending on the return value, Software Management either halts or continues with the rest of the upgrade.

The following sections contain:

- Script Requirements
- Script Parameters
- Sample Script

Script Requirements

- In the Edit Preferences dialog box (Admin > Network > Software Image Management > View/Edit Preferences), enter:
  - Enter the shell scripts (*.sh) on UNIX and batch files (*.bat) on Windows.
    - On UNIX, the scripts should have read, write, and execute permissions for the owner (casuser) and read and execute permissions for group casusers. That is, the script should have 750 permission.
    - On Windows, the script should have read, write, and execute permissions for casuser/Administrator.
    - The other users should have only read permission. You must ensure that the scripts contained in the file has permissions to execute from within the casuser account.
  - The script files must be available at this location:
    - On Solaris and Soft Appliance:
      /var/adm/CSCOpx/files/scripts/swim
    - On Windows:
      NMSROOT\files\scripts\swim
  - User script timeout
    - Software Management waits for the time specified before concluding that the script has failed.
- Software Management verifies that:
  - The script has write and execute permissions for the user casuser.
  - Only users logged in as Administrator, root, or casuser have write and execute permissions.

⚠️ Caution

The script should not write output to the system console. The script can write the output to a file. Writing the script output to the system console can cause the Software Management job to hang.
Script Parameters

Software Management passes a parameter indicating whether the script is running before or after the upgrade. If the script does not intend to perform any pre-upgrade check, the script can return an exit value of zero and perform checks in the post-upgrade. See the Sample Script for reference.

The parameters provided to the script by Software Management are in the form of environment variables. The server environment variables such as PATH, SystemRoot, etc., are not passed on to the script by Software Management. You have to set the relevant environment variables within the script. See the Sample Script for reference.

See Adding Devices to the Device and Credential Repository section in the Inventory Management with Cisco Prime LAN Management Solution 4.2 for further information on device hostname, device name (device name), SNMP v2 community strings, etc.

The different parameters are described in the table below:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM_SCRIPT_CONTEXT</td>
<td>This variable is used to determine if the script has to be invoked before or after image upgrade. If you set the variable to,</td>
</tr>
<tr>
<td></td>
<td>• PRE-DOWNLOAD—Script is invoked by Software Management prior to image upgrade.</td>
</tr>
<tr>
<td></td>
<td>• POST-DOWNLOAD—Script is invoked by Software Management post image upgrade.</td>
</tr>
<tr>
<td>NMSROOT</td>
<td>LMS installed directory.</td>
</tr>
<tr>
<td>TMPDIR</td>
<td>Directory provided to LMS to create temporary files.</td>
</tr>
<tr>
<td>CRM_DEV_NAME</td>
<td>Name of Device Name as entered in Device and Credential Repository.</td>
</tr>
<tr>
<td>CRM_SNMP_V2_RWCOMMUNITY</td>
<td>SNMP version 2 read-write community string.</td>
</tr>
<tr>
<td>CRM_SNMP_V2_ROCOMMUNITY</td>
<td>SNMP version 2 read only community string.</td>
</tr>
<tr>
<td>CRM_SNMP_V3_ENGINE_ID</td>
<td>SNMP version 3 Engine ID</td>
</tr>
<tr>
<td>CRM_SNMP_V3_USER_ID</td>
<td>User ID configured for SNMP version 3 protocol access on the device.</td>
</tr>
<tr>
<td>CRM_SNMP_V3_PASSWORD</td>
<td>SNMP version 3 password for the user ID.</td>
</tr>
<tr>
<td>CRM_ENABLE_PASSWORD</td>
<td>Enable password.</td>
</tr>
<tr>
<td>CRM_PRIMARY_USERNAME</td>
<td>Primary user name configured on the device.</td>
</tr>
<tr>
<td>CRM_PRIMARY_PASSWORD</td>
<td>Primary password configured on the device.</td>
</tr>
<tr>
<td>CRM_DEV_MGMT_IP_ADDR</td>
<td>IP address provided in Device and Credential Repository for management.</td>
</tr>
</tbody>
</table>
Understanding User-supplied Scripts

Sample Script
The sample script illustrates how to use this option before the upgrade to see if the device is accessible and after the upgrade to see whether it was successful.

The sample.bat file contains:

c:\progra~1\cscopx\bin\perl c:\progra~1\cscopx\files\scripts\swim\samplescript.pl

The samplescript.pl file contains:

```perl
#!/usr/bin/perl
BEGIN {
    use lib "$ENV{NMSROOT}/objects/perl5/lib/Net";
}
use Net::Telnet;
#my $output="";
## The following Environment variables are not passed on by Software Image Management
## Need to set these variables for the script to work as expected
$ENV{'Path'}="C:\PROGRA~1\CSCOpx\MDC\tomcat\bin;C:\\PROGRA~1\CSCOpx\MDC\Apache;C:\\PROGRA~1\CSCOpx\MDC\jre\bin;C:\\ PROGRA~1\CSCOpx\MDC\bin;c:\cscopx\bin;C:\WINNT\system32;C:\WINNT;C:\WINNT\System32;C:\Program Files\Common Files\Adaptec Shared\\System;c:\progra~1\cscopx;c:\progra~1\cscopx\bin;;
$ENV{'TMP'}=$ENV{'TMPDIR'};
$ENV{'SystemRoot'}="C:\WINNT";

#### Required Environment variables are set #######
my $prmptchar = '/>/i';
$filename = $ENV{'CRM_DEV_NAME'} . '.txt';
if ($ENV{'CRM_SCRIPT_CONTEXT'} eq 'PRE-DOWNLOAD') {
    open OUTFILE, " > $filename" or die "Can't open file";
    print OUTFILE %ENV;
    my $host = $ENV{'CRM_DEV_MGMT_IP_ADDR'};
    my $pwd = $ENV{'CRM_PRIMARY_PASSWORD'};
    print OUTFILE $host;
    print OUTFILE $pwd;
    $telnet = new Net::Telnet(Input_Log=>"inp.txt");
    $prev = $telnet->host($host);
    print OUTFILE $prev;
    print OUTFILE "Connecting to Host....";
    $telnet->open($host);
    print OUTFILE "Connected ...";
    $telnet->dump_log("dmp.txt");
    $telnet->waitfor(’/Username: $/i’);
    $telnet->print($ENV{'CRM_PRIMARY_USERNAME'});
    $telnet->waitfor(’/Password: $/i’);
    $telnet->print($pwd);
    print OUTFILE "Password sent";
    ($output) = $telnet->waitfor('/#$/i');
    print OUTFILE "Returned after waitfor";
    print OUTFILE $output;
    $telnet->print('terminal length 0');
    $telnet->waitfor('/#$/i');
    $telnet->print('sh ver');
    ($output) = $telnet->waitfor('/#$/i');
    print OUTFILE $output;
    ### If the device is not running the expected Image, return 1
    ### so that Software Image Management application does not proceed.
    if ($output =~ m/Version 12.2\(27\)/) {
        print OUTFILE "Required Software running on Device, Allow to proceed with Upgrade\n"
```
else {
    print OUTFILE "Upgrade stopped, Device not running desired Image";
    close OUTFILE;
    exit(1);
}

else {
    print OUTFILE "Upgrade stopped, Device not running desired Image";
    close OUTFILE;
}

## A return value of zero(0) allows the Software Image Management application to proceed
exit(0);

if ($ENV{'CRM_SCRIPT_CONTEXT'} eq "POST-DOWNLOAD") {
    my $hostnew = $ENV{'CRM_DEV_MGMT_IP_ADDR'};
    my $pwdnew = $ENV{'CRM_PRIMARY_PASSWORD'};
    open OUTFILE, ">>$filename" or die "Can't open file";
    print OUTFILE "======== POST DOWNLOAD RESULTS =========";
    $telnet = new Net::Telnet(Input_Log=>'inp1.txt');
    $telnet->dump_log("dmpo.txt");
    $telnet->open($hostnew);
    $telnet->waitfor('/Username: $/i');
    $telnet->print($ENV{'CRM_PRIMARY_USERNAME'});
    $telnet->waitfor('/Password: $/i');
    $telnet->print($pwdnew);
    ($opt) = $telnet->waitfor('/#$/i');
    $telnet->print('terminal length 0');
    $telnet->waitfor('/#$/i');
    $telnet->print('sh ver');
    ($opt) = $telnet->waitfor('/#$/i');
    if ($opt =~ m/Version 12.3\(10a\)/) {
        print OUTFILE "Required Software running on Device, Upgrade Successful\n";
    }
    print OUTFILE $opt;
    close OUTFILE;
    exit(0);
}

### Locating Software Management Files

This table shows the locations of some of the Software Management directories and log files that describe what is happening in the system.

<table>
<thead>
<tr>
<th>Contents</th>
<th>Operating System</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Management User Interface/job creation debug log file</td>
<td>Solaris and Soft Appliance</td>
<td>/var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>Software Management job execution debug log files.</td>
<td>Windows</td>
<td>NMSROOT\log\swim_debug.log</td>
</tr>
<tr>
<td>You can set the debug mode for Software Management application in the Log Level Settings dialog box (Admin &gt; System &gt; Debug Settings &gt; Config and Image Management Debugging Settings)</td>
<td>Solaris and Soft Appliance</td>
<td>/var/adm/CSCOpx/files/rme\jobs\swim\job-id\swim_debug.log</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
<td>NMSROOT\files\rme\jobs\swim\job-id\swim_debug.log</td>
</tr>
</tbody>
</table>

Where NMSROOT is the LMS installed directory.
Locating Software Management Files
Virtual Switching System Support

Virtual Switching technology is the process of combining two standalone distribution switches found in the local distribution layer into a single management point.

The Virtual Switching System functions and appears as a single switch to the wiring closet and the core layer. You can also create Virtual Switching Systems with a pair of standalone switches available in the core layer.

After the conversion of two distribution switches into one Virtual Switching System, the wiring closet switch creates a port bundle to the Virtual Switching System.

Creating a port bundle allows you to manage Standalone switches, easily because the port bundle has to manage only a single virtual port to the Virtual Switching System.

This Virtual Switching technology is implemented in LAN Management Solutions (LMS) by providing a Virtual Switching System Configuration Tool.

This GUI based conversion tool allows you to select two compatible standalone switches and guides you in converting those standalone switches into one Virtual Switching System.

During the conversion process, the Virtual Switching System Configuration tool generates the required CLI commands, based on your inputs. The process then pushes this configuration to the devices using the protocol order provided in Admin > Collection Settings > Config > Config Transport Settings.

This chapter contains:

- Prerequisites for Conversion
- Virtual Switching System Configuration Process
- Support for Virtual Switching Systems
- Converting Switches from Virtual to Standalone Mode

Note

Only VSS-capable standalone Cisco Catalyst 6000 switches can be converted into a Virtual Switching System.
Prerequisites for Conversion

Before you convert Standalone switches to a Virtual Switching System, you must ensure that:

- Candidate devices that are to be converted to a Virtual Switching System are managed by LMS so that they can use this conversion tool.
- Fresh Inventory and Config Collection has been carried out.
- Only VSS-capable IOS Software Modularity images are running on the Standalone switches.

Virtual Switching System Configuration Process

Two Standalone distribution switches can be converted into a single Virtual Switching System by using the Virtual Switching System Configuration Tool available in LMS. This process of converting to Virtual Switching Systems can also be done for core layer switches.

Before proceeding with conversion, ensure that the prerequisites are met.

For more information, see Prerequisites for Conversion.

To convert standalone switches to a Virtual Switching System:

1. Select Devices for VSS Configuration
2. Perform Hardware Checks on the Devices
3. Perform Software Compatibility Checks on the Two Devices
4. Generate Compliance Report
5. Define Configuration Parameters
6. Deploy Commands on the Two Switches to Enable VSS Mode

Select Devices for VSS Configuration

You need to select two switches and convert them into one Virtual Switching System. Only VSS-capable Standalone devices can be converted to Virtual Switching System.

The Virtual Switching System Configuration Tool consists of a customized device selector. This device selector displays only VSS-capable devices with their sysObjectIDs.

Perform Hardware Checks on the Devices

After you select two devices, sequential hardware checks are carried out by the Virtual Switching System Configuration tool on these two devices to ensure hardware compliance.

The hardware checks carried out are:

- RAM size check
  - The RAM sizes in MB of both the devices are compared.
  - If you try to convert one device with 450 MB RAM and another device with 512 MB RAM into a Virtual Switching System, a warning message is displayed. However, you are allowed to proceed with the conversion.

- Supervisor Type check
  - The Supervisor types of both the devices are compared. You cannot convert one device with Supervisor4 and another device with Supervisor3 into a Virtual Switching System. Only Supervisor4 is supported for VSS Configuration.
Virtual Switching System Configuration Process

Chapter 10      Virtual Switching System Support

Perform Software Compatibility Checks on the Two Devices
After the hardware compatibility check is done, the selected devices undergo a software compatibility check.

The software compatibility checks are:

- Switch mode check
  Check whether both devices are in standalone non-VSS modes.
  You cannot convert a Standalone switch and a Virtual-mode configured switch into a Virtual Switching System.

- IOS Software Modularity Image check
  Both devices must be running VSS-capable IOS Software Modularity images in native IOS mode.
  An image is considered VSS-capable if it has SXH as the last three characters of the image name.

  Example
  The image, 12.2(99)SXH is considered VSS-capable because it has SXH as the last three characters of the image name.

Generate Compliance Report
After the hardware and software compatibility checks have been completed, a Compliance report is generated. This report indicates the various attributes considered for the checks and the status of the checks.

If there are any instances of non-compliance, you need to restart the conversion process to address these non-compliances.

You are allowed to proceed to the next step only if both hardware and software compatibility checks are successful.

For example:
If the devices do not comply with the minimum IOS software image version, you need to upgrade the software images in the two devices to the minimum recommended version.

A link is provided to the software image upgrade page along with the compliance report, if the minimum software requirement is not met. You can use this link to upgrade the software images in the devices to the minimum IOS software image version.

Define Configuration Parameters
When the devices are made compliant with the hardware and software compatibility checks, you need to define configuration parameters for both the devices.

The configuration definition includes:

- Specifying the Domain number for the Virtual Switching System configuration
- Assigning one switch as the Active switch and the other as the Standby switch
- Entering the Switch Priority value for both switches
Chapter 10  Virtual Switching System Support

Virtual Switching System Configuration Process

- Entering the Port Channel numbers for both switches
- Selecting 10 Gigabit Ethernet Interfaces for both switches.

**Deploy Commands on the Two Switches to Enable VSS Mode**

After you have defined the configuration parameters, the Conversion Work Order page is displayed. This page lists the various CLI commands that you must download to the two devices. The CLI commands convert the switches into a Virtual Switching System.

These CLI commands are generated by the Virtual Switching System Configuration tool. You need to deploy the CLI commands on the devices.

LMS uses various protocols such as Telnet, SSH, RCP, SCP, and TFTP to deploy the commands on the devices. The protocols are tried out in the order specified in LMS. If the first protocol in sequence cannot log into the device, the next protocol in the order is tried out, until a suitable protocol is found.

For more information on how to change the protocol order, see *Administration of Cisco Prime LAN Management Solution 4.2*.

The devices reboot after the CLI commands have been deployed on them. One switch is transformed to function as an Active switch and the other as a Standby switch.

After successful conversion, the running configuration of the VSS setup is copied to its startup configuration. The individual switches are then moved to the Suspended state in LMS.

The new Virtual Switching System is added to Device Credentials Repository (DCR) with the device name, same as the IP Address of the Active switch followed by _VSS.

**Note**

After conversion, irrespective of whether an Active or Standby switch boots up first, the conversion to Virtual Switching System takes place successfully. The IP address of the Active device is added to DCR.
Converting Switches from Standalone to VSS Mode

LAN Management Solution (LMS) provides support for Virtual Switching Systems.

You can use the Virtual Switching System Configuration Tool to convert VSS-capable Standalone switches to a Virtual Switching System. This GUI-based tool is a wizard that guides you through the conversion process.

Before you start converting Standalone switches to a Virtual Switching System, you need to ensure that the prerequisites are met.

For more information, see Prerequisites for Conversion.

To convert Standalone switches to a Virtual Switching System:

**Step 1** Select **Configuration > Workflows > Virtual Switching System > VSS Conversion**.

The Virtual Switching System Mode Conversion dialog box appears.

**Step 2** Select two Standalone switches that are VSS-compliant from the Device Selector to convert to a Virtual Switching System.

The device selector is customized to display only Standalone switches that are VSS-compliant.

**Step 3** Click **Convert to VSS Mode**.

- If the switches are compatible, the Checking the Hardware and Software Requirements dialog box appears.
- If the switches are not compatible, an error message is displayed and the conversion is terminated. In this case, you must restart the conversion after making the switches hardware and software compatible.

For more information on the hardware and software checks, see Table 10-1.

**Table 10-1 Hardware and Software Check**

<table>
<thead>
<tr>
<th>Properties</th>
<th>Device 1</th>
<th>Device 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware Checks</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor Type</td>
<td>The Supervisor type for Device 1.</td>
<td>The Supervisor type for Device 2.</td>
</tr>
<tr>
<td>Modules not supported in</td>
<td>Names of modules in Device 1 that do not</td>
<td>Names of modules in Device 2 that do not</td>
</tr>
<tr>
<td>VSS mode</td>
<td>support VSS mode.</td>
<td>support VSS mode.</td>
</tr>
<tr>
<td>Physical Connectivity</td>
<td>The IP Address through which Device 1 is</td>
<td>The IP Address through which Device 2 is</td>
</tr>
<tr>
<td></td>
<td>connected.</td>
<td>connected.</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Status of hardware check.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Software Checks</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Properties</td>
<td>Device 1</td>
<td>Device 2</td>
</tr>
<tr>
<td>VSS Mode</td>
<td>The current mode of Device 1.</td>
<td>The current mode of Device 2.</td>
</tr>
<tr>
<td>Image Version</td>
<td>The software image version in Device 1</td>
<td>The software image version in Device 2.</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Status of software check.</td>
<td></td>
</tr>
</tbody>
</table>
When the RAM size of both the devices are not equal, a warning message is displayed. However, you will be allowed to continue with the conversion.

**Step 4**  Click Next.

The Define Configuration Parameters dialog box appears.

**Step 5**  Enter the required information as shown in Table 10-2

<p>| Table 10-2  Define Configuration Parameters |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Switching System Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Enter Domain Number</td>
<td>Domain number to be used by the Virtual Switching System, which can be any number between 1 to 255. This domain number is common for both the switches.</td>
</tr>
<tr>
<td><strong>Device Name: 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Select Switch Number | Either  
  - Check Switch No.1 if you want to assign Device 1 as Switch No. 1.  
  Or  
  - Check Switch No.2 if you want to assign Device 1 as Switch No. 2.  
  You cannot assign both Device1 and Device 2 as Switch No.1. If Device 1 is assigned Switch No.1 then Device 2 should be assigned as Switch No.2.  
  The configuration of the switch designated as No. 2 is overwritten by the configuration of the switch designated as No. 1.  
  The first switch becomes the Active Switch and the second switch becomes the Standby Switch. |
| Enter Switch Priority | Switch Priority number to be used by the Virtual Switching System, which can be any number between 1 and 255. The switch with the higher value becomes the Active Switch and the other switch becomes the Standby Switch. The priority value should not be the same for both switches. |
| Enter Port Channel Number | Port Channel for Device 1. Enter a number between 1 and 255. The Port channel number must be different for each switch. |
Table 10-2 Define Configuration Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Select Interface | Interface for Device 1. Select the interface for the device from the list box that displays the 10 Gigabit Ethernet interfaces. A minimum of one interface must be selected for the device. Use the Control Key to select more than one interface. Only VSS-capable 10 Gigabit line cards are displayed. Interface modules for Supervisor 4, 6708 10 Gigabit and 6716 10 Gigabit interfaces are available for selection. For 6716 10 Gigabit type cards, only four interfaces are displayed for selection. For example, if there is a 6716 10 Gigabit card in the device, only the following four interfaces (1, 5, 9, 13) are displayed:  
  • TenGigabitEthernet <module number>/1  
  • TenGigabitEthernet <module number>/5  
  • TenGigabitEthernet <module number>/9  
  • TenGigabitEthernet <module number>/13  
Where <module number> is the module number of the Gigabit card. For example, TenGigabitEthernet 6/1, where 6 is the module and 1 is the interface. The number of interfaces selected must be the same for both devices. |

Device Name: 2

| Select Switch Number | Either:  
  • Check Switch No.1 if you want to assign Device 2 as Switch No. 1.  
  Or  
  • Check Switch No.2 if you want to assign Device 2 as Switch No. 2.  
You cannot assign both Device 1 and Device 2 as Switch No.1. If Device 1 is assigned Switch No.1 then Device 2 should be assigned as Switch No.2. The configuration of the switch designated as No. 2 is overwritten by the configuration of the switch designated as No. 1. The first switch becomes the Active Switch and the second switch becomes the Standby Switch. |

Enter Switch Priority | Switch Priority number to be used by the Virtual Switching System, which can be any number between 1 and 255. The switch with higher value becomes the Active Switch and the second switch becomes the Standby Switch. The priority value should not be the same for both switches. |
Chapter 10      Virtual Switching System Support

Virtual Switching System Configuration Process

Table 10-2     Define Configuration Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Port Channel</td>
<td>The Port channel for Device 2. Enter a port channel number for the switch between 1 and 255. The Port channel number must be different for each switch.</td>
</tr>
</tbody>
</table>
| Select Interface       | The Interface for Device 2. This list box lists the 10 Gigabit Ethernet interfaces. Select the interface for the device from the list box. At least one interface must be selected for the device. Use the Control Key to select more than one interface. Only VSS capable 10 Gigabit line cards are displayed. Interface modules for Supervisor 4, 6708 10 Gigabit and 6716 10 Gigabit cards are available for selection. For 6716 10 Gigabit type cards, only four interfaces are displayed for selection. For example, if there is a 6716 10 Gigabit card in the device, only the following four interfaces (1, 5, 9, 13) are displayed:  
  • TenGigabitEthernet <module number>/1  
  • TenGigabitEthernet <module number>/5  
  • TenGigabitEthernet <module number>/9  
  • TenGigabitEthernet <module number>/13  
Where <module number> is the module number of the Gigabit card. For example, TenGigabitEthernet 6/1, where 6 is the module and 1 is the interface. The number of interfaces selected must be the same for both devices. |

Step 6  Click **Next**. The Work Order page appears with the CLI commands that need to be downloaded to each of the switches so that they can be converted into one Virtual Switching System.

Step 7  Click **Finish**.  
  • If the conversion was completed, a message is displayed that the two switches have been converted to a single Virtual Switching System.  
  • If the conversion failed, an error message is displayed indicating the reason for failure. The reason could be that the CLI commands were not properly deployed on the devices.

Note  You cannot set priorities for the two Standalone switches that are considered for VSS conversion. Both the Standalone switches have equal priority by default.
Support for Virtual Switching Systems

The various applications in LMS such as Syslog, Inventory Management, Reporting, Software Management, and Configuration Management provide support for Virtual Switching Systems. The implication of Virtual Switching System support for these applications is discussed below:

- Inventory Management
- Configuration Management
- Syslog
- Software Management - Software Distribution
- Software Management - Scheduling a Software Distribution Job

Inventory Management

The Virtual Switching System is considered as a single switch by Inventory. However Inventory collection happens for both switches.

You can generate a Detailed Device Report for the Virtual Switching System. The output of this report consists of information on both the Active and the Standby switches.

For more information on how to generate a Detailed Device Report, see Reports Management with Cisco Prime LAN Management Solution 4.2.

Configuration Management

After the conversion, the Virtual Switching System will have a single unified configuration. Configuration management provides support for Virtual Switching Systems by managing the configuration of the switch.

You can use Configuration Management to:

- Archive the device configurations
- Determine out-of-sync configuration files
- View the configuration version tree
- Compare the revisions of configurations
- Compare the archived configuration with a baseline template
- Deploy a version of configuration on the device

For more information on Configuration Management, see Archiving Configurations and Managing them using Configuration Archive.

You can also use NetConfig and Config Editor to configure Interfaces on a VSS device.

For more information on using NetConfig and Config Editor, see:

- Making and Deploying Configuration Changes Using NetConfig
- Editing and Deploying Configurations Using Config Editor
Syslog

The Syslog messages are sent from the Active switch of the Virtual Switching System to the LMS server. These messages are treated like any other Syslog message from any other device type. Syslog reports can be generated for the Syslogs received from the Active switch of the Virtual Switching System.

For information on Syslogs, see *Administration of Cisco Prime LAN Management Solution 4.2*.

Software Management - Software Distribution

Software Management is enhanced to support distribution of software images to a Virtual Switching System. Software Management uses Master Chassis - Active Supervisor for software distribution.

Software Distribution through LMS Software Management varies based on the software image or Patch image considered for distribution.

- **Distribution of the Base Image**
  
  Distributing the software Base image consists of:
  
  a. Copying the new software image to the Master switch, Flash storage partition.
  
  b. Copying the same software image to the corresponding slave switch Flash storage partition.
     
     If Master Flash storage is `disk0` the software image will be copied to `slave-disk0` Flash storage of the Slave switch.
  
  c. Loading the Active switch.
  
  d. Loading the Slave switch.
  
  e. Activating the software image on both the Flash storages.
  
  f. Rebooting the Master switch.

- **Distribution of Patch image**
  
  Distribution of software base image consists of:
  
  a. Copying of the new patch image to the Master switch, Flash storage partition.
  
  b. Copying the same Patch image to the corresponding Slave switch, Flash storage partition.
     
     If Master Flash storage is `disk0`, the Patch image will be copied to `slavedisk0` Flash storage of the Slave switch.
  
  c. Loading the Active switch.
  
  d. Loading the Slave switch.
  
  e. Activating the Patch image on both the Flash storages.
     
     You are allowed to reload the device to activate the Patch images, only if you have selected Reload if required option while scheduling the Patch distribution job.
     
     - When you reload, the standby Route Processor(RP) on the Slave switch is reset.
     
     - The device reboots as soon as the installed code starts running.
     
     - A manual switchover to the redundant supervisor engine for a dual processor redundant system takes place.
Chapter 10      Virtual Switching System Support

Converting Switches from Virtual to Standalone Mode

You can only distribute Patch images to a Virtual Switching System running VSS-capable IOS Software Modularity image in Install mode.

For more information on Software Distribution, see Software Distribution.

Software Management - Scheduling a Software Distribution Job

Scheduling a Software Management distribution job for Virtual Switching Systems is almost similar to that of any Standalone switch. In addition to the verifications performed by Software management, there are a few verifications that are carried out for Virtual Switching Systems.

Software management verifies:

- If VSS-capable IOS Software Modularity images are running on the devices.
  The prerequisite for VSS is that the devices should have VSS-capable IOS Software Modularity images running on them. So if you select an image that is not a VSS-capable IOS Software Modularity image, the software distribution job cannot be performed.

- If the RAM space available on the two devices are compatible.
  RAM checks are carried out only for Master switch supervisors and not for Slave switch supervisors.

- If there is an identical Slave switch storage partition with enough space for the selected Master switch storage partition.

For more information on Software Distribution, see:

- Distributing by Devices [Basic]
- Distributing by Devices [Advanced]
- Distributing by Images
- Remote Staging and Distribution
- Patch Distribution

Converting Switches from Virtual to Standalone Mode

Virtual Switching System refers to the conceptual switch that is created by converting two VSS-capable standalone switches into one switch. You can also convert Virtual Switching Systems back to Standalone switches.

To convert Virtual Switching Systems into Standalone switches:

Step 1
Locate the original configurations of the two switches.
These configurations maybe available as files on your server. If not, locate them from the Configuration Archive of LMS.

For more information on locating the configurations, see Using the Configuration Version Tree.

You can continue with this procedure even if the original configuration files are not available. You can manually reconfigure the individual switches, if required.
Step 2  Back up the current VSS setup configuration.
This configuration may be required for future conversions.

Step 3  Connect to the VSS setup using Telnet and:

a. Remove all the loop back interfaces on the VSS.
   Run the command `no loopback` for each loop back address on the switch.
   This removes the loop back addresses from the switch.

b. Go to the running configuration of the VSS setup and configure the IP address on the physical
   interface of the Standby switch.
   This IP address must be in a subnet that is not the physical interface of the Active switch.
   After the IP address is configured on the physical interface, the Standby chassis is accessible
   through the management IP address.

c. Save this configuration change by running the `write mem` command.
   The configuration is saved to the NVRAM of the corresponding device.

d. Run the command `switch convert mode stand-alone` in Enable mode.
   This command will reload the Active switch and release the switch from VSS setup.

Step 4  Connect to the VSS setup using Telnet. You must use the IP address configured in Step 3b.

Step 5  Run the command `switch convert mode stand-alone` in Enable mode.
The switches are now in Standalone mode. You can access them using their own management addresses.

Step 6  Either:

- Add the two devices to the DCR of LMS, if they do not exist there. To do this select Inventory >
  Device Administration > Add / Import / Manage Devices.

Or

- Change the device states if the devices are in Suspended state. This change allows the two devices
  to be managed again by LMS.

Note  Alternatively, you can refer to the VSS Reverse Conversion wizard for the procedures for converting
Virtual Switching Systems to Standalone switches. To access the wizard, go to Configuration >
Workflows > Virtual Switching System > VSS Reverse Conversion.
Use Case: Converting Standalone Switches into a Virtual Switching System

Case:
You are a network administrator and you want to convert two standalone switches into a Virtual Switching System by using the Virtual Switching System Configuration Tool available in LMS.

Solution:
To convert Standalone switches to a Virtual Switching System:

Step 1 Select **Configuration > Workflows > Virtual Switching System > VSS Conversion**.
The Virtual Switching System Configuration dialog box appears.

Step 2 Select 10.77.118.242 and 10.77.118.242_alias, two Standalone switches that are VSS-compliant, from the Device Selector to convert to a Virtual Switching System.

Step 3 Click **Convert to VSS Mode**.
You can view the hardware and software check results.

Step 4 Click **Next**.
The Define Configuration Parameters dialog box appears.

Step 5 Enter the required information in the Define Configuration Parameters dialog box.

Step 6 Click **Next**.
The Work Order page appears with the CLI commands that need to be downloaded to each of the switches so that they can be converted into one Virtual Switching System.

Step 7 Click **Finish**.
A message is displayed that the two switches have been converted to a single Virtual Switching System.

After successful conversion, the running configuration of the VSS setup is copied to its startup configuration. The individual switches are then moved to the Suspended state in LMS.

The new VSS switch is added to the Device Credentials Repository (DCR) with the display name, same as the IP address of the Active switch followed by _VS

So, the IP address of the Virtual Switching System is **10.77.118.242_VSS**
Use Case: Converting Standalone Switches into a Virtual Switching System
Configuring VLAN

LMS collects data about devices so that you can configure and manage Virtual Local Area Network (VLAN) in your network. You must set up your LMS server properly to ensure that Data Collection is successfully performed in your network.

The configuration module in LMS helps you to manage your VLANs. You can configure and manage VLAN, Private VLAN (PVLAN), Trunk, and also assign ports to VLANs.

This chapter contains:

- Understanding Virtual LAN (VLAN)
- Using VLANs
- Configuring VLANs
- Creating Ethernet VLANs
- Configuring Token Ring VLANs
- Interpreting VLAN Summary Information
- Understanding Private VLAN
- Using Private VLAN
- Understanding Inter-VLAN Routing
- Using Inter-VLAN Routing
- VLAN Trunking Protocol
- Understanding Trunking
- EtherChannel
- VLAN Port Assignment
- Using VLAN Port Assignment
- Usage Scenarios for Managing VLANs
Understanding Virtual LAN (VLAN)

A VLAN allows you to create logical broadcast domains that can span across a single switch or multiple switches, regardless of physical positioning. A VLAN contains a group of devices on one or more LANs. These devices are configured in such a way that they can communicate as if they were all on the same network segment. VLANs are based on logical connections instead of physical connections, and hence they are extremely flexible.

VLAN allows you to group ports on a switch to limit unicast, multicast, and broadcast traffic flooding. Flooded traffic originating from a particular VLAN is only flooded out to other ports belonging to that VLAN. This helps to reduce the size of broadcast domains and it allows groups or users to be logically grouped without being physically located in the same place.

The following topics are covered in this section:

- Advantages of VLANs
- VLAN Components
- Using VLANs

Advantages of VLANs

VLANs provide the following advantages:

- Simplification of Adds, Moves, and Changes
- Controlled Broadcast Activity
- Workgroup and Network Security

Simplification of Adds, Moves, and Changes

Adds, moves, and changes are some of the greatest expenses in managing a network. Many moves require re-cabling and almost all moves require new station addressing and hub and router re-configuration.

VLANs simplify adds, moves, and changes. VLAN users can share the same network address space regardless of their location.

If a group of VLAN users move but remain in the same VLAN connected to a switch port, their network addresses do not change.

If a user moves from one location to another but stays in the same VLAN, the router configuration does not need to be modified.

Controlled Broadcast Activity

Broadcast traffic occurs in every network. Broadcasts can seriously degrade network performance or even bring down an entire network, if the network is not properly managed.

Broadcast traffic in a particular VLAN is not transmitted outside that VLAN. This substantially reduces overall broadcast traffic, frees bandwidth for real user traffic, and lowers the vulnerability of the network to broadcast storms.
You can control the size of broadcast domains by regulating the size of their associated VLANs and by restricting both the number of switch ports in a VLAN and the number of people using the ports.

You can also assign VLANs based on the application type and the amount of application broadcasts. You can place users sharing a broadcast-intensive application in the same VLAN group and distribute the application across the network.

**Workgroup and Network Security**

You can use VLANs to provide security Firewalls, restrict individual user access, flag any unwanted network intrusion, and control the size and composition of the broadcast domain.

You can:

- Increase security by segmenting the network into distinct broadcast groups.
- Restrict the number of users in a VLAN.
- Configure all unused ports to a default low-service VLAN.

**VLAN Components**

The VLAN components are:

- Switches that logically segment the end stations connected to it.

  Switches are the entry point for end-station devices into the switched domain and provide the intelligence to group users, ports, or logical addresses into common communities of interest. LAN switches also increase performance and dedicated bandwidth across the network.

  You can group ports and users into communities using a single switch or connected switches. By grouping ports and users across multiple switches, VLANs can span single-building infrastructures, interconnected buildings, or campus networks.

  Each switch can make filtering and forwarding decisions by packet and communicate this information to other switches and routers within the network.

- Routers that extend VLAN communication between workgroups.

  Routers provide policy-based control, broadcast management, and route processing and distribution. They also provide the communication between VLANs and VLAN access to shared resources such as servers and hosts.

  Routers connect to other parts of the network that are either logically segmented into subnets or require access to remote sites across wide area links.

- Transport protocols that carry VLAN traffic across shared LAN.

  The VLAN transport enables information exchange between interconnected switches and routers on the corporate backbone. This backbone acts as the aggregation point for large volume of traffic.

  It also carries end-user VLAN information and identification between switches, routers, and directly attached servers. Within the backbone, high-capacity links with high-bandwidth carry the traffic throughout the enterprise.
Using VLANs

You can use Configuration Management functionality in LMS to create, modify, and delete VLANs. You can use the Topology Services to create Ethernet VLANs.

LMS allows you to modify most of the VLAN characteristics that were entered when you created the VLAN, such as purpose, description, and LANE services.

The following sections brief on the types of VLANs supported by Topology Services:

- Ethernet VLAN (See Ethernet VLANs)
- Private VLANs (See Understanding Private VLAN)

Configuring VLANs

You can configure VLANs using VLAN Configuration wizard.

Creating VLAN

To create VLANs, the VLAN Configuration wizard directs you through:

1. Selecting Devices or Entities
2. Creating VLANs
3. Assigning Ports to VLANs
4. Disallowing VLAN on Trunks
5. Understanding VLAN Creation Summary

Deleting VLAN

To delete VLANs, the VLAN Configuration wizard directs you through:

1. Deleting VLANs
2. Moving Affected Ports to New VLAN
3. Understanding VLAN Deletion Summary
Selecting Devices or Entities

You must select the devices or entities to be included in the VLAN. Domain Selector helps you to select devices in Switch Clouds and VTP Domains.

To select devices or entities for a VLAN:

---

**Step 1**
Select **Configuration > Workflows > VLAN > Configure VLAN.**

The VLAN Configuration page appears.

**Step 2**
Select the devices using the Device Selector or the Domain Selector from the VLAN Configuration dialog box. See Table 11-1

**Table 11-1 VLAN Configuration Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Selector | Lists all the devices in your network.  
|              | Click the radio button to select the Device Selector.                        |
| Domain Selector | Lists the Switch Clouds and VTP Domains in your network.  
|              | Click the radio button to select the Domain Selector.                        |
| All          | Click **All** to view all the devices in the network. Check the checkboxes to select the devices. |
| Selection    | Displays the devices that you have selected in the **All** pane.             |

**Step 3**
Either:

a. Click **Create** to create VLANs.
   The Create VLAN page appears.

b. Go to **Creating VLANs.**

Or

a. Click **Delete** to delete the VLANs.
   The Select VLAN to Delete page appears.

b. Go to **Deleting VLANs.**
Creating VLANs

After you select devices using the Device Selector or the Domain Selector and click Create in the VLAN Configuration page, the Create VLAN page appears. For more details, see Selecting Devices or Entities. You must enter the details as described in the Table 11-2.

Table 11-2 Create VLAN Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Name</td>
<td>Enter a name for the new VLAN.</td>
</tr>
<tr>
<td>VLAN Index</td>
<td>Enter a number to identify the VLAN. You can enter a number within the range:</td>
</tr>
<tr>
<td></td>
<td>- 2 to 1001</td>
</tr>
<tr>
<td></td>
<td>- 1025 to 4094</td>
</tr>
<tr>
<td></td>
<td>You cannot enter 1 or a number in the range 1002 to 1024, as the VLAN Index. These are reserved numbers.</td>
</tr>
<tr>
<td>Create on all transparent switches</td>
<td>Check the checkbox to include all switches that are VTP transparent. VTP transparent switches do not send VTP updates and do not act on VTP updates received from other switches. This checkbox is available only for VTP domain based VLAN creation. For more details on this, see Creating VLANs on Transparent Devices.</td>
</tr>
<tr>
<td>Copy running to start-up config</td>
<td>Check the checkbox to copy the running configuration to the start-up configuration.</td>
</tr>
</tbody>
</table>

Click any of the following:

- **Next** to continue.
  - The Assign Ports to VLAN page appears. For details, see Assigning Ports to VLANs.
  - Assigning ports to VLANs cannot be done for more than 100 devices at a time, since it results in memory issues. If you have selected more than 100 devices, click Finish to save VLAN creation. Do VLAN port assignment for 100 devices at a time.

- **Cancel** to exit.
- **Finish** to save changes.
  - VLANs are created on the specified devices and the initial VLAN Configuration page appears.
Creating VLANs on Transparent Devices
When you create VLANs without checking the *Create On All Transparent Switches* option in the VLAN creation page, the following is the behavior:

<table>
<thead>
<tr>
<th>Device Selected</th>
<th>Access and Trunk ports listed in the VLAN Creation flow</th>
<th>VLAN created on</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTPv2 Server</td>
<td>• VTPv2 Server</td>
<td>VTPv2 Server</td>
</tr>
<tr>
<td></td>
<td>• VTPv2 Client</td>
<td></td>
</tr>
<tr>
<td>VTPv3 Primary Server</td>
<td>• VTPv3 Server</td>
<td>VTPv3 Primary Server</td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Client</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Primary Server</td>
<td></td>
</tr>
<tr>
<td>VTPv2 or VTPv3 Transparent device</td>
<td>Selected Transparent device</td>
<td>Selected Transparent device</td>
</tr>
<tr>
<td>Device that has VTPv3 in Off Mode</td>
<td>Selected Off Mode device</td>
<td>Selected Off Mode device</td>
</tr>
</tbody>
</table>

When you create VLANs with the *Create On All Transparent Switches* option in the VLAN creation page, the following is the behavior:

<table>
<thead>
<tr>
<th>Device Selected</th>
<th>Access and Trunk ports listed in the VLAN Creation flow</th>
<th>VLAN created on</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTPv2 Server</td>
<td>• VTPv2 Server</td>
<td>VTPv2 Server</td>
</tr>
<tr>
<td></td>
<td>• VTPv2 Client</td>
<td>VTPv2 Transparent</td>
</tr>
<tr>
<td>VTPv3 Primary Server</td>
<td>• VTPv3 Server</td>
<td>VTPv3 Primary Server</td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Client</td>
<td>VTPv3 Transparent device</td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Primary Server</td>
<td>VTPv3 Off Mode device</td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Transparent device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Off Mode device</td>
<td></td>
</tr>
<tr>
<td>VTPv2 or VTPv3 Transparent device</td>
<td>• VTPv2 or VTPv3 Transparent device</td>
<td>VTPv2 or VTPv3 Transparent device</td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Off Mode device</td>
<td>VTPv3 Off Mode device</td>
</tr>
<tr>
<td>Device that has VTPv3 in Off Mode</td>
<td>• VTPv3 Transparent device</td>
<td>VTPv3 Transparent device</td>
</tr>
<tr>
<td></td>
<td>• VTPv3 Off Mode device</td>
<td>VTPv3 Off Mode device</td>
</tr>
</tbody>
</table>

In the above tables, VTPv2 refers to VTP version 2 and VTPv3 refers to VTP version 3.
Assigning Ports to VLANs

A VLAN created in a management domain remains unused until you assign one or more switch ports to the VLAN.

The Assign VLANs to Port page appears after you create the VLAN name and index.

To assign ports to VLANs:

---

Step 1 Select Configuration > Workflows > VLAN > Configure VLAN.
The VLAN Configuration page appears.

Step 2 Select device or domain from the VLAN Configuration page.

Step 3 Click Create.

Step 4 Enter VLAN Name and VLAN Index in the Create VLAN page and click Next.
The Assign Ports to VLAN page appears.

Step 5 Select the ports and click Next.

Table 11-3 describes the entries in the Assign Ports to VLAN page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Displays the name of the new VLAN.</td>
</tr>
<tr>
<td>Filter</td>
<td>Select any of the following criteria based on which you want to filter the list:</td>
</tr>
<tr>
<td></td>
<td>• Link</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• Device Name</td>
</tr>
<tr>
<td></td>
<td>• Device Address</td>
</tr>
<tr>
<td></td>
<td>• Port Status</td>
</tr>
<tr>
<td></td>
<td>• VLAN Index</td>
</tr>
<tr>
<td></td>
<td>• VLAN Name</td>
</tr>
<tr>
<td></td>
<td>• Association type</td>
</tr>
<tr>
<td></td>
<td>Or enter * or leave the field blank and click Filter to get all the records.</td>
</tr>
<tr>
<td>Advanced Filter</td>
<td>Click Advanced Filter to open Advanced Filter dialog box. Advanced filtering allows you to search ports using more search criteria.</td>
</tr>
<tr>
<td></td>
<td>For more details on Advanced Filter, see Advanced Filter.</td>
</tr>
</tbody>
</table>

**Column**

<table>
<thead>
<tr>
<th>Link</th>
<th>Shows whether the port is connected to a switch or not. The value can either be True or False.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Name of the port.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device to which the port belongs to.</td>
</tr>
<tr>
<td>Device Address</td>
<td>IP address of the device to which the port belongs to.</td>
</tr>
<tr>
<td>Port Status</td>
<td>Status of the port. Shows whether the port is active or down.</td>
</tr>
</tbody>
</table>
Step 6  
Click any of the following:
- **Next** to continue.  
The Disallow VLAN on Trunks page appears.
- **Back** to modify the Create VLAN page.
- **Cancel** to exit.
- **Finish** to save changes.

VLANs are created on the specified devices, selected ports are assigned to new VLAN and the initial VLAN Configuration page appears.
For more details, see **Disallowing VLAN on Trunks**.

### Advanced Filter

The Advanced Filter allows you to filter and choose the ports using various parameters and criteria, for assigning the ports to the VLAN. **Table 11-4** describes the fields in the Filter Ports Window, when you click Advanced Filter from the Assign Ports to VLAN Window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match All</td>
<td>Select the radio button to filter the ports that match all the selected parameters.</td>
</tr>
<tr>
<td>Match Any</td>
<td>Select the radio button to filter the ports that match any of the selected parameter.</td>
</tr>
</tbody>
</table>
Chapter 11      Configuring VLAN

Table 11-4  Filter Ports Field Description (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Select a parameter for which you want to filter the ports. Parameter is the attribute of a port. The values displayed for Assigning ports to VLANs are:</td>
</tr>
<tr>
<td></td>
<td>• Device Name</td>
</tr>
<tr>
<td></td>
<td>• Device Address</td>
</tr>
<tr>
<td></td>
<td>• Link</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• Port Status</td>
</tr>
<tr>
<td></td>
<td>• Port Description</td>
</tr>
<tr>
<td></td>
<td>• VLAN Index</td>
</tr>
<tr>
<td></td>
<td>• VLAN Name</td>
</tr>
<tr>
<td></td>
<td>• Association Type</td>
</tr>
<tr>
<td></td>
<td>The values displayed for Configuring Promiscuous ports are:</td>
</tr>
<tr>
<td></td>
<td>• Link</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• Device Name</td>
</tr>
<tr>
<td></td>
<td>• Device Address</td>
</tr>
<tr>
<td></td>
<td>• VLAN Name</td>
</tr>
<tr>
<td></td>
<td>• Port Mode</td>
</tr>
<tr>
<td>Criteria</td>
<td>Select the right criterion with respect to the parameter. The values are:</td>
</tr>
<tr>
<td></td>
<td>• contains</td>
</tr>
<tr>
<td></td>
<td>• begins with</td>
</tr>
<tr>
<td></td>
<td>• ends with</td>
</tr>
<tr>
<td></td>
<td>• is</td>
</tr>
<tr>
<td>Value</td>
<td>Enter a value corresponding to the parameter that you have selected.</td>
</tr>
</tbody>
</table>

Click any of the following:

- **More** to add filter.
- **Fewer** to remove filter from the existing filters.
  
  You can add or remove only one filter at a time.
- **Filter** to filter the ports based on the values for the Parameters.
Disallowing VLAN on Trunks

You can select the links on which you do not want to allow Trunking in the newly created VLAN. After you Assign the ports to the VLAN (See Assigning Ports to VLANs), the End-to-end VLAN wizard directs you to Disallow VLAN on Trunks page.

To disallow trunking on the links in your VLAN, check the checkboxes corresponding to those links, and click Next. The VLAN Creation Summary page appears.

Clicking Back takes you to the Assign Ports to VLAN page, where you can modify the port assignment. Clicking Finish saves the changes and takes you to the initial VLAN Configuration page.

For more details, see Understanding VLAN Creation Summary.

Table 11-5 describes the fields in the Disallow VLAN on Trunks page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Name</td>
<td>Name of the VLAN.</td>
</tr>
<tr>
<td>Port1</td>
<td>Port on the first device linked to the VLAN.</td>
</tr>
<tr>
<td>Device1</td>
<td>Name of the first device in the link.</td>
</tr>
<tr>
<td>Device1 Address</td>
<td>IP Address of the first device in the link.</td>
</tr>
<tr>
<td>Domain1</td>
<td>Domain to which the device belongs to.</td>
</tr>
<tr>
<td>Port2</td>
<td>Port on the second device linked to the VLAN.</td>
</tr>
<tr>
<td>Device2</td>
<td>Name of the second device in the link.</td>
</tr>
<tr>
<td>Device2 Address</td>
<td>IP Address of the second device in the link.</td>
</tr>
<tr>
<td>Domain 2</td>
<td>Domain to which the device belongs to.</td>
</tr>
</tbody>
</table>

Understanding VLAN Creation Summary

The VLAN Creation Summary page summarizes the operations that you performed through the VLAN Configuration wizard. The Summary provides the following information:

- **VTP Domain**—Lists the VTP domains.
- **Summary**—Lists different parameters that you have entered.
  - **VLAN Creation Parameters**—Lists the VLAN name and index, and the value of the parameters Create on all transparent switches and Copy running-config to startup-config.
  - **VLAN Port Assignment Parameters**—Lists the VLAN name and index, and ports to which the VLAN is assigned.
  - **VLAN Trunk Configuration Parameters**—Lists the Trunks on which the VLAN is allowed or disallowed.
**Example:**

**VLAN Creation Parameters**

- **VLAN Name:** Test
- **VLAN Index:** 912
- **Create on all transparent switches:** true
- **Copy running-config to startup-config:** true

**VLAN Port Assignment Parameters**

- **VLAN Name:** Test
- **VLAN Index:** 912
- **Operation:** Assign the VLAN to selected port(s)
- **Port:** Fa4/28
- **Device:** 10.77.209.43
- **Device Address:** 10.77.209.43

**VLAN Trunk Configuration Parameters**

- **VLAN Name:** Test
- **VLAN Index:** 912
- **Operation:** Disallow VLAN on selected Trunk(s)
- **Trunk:** 10.77.209.52:2/1 => 10.77.209.61:2/25
- **Trunk:** 10.77.210.211:2/Gi0/2 => 10.77.210.204:Gi1/0/24

Review the Summary, and click **Finish** to create the new VLAN, or click **Back** to modify the Disallow VLAN on Trunks page, or click **Cancel** to exit.

** Deleting VLANs **

You can delete the VLANs configured on the devices in your network. The VLAN Configuration wizard directs you to delete a VLAN.

**Step 1**  Select **Configuration > Workflows > VLAN > Delete VLAN.**

The VLAN Configuration page appears.

**Step 2**  Select devices or entities from the VLAN Configuration page.

For more details on selecting the devices, see Selecting Devices or Entities.
Step 3 Click **Delete**.

The Select VLAN to Delete page appears.

Table 11-6 describes the fields in the Select a VLAN to Delete dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Running Config to Start-up Config</td>
<td>Check the checkbox to copy the running configuration to start-up configuration.</td>
</tr>
<tr>
<td>Delete on all Transparent Switches</td>
<td>Check the checkbox to delete VLANs on all transparent switches. If you have created VLANs by checking Create on all transparent switches, it is mandatory that you check Delete on all Transparent Switches option to delete the VLANs created in VTP Domains.</td>
</tr>
<tr>
<td>Filter Source</td>
<td>Select the Filter type of the source:</td>
</tr>
<tr>
<td></td>
<td>• VLAN</td>
</tr>
<tr>
<td></td>
<td>• VLAN Name</td>
</tr>
<tr>
<td></td>
<td>• Domain Name</td>
</tr>
<tr>
<td></td>
<td>Or enter * or leave the field blank and click <strong>Filter</strong> to get all the records.</td>
</tr>
<tr>
<td>Select</td>
<td>Select the radio button corresponding to the VLAN you want to delete.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Index of the VLAN.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Name of the VLAN.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Name of the domain in which the VLAN belongs to.</td>
</tr>
</tbody>
</table>

Step 4 Click any of the following:

- **Next** to continue.
  
  The Move Affected Ports to New VLAN page appears. For more details, see Moving Affected Ports to New VLAN.

- **Cancel** to exit.
  
  The VLAN configuration appears.

- **Finish** to save changes.
  
  The selected VLANs are deleted from the devices. The ports in the deleted VLAN are automatically assigned to the default VLAN. The VLAN configuration page appears.
Moving Affected Ports to New VLAN

When you delete a VLAN, any port assigned to that VLAN becomes inactive. Such ports remain associated with the VLAN (and thus inactive), until you assign them to a new VLAN. You can move affected ports to a new VLAN using LMS.

You can move the ports in the VLAN you want to delete, to a new VLAN, only after you select the VLAN you want to delete. For more details on selecting a VLAN to delete, see Deleting VLANs.

To move affected ports to a new VLAN:

Step 1  Select Configuration > Workflows > VLAN > Configure VLAN.
The VLAN Configuration page appears.

Step 2  Select devices or entities from the VLAN Configuration page.
For more details on selecting the devices, see Selecting Devices or Entities.

Step 3  Click Delete.
The Select VLAN to Delete page appears.

Step 4  Select the radio button corresponding to the VLAN you want to delete and click Next.
The Move Affected Ports to New VLAN page appears.

Table 11-7, Move Affected Ports to New VLAN Page Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Affected port in the VLAN.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device to which the port belongs to.</td>
</tr>
<tr>
<td>Device Address</td>
<td>IP address of the device.</td>
</tr>
<tr>
<td>Port Status</td>
<td>Status of the port.</td>
</tr>
<tr>
<td>Connected To</td>
<td>End Host, Network Device</td>
</tr>
</tbody>
</table>

Step 5  Select the new VLAN from the Move affected ports to new VLAN drop-down menu.
If you do not select any VLAN, the affected ports are moved to the default VLAN—VLAN 1.

Step 6  Click any of the following:

- **Next** to continue.
  The VLAN Deletion Summary page appears. For more details, see Understanding VLAN Deletion Summary.
- **Back** to modify the Select VLAN to Delete page.
- **Cancel** to exit.
  The VLAN configuration appears.
- **Finish** to save changes.
  The selected VLANs are deleted from the devices. The ports in the deleted VLAN are assigned to the VLANs selected by you. The VLAN configuration appears.
Understanding VLAN Deletion Summary

The VLAN Deletion Summary page summarizes the operations that you performed through the VLAN Configuration wizard to delete the VLAN. The Summary provides the following information:

- **VLAN Deletion**—Lists the domain name, name of the VLAN that is deleted, and the VLAN ID.
- **Operation: Move the affected Ports to another VLAN**—Lists the name and ID of the new VLAN to which the ports have been moved, and lists the details of the ports including the name and IP address of the device.

**Example:**

VLAN Deletion:

```
VLAN Domain       :DMZ_10.77.209.43(T)
VLAN Deleted      :VLAN0002
VLANId            :2

------------------------------------------
Operation: Move the affected Ports to another VLAN
New VLAN Name :internal VLAN 4
New VLAN Id    :4

Port:Gi1/6
Device :172.20.118.182
Device Address :172.20.118.182

------------------------------------------
```

Review the Summary and click **Finish** to delete the VLAN, or click **Back** to modify the Select VLAN to Delete page, or click **Cancel** to exit.

Creating Ethernet VLANs

You can use Topology Services to create Ethernet VLANs (which is the typical VLAN design). For details, see **Ethernet VLANs**.

**Ethernet VLANs**

An Ethernet VLAN is the typical VLAN design. This consists of a logical group of end-stations, independent of physical location on an Ethernet network. Catalyst switches support a port-centric or static VLAN configuration.

All end stations that are connected to ports that belong to the same VLAN, are assigned to the same Ethernet VLAN. For further details see **Creating Ethernet VLANs**.
Chapter 11 Configuring VLAN

Creating Ethernet VLANs

Before you create Ethernet VLANs, you must create a VTP domain in your network. Your login determines whether you can use this option. To create Ethernet VLANs in your network:

Step 1 Either:
• Select Configuration > Topology.
Or
• Select Monitor > Monitoring Tools > Topology Services.
The Topology Services Main Window appears.

Step 2 Select a VTP domain from the Tree View.

Step 3 Select Tools > VLAN Management > Create > Ethernet from the menu.
The VLAN Creation wizard appears. For more details, see Creating VLANs.

Configuring Token Ring VLANs

A Token Ring VLAN is a set of rings interconnected through a bridging function. There are two Token Ring VLAN types defined in VTP version 2:

• Token Ring Bridge Relay Function (trBRF)—Domain of interconnected rings formed, using an internal multiport bridge function.
• Token Ring Concentrator Relay Function (trCRF)—Logical ring domains formed by defining groups of ports that have the same ring number.

You can create Token Ring Bridge Relay Function (trBRF) VLANs and Token Ring Concentrator Relay Function (trCRF) VLANs. Multiple trCRFs can be interconnected using a single trBRF.

A trBRF VLAN is a domain of interconnected rings formed using an internal multiport bridge function. A trCRF VLAN is a logical ring domain formed by defining groups of ports that have the same ring number.

This section contains:
• Understanding trBRF VLANs
• Creating trBRF VLANs
• Understanding trCRF VLANs
• Creating trCRF VLANs
• Deleting trBRF and trCRF VLANs
Understanding trBRF VLANs

A Token Ring Bridge Relay Function (trBRF) is a logical grouping of trCRFs. The trBRF is used to join different trCRFs. In addition, the trBRF can be extended across a network of switches through high-speed uplinks between the switches to join trCRFs contained in different switches.

A trBRF has two global parameters: a bridge number and a bridge type. The bridge number is used to identify the logical distributed source-route bridge (SRB), which interconnects all logical rings that have the same parent trBRF.

Creating trBRF VLANs

To create Token Ring Bridge Relay Function (trBRF) VLANs in your network.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select a VTP domain from the Tree View.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select <strong>Tools &gt; VLAN Management &gt; Create &gt; Token Ring BRF</strong> from the menu. See Table 11-8 for details.</td>
</tr>
</tbody>
</table>

Table 11-8  Creating trBRF VLANs Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP Domain</td>
<td>Name of VTP domain in which this VLAN will be created.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Enter a name for the trBRF.</td>
</tr>
<tr>
<td>VLAN Index</td>
<td>Topology Services automatically assigns a VLAN index. This number is incremented each time you create a VLAN in this VTP domain. If you want to change the VLAN index, enter a number between 1 and 1024 to identify the VLAN.</td>
</tr>
<tr>
<td>Purpose</td>
<td>Enter a word or phrase that describes the purpose of the VLAN.</td>
</tr>
<tr>
<td>Description</td>
<td>Describe the contents of the VLAN.</td>
</tr>
<tr>
<td>Create VLAN on all Transparent Switches</td>
<td>Check this box to include this VLAN on switches configured as VTP transparent.</td>
</tr>
<tr>
<td>BRF Parameters</td>
<td></td>
</tr>
<tr>
<td>Bridge Number</td>
<td>Integer in hexadecimal format. The default is 0xF.</td>
</tr>
<tr>
<td>STP Type</td>
<td>Spanning Tree protocol used in the network.</td>
</tr>
</tbody>
</table>

| Step 3 | Click **Apply**. |
Understanding trCRF VLANs

A Token Ring Concentrator Relay Function (trCRF) is a logical grouping of ports. Each trCRF is contained in only one trBRF, which is called its parent. When a port is assigned to the trCRF, only ports on that switch can belong to that trCRF.

As a rule, a trCRF cannot span different switches. This type of trCRF is called an undistributed trCRF. However, if your switches are connected through Inter-Switch Link (ISL), the Cisco Duplicate Ring Protocol (DRiP) allows two types of trCRFs in which the ports of a single trCRF can be on different switches.

These types of trCRFs are the default and the backup trCRF:

- **Default trCRF**
  
  The default trCRF can contain ports that are located on multiple switches. The default trCRF is associated with the default trBRF, which can span switches through ISL.

  Since the default trCRF is the only trCRF that can be associated with the default trBRF, the default trBRF does not perform any bridging functions, but uses source-route switching to forward traffic between the ports of the default trCRF.

- **Backup trCRF**
  
  The backup trCRF allows you to configure an alternate route for traffic between undistributed trCRFs located on separate switches that are connected by a trBRF. The backup trCRF is only used if the ISL connection between the switches becomes inactive.

Creating trCRF VLANs

You must configure a Token Ring Bridge Relay Function (trBRF) VLAN before creating the trCRFs that you want associated with the trBRF.

To create Token Ring Concentrator Relay Function (trCRF) VLANs in your network:

**Step 1** Select a trBRF from the Tree View.

**Step 2** Select Tools > VLAN Management > Create > Token Ring CRF from the menu.

For more information, see Table 11-9.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP Domain</td>
<td>Name of VTP domain in which this VLAN will be created.</td>
</tr>
<tr>
<td>trBRF</td>
<td>Name of trBRF to which this trCRF belongs.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name for the VLAN.</td>
</tr>
<tr>
<td>VLAN Index</td>
<td>Topology Services automatically assigns a VLAN index. This number is incremented each time you create a VLAN in this VTP domain. If you want to change the VLAN index, enter a number between 1 and 1024 to identify the VLAN.</td>
</tr>
</tbody>
</table>
Configuration Management with Cisco Prime LAN Management Solution 4.2

Chapter 11      Configuring VLAN

Configuring Token Ring VLANs

Table 11-9    Creating trCRF VLANs Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Enter a word or phrase that describes the purpose of the VLAN.</td>
</tr>
<tr>
<td>Description</td>
<td>Describe the contents of the VLAN.</td>
</tr>
<tr>
<td>Create VLAN on all Transparent</td>
<td>Check this box to include this VLAN on switches configured as VTP transparent.</td>
</tr>
<tr>
<td>Switches</td>
<td></td>
</tr>
<tr>
<td>Ring Number</td>
<td>Enter an integer between 1 and 0FFFH, or accept the ring number Topology Services creates.</td>
</tr>
<tr>
<td>VLAN Bridge Type</td>
<td>Select a bridging mode for this trCRF.</td>
</tr>
<tr>
<td>ARE (All Routes Explorer) Hop Count</td>
<td>Enter the ARE hop count. Valid numbers are 1 to 13, and 7 is the default.</td>
</tr>
<tr>
<td>STE (Spanning Tree Explorer) Hop</td>
<td>Enter the STE hop count. Valid numbers are 1 to 13, and 7 is the default.</td>
</tr>
<tr>
<td>Count</td>
<td></td>
</tr>
<tr>
<td>Backup CRF</td>
<td>Check this option if this trCRF is going to be the backup trCRF. A backup trCRF will replace the trBRF if the trBRF fails.</td>
</tr>
</tbody>
</table>

Step 3  Click Apply.

The LANE Services option is active.

To configure LANE in your network, click LANE Services.

Step 4  Click OK.

Your changes are saved and the window closes.

Deleting trBRF and trCRF VLANs

You can delete VLANs in your network. If you delete a VLAN with active ports, it disables the active ports in that VLAN.

You can use VLAN Port Assignment application to move any port to another VLAN.

You can delete a token ring Bridge Relay Function (trBRF) only if all token ring Concentrator Relay Functions (trCRFs) within it have been deleted, or if they do not contain any ports.

Deleting a VLAN with an associated ATM-VLAN does not delete the ATM-VLAN. The ATM-VLAN remains intact and appears in the Standalone ATM-VLANs folder for the ATM domain to which it belongs.

Your login determines whether you can use this option.

To delete a VLAN:

Step 1  Select Config > Topology Services.

The Topology Services Main Window appears.

Step 2  Select a VLAN that you want to delete, from the Tree View under Managed Domains.
Step 3 Select **Tools > VLAN Management > Delete**.

The domain window appears with a message:
The selected VLAN will be deleted if no ports are associated with this VLAN. Do you want to continue?

Step 4 Check the check box **Delete** on all Transparent Switches, if required.

Step 5 Click **Yes** to delete the VLAN or click **No** to exit.

---

### Interpreting VLAN Summary Information

This section contains:

- Displaying VLAN Reports
- Interpreting VLAN Reports

To display summary information about the VLANs in your network:

From Tree View in Topology Services, open a VTP domain and select a VLAN. The Summary information is displayed in the right pane of the Topology services window. See Table 11-10 to interpret this information.

---

**Note**

Information on Bridge Number and Ring Number are not applicable to Ethernet VLANs.

---

**Table 11-10 VLAN Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td>Number of ports in the domain.</td>
</tr>
<tr>
<td>Up Ports</td>
<td>Number of active ports in the domain.</td>
</tr>
<tr>
<td>ISL Index</td>
<td>Inter-Switch Link (ISL) index of the VLAN.</td>
</tr>
<tr>
<td>Port List</td>
<td></td>
</tr>
<tr>
<td>Link</td>
<td>A lightning bolt indicates a port that is connected to a switch.</td>
</tr>
<tr>
<td>PortDescription</td>
<td>Description about the port.</td>
</tr>
<tr>
<td>PortName</td>
<td>Name of the port.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of device to which the port belongs.</td>
</tr>
<tr>
<td>Device Address</td>
<td>IP address of device to which the port belongs.</td>
</tr>
<tr>
<td>Port Status</td>
<td>Whether the port is active, down, dormant, or testing.</td>
</tr>
<tr>
<td>isTrunk</td>
<td>If checked, the port is configured as a VLAN trunk.</td>
</tr>
<tr>
<td>Association Type</td>
<td>Type of VLAN.</td>
</tr>
<tr>
<td>Port Mode</td>
<td>Displays mode of port. For example, PVLAN-Host, Promiscuous, or non PVLAN.</td>
</tr>
</tbody>
</table>
Displaying VLAN Reports

LMS allows you to generate VLAN reports for devices, switch clouds, or VTP domains.

**Step 1**  
Select **Reports > Technology > VLAN**.

The Report Generator page appears.  
The left drop-down list displays LMS Reports.

**Step 2**  
Select **VLAN** from Select a Report drop-down list.

The VLAN page appears with the following information. See Table 11-11:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>Select a run type from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>The following run types are available: Immediate, Once, Daily, Weekly,</td>
</tr>
<tr>
<td></td>
<td>Monthly.</td>
</tr>
<tr>
<td></td>
<td>If you select Immediate, the Job Info fields and Scheduling Date will be</td>
</tr>
<tr>
<td></td>
<td>dimmed.</td>
</tr>
<tr>
<td>Note</td>
<td>Launching immediate VLAN reports for more than 500 devices results in an</td>
</tr>
<tr>
<td></td>
<td>error. You can schedule reports to run for all devices or launch immediate</td>
</tr>
<tr>
<td></td>
<td>reports for less than 500 devices.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the date and time at which you need to generate the report.</td>
</tr>
<tr>
<td></td>
<td>Format: 20 Apr 2005 at 01 20</td>
</tr>
</tbody>
</table>
Interpreting VL AN Summary Information

Step 3

Click **Submit** to generate the report. The VLAN reports window appears.

Or

Click **Reset** to change the settings.

You can open VLAN reports page from Topology Services.

To open VLAN reports from Topology Services:

**Step 1**

Either:

- Select **Configuration > Topology**.

Or

- Select **Monitor > Monitoring Tools > Topology Services**.

The Topology Services Main Window appears.

**Step 2**

Select a view that contains the device, switch cloud, or the VTP Domain for which you want to view the report.

This view is in the Tree View in the Topology Services Main Window.
Step 3  Select Reports > VLAN Report from the menu.
   or
   Right-click the VTP Domain or the device, and select Display View.
   The Network Topology window appears.

Step 4  Select the device or the switch cloud.

Step 5  Right-click and select VLAN Report from the popup menu.
   or
   Select Reports > VLAN Report.
   The VLAN Report window appears.

Interpreting VLAN Reports

The following information is displayed at the top of the report:

- Device Name
- Device IP
- Device Type
- Domain

Table 11-12 describes the fields in VLAN Report.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>VLAN index.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Name of the VLAN to which the device belongs.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of device can be operational or suspended.</td>
</tr>
<tr>
<td>VLAN Type</td>
<td>Types of VLANs to which the device is associated. The VLANs can be normal, primary, isolated, community, or two-way community VLANs.</td>
</tr>
<tr>
<td>Associated Primary</td>
<td>VLAN ID of the associated primary VLAN.</td>
</tr>
<tr>
<td>MTU Size</td>
<td>MTU size for the corresponding VLAN on that device.</td>
</tr>
<tr>
<td>Media Type</td>
<td>Explains in which media type the device operates. Device can be in ethernet, FDDI, or inactive.</td>
</tr>
</tbody>
</table>
Understanding Private VLAN

A Private VLAN (PVLAN) is a VLAN that isolates devices at Layer 2 (L2), from other ports within the same broadcast domain or subnet. PVLAN segregates traffic at L2 and converts a broadcast segment into a non-broadcast multi-access segment.

PVLANs can stop L2 connectivity between end stations on a switch without distributing them into different IP subnets, thus preventing wastage of IP addresses.

You can also assign a specific set of ports within a PVLAN, and thus control the connectivity among them. You can configure PVLANs and normal VLANs on the same switch.

This topic contains Types of Private VLAN Ports

Types of Private VLAN Ports

The ports in a private VLAN are categorized as:

- **Promiscuous Ports**
- **PVLAN Host Ports**
- **PVLAN Trunk Ports**

Promiscuous Ports

Promiscuous port communicates with all other interfaces and ports within a PVLAN. Such ports are used to communicate with external routers, local directories, network management devices, backup servers, administrative workstations, etc.

Ports to the routing module in some switches are promiscuous in nature (for example, MSFC).

PVLAN Host Ports

A PVLAN host port is a port connected to a server or an end host that requires Layer 2 (L2) isolation. A host port exists in the PortFast mode and the BPDU Guard feature is enabled on these ports. These ports can be further classified into:

- **Isolated Ports**
- **Community Ports**

This depends on the secondary VLAN to which the ports belong.

Isolated Ports

Isolated ports are completely isolated in L2, from other ports in the same PVLAN. These ports cannot receive the broadcasts from other ports within the same PVLAN, but receive broadcasts from promiscuous ports.

Privacy for the VLAN is ensured at L2 level by blocking the traffic to all isolated ports, except the promiscuous ports. Broadcasts from an isolated port is always forwarded to all promiscuous ports.

Community Ports

Community ports communicate among themselves and with their promiscuous ports. These ports are isolated at L2 from all other ports in other communities, or isolated ports within their private VLAN. Broadcasts propagate only between associated community ports and the promiscuous port.
PVLAN Trunk Ports

Private VLAN Trunk ports are similar to Host ports that can carry multiple VLANs. A Trunk port carries the primary VLAN and the secondary VLANs to the neighboring switch. The Trunk port is unaware of PVLAN and will carry PVLAN traffic without any special action.

Using Private VLAN

A Private VLAN has four distinct parts:

- **Primary VLAN**
  Manages the incoming traffic from the promiscuous port to isolated, community, two-way community ports, and all other promiscuous ports, in the same primary VLAN.

- **Isolated VLAN**
  Isolated ports use this VLAN to communicate to the promiscuous ports. The traffic from an isolated port is blocked from reaching all adjacent ports within its private VLAN, except for its promiscuous ports.

- **Community VLAN**
  A group of community ports use this unidirectional VLAN to communicate among themselves and to manage the outgoing traffic through the designated promiscuous ports from the private VLAN.

- **Two-way community VLAN**
  A group of community ports use this VLAN to communicate among themselves. This bidirectional VLAN manages the incoming and outgoing traffic for community ports and Multilayer Switch Feature Cards (MSFC).

Isolated and community VLANs are called secondary VLANs.

This section explains:

- Creating PVLAN
- Configuring Promiscuous Ports
- Deleting PVLAN

While creating private VLANs, you:

- Must set VTP to **Transparent** or **Off** modes, for VTP version 2.
- Can create PVLAN on primary server, **Transparent** and **Off** modes for VTP version 3.

LMS enables you to:

- Create primary Private VLAN.
- Create isolated, community or two-way community VLANs.
- Associate secondary VLANs to primary VLANs.
- Assign ports to secondary VLANs.
- Configure promiscuous ports.
Creating PVLAN

To create a Private VLAN, you must designate one VLAN as primary and another as either isolated, community, or two-way community VLAN. Then, you can assign additional VLANs as secondary VLANs.

After creating primary and secondary VLANs you must associate the secondary VLANs to the respective primary VLANs.

Creating a private VLAN involves the following steps:
- Creating Primary VLAN
- Creating Secondary VLAN and Associating to Primary VLAN
- Associating Ports to Secondary VLAN

Creating Primary VLAN

You must create primary VLAN before creating any other secondary VLAN.

To create Primary VLANs:

**Step 1** Either
- Select **Configuration > Workflows > VLAN > Create Private VLAN**.
  The Create PVLAN page appears.
- Or
  - Select **Configuration > Topology**.
- Or
  - Select **Monitor > Monitoring Tools > Topology Services**.
  The Topology Services Main Window appears.
  - Select a VTP domain from the VTP Tree View, under the Managed Domain or Network View.
  - Select **Tools > PVLAN Management > Create**.
  The Create PVLAN page appears.

**Step 2** Select the devices using the Device Selector or the Domain Selector.
For more details, see **Step 2 of Selecting Devices or Entities**.

**Step 3** Select **Primary** from the Private VLAN Type drop-down list.
The Get Primary VLANs tab and the Associated Primary VLAN field is disabled.

**Step 4** Enter a name for the VLAN in the VLAN Name field.

**Step 5** Enter the VLAN index number for the new Primary VLAN, in the VLAN Index field.
Step 6  Check the check boxes as required:
• To create private VLAN on all transparent switches.
• To copy Running to Startup config for IOS switches.

The check box for creating private VLANs on all transparent switches, is enabled only when the VLAN contains a device in transparent mode.

Step 7  Click Create to create primary PVLAN.

Note  You must create primary VLAN before creating any other secondary VLAN.

Creating Secondary VLAN and Associating to Primary VLAN

After creating a primary VLAN, you can create secondary VLANs. Once you create a secondary VLAN, you must associate that to a primary VLAN.

To do this:

Step 1  Either:
• Select Configuration > Workflows > VLAN > Create Private VLAN.

The Create PVLAN page appears.

Or
• Select Configuration > Topology.

Or
• Select Monitor > Monitoring Tools > Topology Services.

The Topology Services Main Window appears.
– Select a VTP domain from the VTP Tree View, under the Managed Domain or Network View.
– Select Tools > PVLAN Management > Create.

– The Create PVLAN page appears.

Step 2  Select one of the following options from the Private VLAN Type drop-down list:
• Isolated
• Community
• Two-Way Community

Step 3  Select the Associated Primary VLAN.

You can associate a secondary VLAN that you have created to a primary VLAN.
VTP Domain field displays the domain you have chosen.
You may enter the Private VLAN Name that you want to assign.

Step 4  Select the Private VLAN Index.
Chapter 11      Configuring VLAN

Using Private VLAN

Step 5  Check the check boxes as required:
• To create private VLAN on all transparent switches.
• To copy Running to Startup config for IOS switches.
  The check box for creating private VLANs on all transparent switches, is enabled only when the
  VLAN contains a device in transparent mode.

Step 6  Click **Apply** to create PVLAN or click **Cancel** to exit.

Associating Ports to Secondary VLAN

You must associate ports to the secondary VLAN that you have created. You can assign ports to a
secondary VLAN as you assign for normal VLANs. For assigning ports to VLANs, see Using
VLAN Port Assignment

Configuring Promiscuous Ports

You must associate the promiscuous ports to the PVLANs you have created, to receive traffic from
outside the PVLAN.

You can configure only the ports on which Trunking is not enabled.

To configure a Promiscuous Port:

Step 1  Select **Configuration > Workflows > VLAN > Configure Promiscuous Ports**.
  The Configure Promiscuous Ports page appears.

Step 2  Select a device or entities from the list using Device Selector or Domain Selector.

Step 3  Click **List Ports**.
  The Port List displays the list of ports on the selected devices.
  You can filter the list using the Filter or Advanced Filter.

Step 4  Select the ports from the ports listed in the table.

Step 5  Click **Configure**.
  The Configure Promiscuous Port window appears.
  The Port Details table displays:
  • Device Name
  • Port Name
  • Device IP Address
  • IfName

Step 6  Select the VLANs from the list of Available PVLANs.
Step 7  Click Add to add to list of Mapped VLANs.

Or

Click Remove to remove the VLANs from the Map VLANs table.

You can select the Copy Running to Start-up config check-box to copy the running configuration to the start-up configuration.

Step 8  Click Apply to configure.

Deleting PVLAN

To delete PVLAN:

Step 1  Select Configuration > Workflows > VLAN > Delete Private VLAN.

The Delete PVLAN page appears.

Step 2  Select a device or entities from the list using Device Selector or Domain Selector.

Step 3  Click List PVLANs to see a list of PVLANs. See Table 11-13.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PVLAN List</td>
<td>You can select any of the following filter criteria:</td>
</tr>
<tr>
<td></td>
<td>• PVLAN Index</td>
</tr>
<tr>
<td></td>
<td>• PVLAN Name</td>
</tr>
<tr>
<td></td>
<td>• PVLAN Type</td>
</tr>
<tr>
<td></td>
<td>• Associated Primary</td>
</tr>
<tr>
<td></td>
<td>• Domain</td>
</tr>
<tr>
<td>Filter</td>
<td>Enter the filter string, then click Filter.</td>
</tr>
<tr>
<td>PVLAN Index</td>
<td>Index value of the PVLAN.</td>
</tr>
<tr>
<td>PVLAN Name</td>
<td>Name of the PVLAN.</td>
</tr>
<tr>
<td>PVLAN Type</td>
<td>Type of PVLAN. Values are: Primary, Secondary, Community</td>
</tr>
<tr>
<td>Associated Primary</td>
<td>Name of the Associated Primary VLAN.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain to which the VLAN belongs to.</td>
</tr>
</tbody>
</table>

Step 4  Select the check box corresponding to the PVLAN you want to delete.

To select all, select the check-box in the table heading.

Step 5  Click Delete.
Understanding Inter-VLAN Routing

Inter-VLAN Routing enables to route the traffic between different VLANs. This feature is required when an end station wants to communicate with another end station in a different VLAN. Devices within a VLAN can communicate with one another without the help of a router.

On the contrary, devices in separate VLANs require a routing device to communicate with one another. Network devices in different VLANs cannot communicate with one another without a router to route the traffic between the VLANs.

In most of the network environments, VLANs will be associated with individual networks or subnetworks. In a switched network, VLANs segregate devices into different collision domains and Layer 3 (L3) subnets.

Configuring VLANs for inter-VLAN routing helps to control the size of the broadcast domain and to keep local traffic local. You can configure one or more routers to route traffic in the network.

Layer 2 switches require a L3 routing device (either external to the switch or in another module on the same chassis).

The new L3 Switches accommodate routing capabilities. The router or the switch receives a packet, determines the VLAN to which it belongs, and sends the packet to the appropriate port on the other VLAN.

Using Inter-VLAN Routing

Configuring Inter-VLAN Routing

LMS supports Inter-VLAN Routing configuration on devices like MSFC, RSM, and external routers with IPv4.

Prerequisite for configuring Inter-VLAN Routing

Configuration Functionality in LMS is a prerequisite for configuring Inter-VLAN Routing.

If you want to configure Inter-VLAN Routing on a device:

- LMS must manage the devices.
- The device must have the same device name when managed by LMS.

See Inventory Management with Cisco Prime LAN Management Solution 4.2 for more details on how to manage devices.

This section contains:

- Configuring Inter-VLAN Routing on RSM, MSFC, L2/L3 Devices
- Configuring Inter-VLAN Routing on External Routers
Configuring Inter-VLAN Routing on RSM, MSFC, L2/L3 Devices

To configure Inter-VLAN Routing on a VLAN interface:

**Step 1** Either:
- Select **Configuration > Topology**.
  Or
- Select **Monitor > Monitoring Tools > Topology Services**.

  The Topology Services Main Window appears.

**Step 2** Select a device from the Topology Services Tree View, under the Network Views.

**Step 3** Right-click the device and select **Config Inter-VLAN Routing** from the popup menu.

  The Configure Inter-VLAN Routing window appears. This window displays the Device Name and the Device IP of the selected device.

**Step 4** Select a device interface from Device interface configuration list.

**Step 5** Click **Edit** to edit an existing VLAN configuration.

  Or

  Click **New** to configure Inter-VLAN Routing for a new VLAN interface.

  You can edit IP Address, Admin Status, and Subnet Mask. See **Table 11-14**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Interface</td>
<td>Enter the VLAN interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address for the interface</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the subnet mask address.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Select the Admin status:</td>
</tr>
<tr>
<td></td>
<td>• Up</td>
</tr>
<tr>
<td></td>
<td>• Down</td>
</tr>
</tbody>
</table>

1. You can enter the VLAN interface name to create a new interface. You cannot edit an existing VLAN interface.

You can also delete a Device Interface from the list of Interfaces for which you do not want to configure Inter-VLAN Routing.
Step 6 Click **Move to Interface Set**.
If you want to edit the configuration details again:
   a. Select the VLAN interface from the Interface Set.
   b. Click **Delete from Interface Set**
   c. Repeat the steps from Step 4.

Step 7 Click **Apply**.
You can configure Inter-VLAN Routing for more than one VLAN interface, at a time.
Inter-VLAN Routing is configured for all the VLAN interfaces in Interface Set.

---

**Configuring Inter-VLAN Routing on External Routers**

To configure Inter-VLAN Routing on a VLAN interface of an external router:

---

**Step 1** Either:
   • Select **Configuration > Topology**.
   Or
   • Select **Monitor > Monitoring Tools > Topology Services**.
The Topology Services Main Window appears.

**Step 2** Select a device from the Topology Services Tree View, under the Network Views.

**Step 3** Right-click the device and select **Config Inter-VLAN Routing** from the popup menu.
The Configure Inter-VLAN Routing window appears.

**Step 4** Select a device interface from Device interface configuration list.

**Step 5** Click **Edit** to edit an existing VLAN configuration.
Or
Click **New** to configure Inter-VLAN Routing for a new VLAN interface.
You can edit IP Address, Admin Status, Encapsulation, and Subnet Mask. See Table 11-15

---

**Table 11-15 Configuring Inter-VLAN Routing Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Interface¹</td>
<td>Enter the VLAN interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address for the interface.</td>
</tr>
<tr>
<td>Sub-Interface ID</td>
<td>Enter the ID for the sub-interface.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Select the Admin status:</td>
</tr>
<tr>
<td></td>
<td>• Up</td>
</tr>
<tr>
<td></td>
<td>• Down</td>
</tr>
</tbody>
</table>
You can also delete a device interface from the list of interfaces for which you do not want to configure Inter-VLAN Routing.

**Step 6**  
Click **Move to Interface Set**.

If you want to edit the configuration details again:

a. Select the VLAN interface from the Interface Set.

b. Click **Delete from Interface Set**

c. Repeat the steps from **Step 2**.

**Step 7**  
Click **Apply**.

You can configure Inter-VLAN Routing for more than one VLAN interface, at a time. Inter-VLAN Routing is configured for all VLAN interfaces in the Interface Set.

### VLAN Trunking Protocol

VLAN Trunking Protocol (VTP) is a Layer 2 multicast messaging protocol that maps VLANs across all media types and VLAN tagging methods between switches. In this way it maintains the VLAN configuration consistency throughout a network.

VTP reduces the effort in adding, deleting, or renaming a VLAN at each switch, when the VLAN extends to other switches in the network.

VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

With VTP, you can make configuration changes centrally on one switch and have those changes automatically communicated to all the other switches in the network.

The major function of VTP is to distribute VLAN information. You must configure VTP before you configure any VLAN.

Using VTP, each switch in server mode displays the following:

- Management domain on the Trunk ports
- Configuration revision number
- VLANs and their specific parameters.

For more details on VLAN, see [Understanding Virtual LAN (VLAN)](#), and for VTP Domains, see [VTP Domains](#).
This topic contains:
  • VTP Domains
  • Understanding VLAN Trunking Protocol Version 3
  • Using VLAN Trunking Protocol (VTP)
  • Using VTP Views

VTP Domains

A VTP domain is made up of one or more interconnected devices that share the same VTP domain name. A switch can be configured to be in only one VTP domain, and each VLAN has a name that is unique within a management domain.

Typically, you use a VTP domain to ease administrative control of your network or to account for physical boundaries within your network. However, you can set up as many or as few VTP domains as are appropriate for your administrative needs.

Consider that VTP is transmitted on all Trunk connections, including ISL, IEEE 802.1Q, 802.10, and LANE.

VTP Domains display and monitor the details of the VLANs in your network. Sometimes includes special cases labeled NULL or NO_VTP.
  • NULL—Lists devices that are in transparent mode and that support VTP, but do not have configured domain names. Each of these devices is identified in the list by its IP address.
  • NO_VTP—Lists devices that do not support VTP. Each of these devices is identified in the list by its IP address.

However, devices which do not support VTP but support VLANs (for example, Catalyst 2900XL Standard Edition switches) are placed in the NO_VTP domain.

The devices that do not support VLANs and VTP (for example, Catalyst 1900 Standard Edition switches) are placed in the domain category of the neighbor device.

Components of VTP Domains

Within a VTP domain, you can configure switches as follows:
  • Server—VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over Trunk links. VTP server is the default mode.
  • Client—VTP clients operate in the same way as VTP servers. However, you cannot create, change, or delete VLANs on a VTP client. VTP clients also do not broadcast VTP advertisements like the VTP servers do.
  • Transparent—VTP transparent switches do not participate in VTP. A VTP transparent switch does not display its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements.

Your VTP domain structure influences the behavior of Topology Services.
Understanding VLAN Trunking Protocol Version 3

VTP version 3 can distribute a list of opaque databases over an administrative domain. VTP version 3 provides these enhancements to the previous VTP versions:

- Support for extended VLANs.
- Support for creating and advertising private VLANs.
- Support for VLAN instances and MST mapping propagation instances.
- Allows improved server authentication.
- Prevents you from adding the wrong database to a VTP domain.
- Allows interaction with VTP version 1 and VTP version 2.
- Support for configuring VTP version 3 on a per-port basis.
- Enables the network to propagate the VLAN database and other databases.

VTP version 3 is a collection of protocol instances. Each instance handles one database, which is associated with a given feature. VTP version 3 runs multiple instances of the protocol by which it handles the configuration propagation of multiple databases that are independent of one another.

For further details see Support for VTP Version 3.

Support for VTP Version 3

LMS supports the version 3 of VTP. Following are the major features supported in this release:

- Displays Primary server as a subfolder under the parent VTP domain:
  If your network contains devices running VTP version 3, the primary server is displayed as a subfolder under the parent Domain in the VTP Domains. Under Primary server folder, you can find all the server and client modes.

- Supports devices with VTP set to Off mode:
  The devices which are set to Off mode are supported as for the transparent mode devices. The Tree View displays the Off mode devices in subfolder under the parent domain.

- Provides VTP filters:
  Topology Filters contains a filter for devices running VTP version 3 in the Network Topology view for the VTP Domains and VTP Views.
  You can enable the filters to view the primary, server, client, transparent, and Off mode devices. The Off mode devices in VTP version 2 and version 3 domains, are displayed under different subfolders of the parent domain, in the Tree View.
  When you change the configuration through LMS, the Off mode devices are considered similar to the Transparent mode devices.
  For more details, see Figure 11-1.
Figure 11-1  VTP Filters

- Supports creating Private VLANs in VTP version 3 environment.

You can create a VLAN or PVLAN using a primary server domain or the parent domain. You can create a VLAN or PVLAN only on the Primary server, **Transparent** and **Off** mode devices, in a VTP version 3 environment.
Notes on creating VLAN or PVLAN in VTP version 3 domain using LMS

- You must select the parent VTP domain folder under the VTP domain Tree to create VLAN or PVLAN.
- To create VLAN or PVLAN on all transparent switches in the domain, you can check the check box Create VLAN on all transparent switches in the Creating VLAN or PVLAN windows.
  For more details, see Creating Ethernet VLANs and Creating PVLAN.
- You must select the primary domain subfolder under the VTP domain, while creating VLAN and PVLAN on the Primary server mode devices that has clients and secondary servers.
- You must select Transparent or Off mode subfolders under the parent VTP domain to create VLAN or PVLAN on a single Transparent or Off mode device respectively.

Using VLAN Trunking Protocol (VTP)

Using VLAN Trunking Protocol (VTP), each switch in server mode advertises its management domain on its Trunk ports, its configuration revision number, and its known VLANs and their specific parameters.

Therefore, a new VLAN must be configured on only one device in the management domain, and the information is automatically learned by all other devices (not in VTP transparent mode) in the same management domain.

After a device learns about a VLAN, it receives all frames on that VLAN from any Trunk port and, if appropriate, forwards them to each of its other Trunk ports.

This topic contains:
- Displaying VTP Reports
- Using VTP Views

Displaying VTP Reports

To display a VTP report for the VTP domains in your network.

**Step 1**

Either:
- Select Configuration > Topology.

Or
- Select Monitor > Monitoring Tools > Topology Services.

The Topology Services Main Window appears.

**Step 2**

Select a VTP domain under the VTP views for which you want to view the report. This view is in the Tree View in the Topology Services Main Window.

The VTP Report, which is the Summary view, appears.
Interpreting VTP Reports

See Table 11-16 to interpret the fields shown in the VT Reports Summary view.

Table 11-16  Field Description for VTP Report

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>A lightning bolt indicates a port that is linked to a switch.</td>
</tr>
<tr>
<td>Port</td>
<td>Number of ports in the domain.</td>
</tr>
<tr>
<td>IfName</td>
<td>Interface Name.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device to which the port belongs.</td>
</tr>
<tr>
<td>Device Address</td>
<td>Address of the device to which the port belongs.</td>
</tr>
<tr>
<td>PortStatus</td>
<td>Displays the status of the port, whether the port is active or dormant.</td>
</tr>
<tr>
<td>isTrunk</td>
<td>If the box is checked, the port is configured as a VLAN Trunk.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Name of the VLAN.</td>
</tr>
<tr>
<td>Association Type</td>
<td>Type of VLAN</td>
</tr>
<tr>
<td>Port Mode</td>
<td>Displays the mode of the port. For example, PVLAN-Host, Promiscuous, or a non-PVLAN.</td>
</tr>
</tbody>
</table>
Using VTP Views

VTP Views shows devices that participate in VTP domains. VTP Views also shows the non-VTP devices connected directly to the VTP domain. See Figure 11-2

**Figure 11-2 VTP Tree View**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VTP domain in the Topology Tree View</td>
</tr>
<tr>
<td>2</td>
<td>Parent VTP domain</td>
</tr>
<tr>
<td>3</td>
<td>Switch in Transparent mode</td>
</tr>
<tr>
<td>4</td>
<td>VLANs under the Transparent switch mode</td>
</tr>
<tr>
<td>5</td>
<td>VTP Views under the Network View</td>
</tr>
<tr>
<td>6</td>
<td>Parent VTP domain under VTP views</td>
</tr>
</tbody>
</table>

Use the VTP views to:
- Display Device Attributes
- Display Port Attributes
- Display Link Attributes
- Display information about multi-layer switching (MLS) devices in your network.
Understanding Trunking

A Trunk is a point-to-point link carrying traffic for several VLANs, and are typically used to connect switches. Instead of configuring several access links to carry multi-VLAN traffic, its economical to do it with a single trunk link.

Trunking is hence a type of configuration on an interface which allows VLANs to span the entire network, instead of just one switch. The Trunked interface that connects to another network device is allowed to pass traffic for multiple VLANs, instead of only one VLAN as in a non-Trunked interface on a switch.

This topic contains:

- Trunking Considerations
- Dynamic Trunking Protocol (DTP)
- Trunk Encapsulation
- Trunk Characteristics
- Encapsulation Types
- Creating Trunk
- Modifying Trunk Attributes

Trunking Considerations

While using a Trunk, consider the following:

- VLANs are local database of a switch. VLAN information is not passed between switches.
- Trunk links provide VLAN identification for frames traveling between switches.
- You can use either of the two Ethernet Trunking mechanisms: ISL and IEEE 802.1Q.
- Trunks carry traffic from all VLANs to and from the switch by default. However, they can be configured to carry only specified VLAN traffic too.
- Trunk links must be configured to allow Trunking on each end of the link.

Dynamic Trunking Protocol (DTP)

Dynamic Trunking Protocol (DTP) is a Cisco proprietary protocol. Trunk negotiation is managed by the DTP on a link between two devices. DTP is also used for negotiating the type of Trunking encapsulation to be used.

Dynamic Trunking is the ability to negotiate the Trunking method with the other device, and DTP is a point-to-point protocol that supports auto-negotiation of both ISL and 802.1Q Trunks. DTP sends the VTP domain name in a DTP packet.

Therefore, if you use DTP, and if the two ends of a link belong to a different VTP domain, the Trunk will not function.

The Catalyst operating system options of auto, desirable, and on, and the IOS options of dynamic auto, dynamic desirable, and trunk, configure a Trunk link using DTP. If one side of the link is configured to Trunk and sends DTP signals, the other side of the link will dynamically begin to Trunk, if the options match correctly.
To enable Trunking and not send any DTP signaling, you can use the option `nongotiate` for switches that support that function. If you want to disable Trunking completely, you can use the `off` option for a Catalyst operating system switch or the `no switchport mode trunk` command on an IOS switch.

DTP is a second generation Dynamic Inter-Switch Link Protocol (DISL) and allows the Cisco Catalyst devices to negotiate whether to use 802.1Q encapsulation. DISL and DTP do not negotiate Trunking in case of EtherChannel—they only negotiate whether to enable Trunking.

**Trunk Encapsulation**

The following Trunking encapsulations are available on all Ethernet interfaces:

- Inter-Switch Link (ISL)—A Cisco-proprietary Trunking encapsulation.
- 802.1Q—An industry-standard Trunking encapsulation.

**Trunk Characteristics**

Table 11-17 shows the DTP signaling and the characteristics of each mode.

<table>
<thead>
<tr>
<th>Trunking Mode</th>
<th>Frames Sent</th>
<th>Description</th>
<th>Final state (local port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>YES, periodic</td>
<td>Trunking is active. The interfaces sends DTP signals that actively attempt to convert the link to a Trunk link. The interface becomes a Trunk interface if the neighboring interface is set to on, auto or desirable, and is running DTP. A port that is in on mode always tags frames sent out from the port.</td>
<td>Trunking, unconditionally.</td>
</tr>
<tr>
<td>auto</td>
<td>YES, periodic</td>
<td>These links will only become Trunk links if they receive a DTP signal from a link that is already Trunking or desires to trunk. This will only form a Trunk if the neighboring interface is set to on or desirable. This is the default mode for Catalyst operating system switches.</td>
<td>The port will end up in Trunking state only if the neighboring interface wants to.</td>
</tr>
<tr>
<td>desirable</td>
<td>YES, periodic</td>
<td>These links would like to become Trunk links and send DTP signals that attempt to initiate a Trunk. They will only become Trunk links if the other side responds to the DTP signal. This will form a Trunk if the neighboring interface is set to on, auto, or desirable and is running DTP. This is the default mode for all Ethernet interfaces.</td>
<td>If the port detects that the neighboring interface is able to Trunk (remote in on, desirable or auto mode), it will end up in Trunking state. Otherwise, it will stay non-Trunking.</td>
</tr>
</tbody>
</table>
Understanding Trunking

Encapsulation Types

The encapsulation type allows you to specify whether ISL or 802.1q should be used for Trunking. The parameter is only relevant if the module you are using is able to use both types of encapsulation. The parameter can have three different values as shown in table below.

<table>
<thead>
<tr>
<th>Encapsulation Type</th>
<th>Description and Trunking</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISL</td>
<td>Sets the port encapsulation to ISL.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Sets the port encapsulation to 802.1q.</td>
</tr>
</tbody>
</table>
| negotiate          | Only available in auto or desirable Trunking modes:  
|                    | • If the neighboring interface has encapsulation type set to negotiate, the Trunk will eventually be set up with ISL.  
|                    | • If the interface is configured for ISL or 802.1q or only able to use ISL or 802.1q, the Trunking encapsulation used will be the same as the neighboring interface. |

Creating Trunk

To create trunk for a port:

**Step 1** Select **Configuration > Workflows > VLAN > Create Trunk**.

The Create Trunk page appears.

**Step 2** Select the device or domain from the list, and click **Show Links**.

The Available Links pane displays the links for each device that you have selected. **Table 11-18** describes the fields in the Available Links pane.

**Table 11-17 Trunking Mode Characteristics (continued)**

<table>
<thead>
<tr>
<th>Trunking Mode</th>
<th>Frames Sent</th>
<th>Description</th>
<th>Final state (local port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>nonegotiate</td>
<td>NO</td>
<td>Sets Trunking on and disables DTP. These will only become Trunks with ports in on or nonegotiate mode.</td>
<td>Trunking, unconditionally.</td>
</tr>
<tr>
<td>off</td>
<td>YES</td>
<td>This option sets Trunking and DTP capabilities off. This is usually the recommended setting for any access port since it prevents any dynamic establishments of Trunk links.</td>
<td>Non Trunking, unconditionally.</td>
</tr>
</tbody>
</table>
Step 3  Click the radio button corresponding to the link to select link for which you want to create trunk.

Step 4  Click Create Trunk.

Or

From Topology Map, right-click the link for which you want to create trunk, and select Create Trunk from the popup menu.

The Create Trunk window appears.

Table 11-19 describes the fields in the Create Trunk page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device IP addresses of the devices forming the link.</td>
<td><strong>Device Information</strong></td>
</tr>
<tr>
<td>Port numbers of the devices forming the link.</td>
<td></td>
</tr>
<tr>
<td>Select the Encapsulation type for the trunk. LMS supports: Dot1Q, ISL, Negotiate.</td>
<td><strong>Trunk Settings</strong></td>
</tr>
<tr>
<td>Trunking mode of the port is set to Desirable. LMS supports only the Desirable mode.</td>
<td></td>
</tr>
<tr>
<td>Lists only the active VLANs.</td>
<td><strong>Configure VLANs on Trunk</strong></td>
</tr>
<tr>
<td>1. Select the VLANs for which you do not want to configure Trunk.</td>
<td></td>
</tr>
<tr>
<td>2. Click Add to move the VLANs to Disallowed VLANs list.</td>
<td></td>
</tr>
<tr>
<td>1. Select the VLAN IDs of the VLANs, which must pass through the Trunk.</td>
<td></td>
</tr>
<tr>
<td>2. Click Remove to move the VLANs to the list of Allowed VLANs.</td>
<td></td>
</tr>
</tbody>
</table>

Table 11-18  Available Links Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Select the filter type and then enter the string. Leave the field blank to display all. You can filter the list based on the Port1, Device1, Port2, or Device2. For example, if you want to see only the trunks on the selected devices which starts with IP address 10.77, select Device1 from the Filter type, then enter 10.77.* in the filter field and click Filter.</td>
</tr>
<tr>
<td>Port 1</td>
<td>Port of the first device in the link.</td>
</tr>
<tr>
<td>Device 1</td>
<td>IP Address (IPv4 or IPv6 Address) of the device to which the port1 belongs to.</td>
</tr>
<tr>
<td>Port 2</td>
<td>Port of the second device in the link.</td>
</tr>
<tr>
<td>Device 2</td>
<td>IP Address (IPv4 or IPv6 Address) of the device to which the port2 belongs to.</td>
</tr>
</tbody>
</table>

Table 11-19  Create Trunk Page Field Description
Understanding Trunking

To copy the running configuration to start-up configuration, select Copy Running to Start-up Config check-box.

**Step 5**  
Click **Create** to create the Trunk or click **Close** to exit.

After you click **Create**, it will be idle for 2 minutes to see if the device goes down on setting the port to trunking mode. After 2 minutes, if the creation of trunk is successful, Data Collection for these devices is triggered.

Only after the completion of Data Collection, you can see the newly configured trunk ports in the Modify Trunk Attributes page.

| Note | If the trunk link is configured in a port that flaps between blocking and non-blocking states due to STP, then the port will be listed in both Create Trunk page and Modify Trunk Attributes page. To know whether the port is trunking or not, enable logging in the device and see the log messages. |

### Modifying Trunk Attributes

To modify trunk attributes:

**Step 1**  
Select **Configuration > Workflows > VLAN > Modify Trunk Attributes**.

The Modify Trunk Attributes page appears.

**Step 2**  
Select devices from the device list, and click **Show Trunks**.

The trunks configured on the devices are listed in the Trunk List. See Table 11-20.
Step 3  Select the radio-buttons corresponding the trunk you want to modify, and click **Modify Trunk**.
The Modify Trunk window appears.
The Device Information pane displays the device IP address and the port number of all the devices you have selected.

Step 4  Select the Trunk Settings
a. Select Encapsulation:
   – Dot1Q
   – ISL
   – Negotiate
b. Mode

Step 5  Configure VLANs on Trunk.
   • Allow VLAN(s)—Enter VLAN IDs of the VLANs, which must pass through the Trunk, in a range between 1 to 1005 and 1025 to 4094. The other VLANs are not supported for Trunking. * indicates that the VLANs were previously disallowed.
   • Disallow VLAN(s)—Enter VLAN IDs of the VLANs, which must not pass through the Trunk, in a range between 1 and 4096.

Use the Add or Remove buttons to allow or disallow VLANs.

To copy the running configuration to start-up configuration, select Copy Running to Start-up Config check-box.

Step 6  Click **Modify**.
EtherChannel

EtherChannel is a technology that bundles individual Fast Ethernet and Gigabit Ethernet links into a single logical link that would provide higher bandwidth. EtherChannels thus enable you to aggregate up to Gigabit Ethernet connections, providing up to 16 Gbps of bandwidth (in full duplex mode).

The channel is treated as a single logical connection between two switches. If one of the connections fails in the EtherChannel, the other connections will be operating so that the connection is not down.

This topic contains:

- Understanding EtherChannel
- Using EtherChannel

Understanding EtherChannel

EtherChannel provides incremental Trunk speeds between Fast Ethernet (FE) and Gigabit Ethernet (GE) by grouping multiple equal-speed ports into a logical port channel. EtherChannel combines multiple FEs up to 800 Mbps or GEs up to 8 Gbps, providing fault-tolerant, high-speed links between switches, routers, and servers.

LMS supports only PAgP, the aggregation protocol. When a user selects a port or link for configuring EtherChannel, the user is prompted with all available ports that can participate in the channel (Ports that are directly connected between devices).

Admin Group ID attribute for each port is also provided under group attribute. User can change them accordingly to choose which ports need to aggregate into a channel.

All ports that have same group value will participate in channel. LMS supports only the Desirable mode for EtherChannel configuration.

LMS does not support EtherChannel configuration between a switch and router.

Using EtherChannel

LMS allows you to:

- Aggregate multiple links between switches into one or more EtherChannels.
- Configure frame distribution parameters for EtherChannel load balancing.

Configuring EtherChannel

To configure EtherChannel:

**Step 1**

Either:

- Select **Configuration > Topology**.

Or

- Select **Monitor > Monitoring Tools > Topology Services**.

The Topology Services Main Window appears.

**Step 2**

Select a view that contains the devices for which you want to configure EtherChannel.
This view is in the Tree View in the Topology Services Main Window.

**Step 3**
Right-click the view and select **Display View** from the popup menu.

The Network Topology View window appears.

**Step 4**
From the Network Topology View select the link on which you want to configure EtherChannel.

**Step 5**
Right-click the link and select **Configure EtherChannel**.

The EtherChannel Configuration window appears.

Protocol field displays PAgP. Port Aggregation Protocol (PAgP) is the Protocol that is supported for configuring EtherChannel.

**Step 6**
Select one of the Distribution Protocols from the drop-down menu:
- ip
- mac
- port
- leave default

Select **leave default** when you do not want to configure distribution protocols.

The Channel Mode field displays the mode of the port.

LMS supports only the **Desirable** mode for EtherChannel configuration.

**Step 7**
Select one of these Distribution Address Types from the drop-down menu:
- source
- destination
- both
- leave default

Select **leave default** when you do not want to configure distribution address type.

**Step 8**
Select the link for which you want to configure EtherChannel.

**Step 9**
Click **Copy Running to StartUp config for IOS switches**, if required.

**Step 10**
Click **Apply** to continue or click **Close** to exit.

---

**VLAN Port Assignment**

VLAN Port Assignment is an application that displays device, port, and related VLAN information for an associated VTP domain in a tabular format and helps you manage ports on your network’s VLANs.

Use VLAN Port Assignment to:
- Assign or move ports to a VLAN.
- View port, device, and Trunk attributes.
- View and find port information in a VTP domain.
- Configure VLANs on a Trunk.
- Show and highlight a selected device or VLAN on a selected VTP domain.
Note
Assigning ports to VLANs cannot be done for more than 100 devices at a time, since it results in memory issues. Do VLAN port assignment for 100 devices at a time.

This topic contains the following sections:

- Understanding VLAN Port Assignment
- Starting VLAN Port Assignment
- Using VLAN Port Assignment

Prior to using VLAN Port Assignment, you should understand the concepts of VLANs and VTP domains. For more details on this, see:

- Understanding Virtual LAN (VLAN)
- VTP Domains

Understanding VLAN Port Assignment

To enable end-user ports to participate in a specific VLAN, you must first assign the ports. You assign ports to specified VLANs. The VLANs allow the ports to share the same broadcasts.

Ports that are not assigned to the VLAN cannot share these broadcasts. For more information about VLANs, see Understanding Virtual LAN (VLAN).

For VLAN Port Assignment to work correctly, LMS must discover the network. LMS requires a properly configured network to complete network discovery.

VLAN Port Assignment queries the ANI database based on criteria you enter.

After you submit the query, VLAN Port Assignment displays the device, port, and related VLAN information for an associated VTP domain. This is displayed in a tabular format.

You can use VLAN Port Assignment to:

- View and find port information in a VTP domain
- View port, device, and Trunk Attributes
- Show and highlight a selected device or VLAN in the VTP domain view

Starting VLAN Port Assignment

To start VLAN Port Assignment:

Step 1 Verify that your network is set up properly.
Step 2 Verify that the LMS server is set up properly and running.
Step 3 Select Configuration > Workflows > VLAN > Configure Port Assignment.

If you are prompted to install the Java plug-in, you can download and install the plug-in using the displayed installation screens. The next time you start the application, it will automatically use the plug-in.
Using VLAN Port Assignment

This section provides information to assign ports to VLAN.

To assign ports to a VLAN:

**Step 1** Select Configuration > Workflows > VLAN > Configure Port Assignment.

The VLAN Port Assignment page appears.

**Step 2** Select device or domain from the list using Device Selector or Domain Selector.

**Step 3** Click List Ports.

A list of ports in the selected devices or entities appears under the Port List. See Table 11-21 for the Port List:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Filter              | • Device Name  
• Device Address  
• Link  
• Port  
• Port Status  
• Port Description  
• VLAN Name  
• VLAN Index  
• Association Type |

Enter the filter string, and click Filter to filter the list based on the inputs. Leave this field blank to list all ports.

**Advanced Filter**

Click Advanced Filter to open Advanced Filter dialog box. Advanced filtering allows you to search ports using more search criteria.

For more details on Advanced Filter, see Advanced Filter.

**Columns**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>Shows whether the port is connected to a switch or not. The value can either be True or False.</td>
</tr>
<tr>
<td>Port</td>
<td>Name of the port.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device to which the port belongs to.</td>
</tr>
<tr>
<td>Device Address</td>
<td>IP address of the device to which the port belongs to.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Name of the VLAN to which the port belongs to.</td>
</tr>
<tr>
<td>Port Status</td>
<td>Status of the port. Shows whether the port is active or down.</td>
</tr>
</tbody>
</table>
| Port Description | Description for the port.  
Example: Intra-area 0.2.0.0 Resilient link |
| VLAN Index     | Index number of the VLAN to which the port belongs to.                      |
| Association Type | Type of Association.                                                         |
**Step 4** Select a VLAN from the VLAN drop-down list.

To copy the running configuration to the start-up configuration, select Copy running to start-up config check-box.

**Step 5** Click Assign.

---

**Usage Scenarios for Managing VLANs**

You can use the following scenarios to manage your network using LMS.

**Configuring PVLANs in External Demilitarized Zone**

**Scenario**

Web servers and Domain Name Servers (DNS) are connected to a Demilitarized Zone (DMZ) switch. The DMZ switch is configured with the VTP domain name, DMZ, where the switch is in transparent mode running VTP version 2. The servers belong to the same broadcast domain or VLAN.

**Understanding the Scenario**

This scenario would help you to isolate Layer 2 devices using PVLAN, and ensure that the DMZ servers do not send data across them, while internal and external hosts access these servers.

DMZ servers must be accessible from external clients as well as from the internal network. DMZ servers eventually needs access to some internal resources, and the servers must not send data across. The servers must not initiate traffic from the DMZ switch to the Internet. The DMZ servers reply only to the traffic from the internal resources.

**Understanding Concepts**

LMS provides an end-to-end solution for configuring Private VLANs, the security feature which LMS provides for managing LANs. You can configure PVLANs using LMS.

You can configure PVLANs in scenarios where Demilitarized Zone (DMZ) switches are configured without adhering to the right policies, leading to potential intrusions into your network.

**Demilitarized Zone**

Demilitarized Zone is a small subnetwork, which lies between a secure internal network, such as a corporate private LAN, and a non-secure external network, such as the public Internet. DMZ contains devices like Web servers, FTP servers, SMTP servers and DNS that are accessible to the Internet traffic. DMZ servers process incoming requests from the Internet, and initiate connections to certain internal servers or other DMZ segments, such as database servers.

DMZ servers must not send data or initiate any connection to the external networks. This shows that the necessary traffic flows on the basis of a trust model; but the model is not adequately enforced in many networks.

This section contains:

- **Prerequisites**
- **Reproducing Scenario**
- **Verifying Configuration**
Prerequisites

In this scenario, you need the following applications and tools in LMS.

- Topology Services
- PVLAN configuration user interface
- VLAN Port Assignment
- Promiscuous port configuration user interface
- VLAN report

Reproducing Scenario

To set up the scenario you must configure secondary VLAN on the servers, with isolated ports and community ports. The Firewall, the only device within the primary VLAN, must be defined in a primary VLAN with a promiscuous port.

Step 1

Create a primary VLAN: VLAN 100.
Enter VLAN 100 in the Private VLAN Name field to name the primary VLAN. For more details on creating primary VLAN, see Creating Primary VLAN.

Step 2

Create a community VLAN: VLAN 50.

- Enter VLAN 50 in the Private VLAN Name field.
- Associate VLAN 50 to the primary VLAN, VLAN 100.

For more details on creating secondary VLAN, see Creating Secondary VLAN and Associating to Primary VLAN.

Step 3

Create an isolated VLAN: VLAN 60.

- Enter VLAN 60 in the Private VLAN Name field to name the isolated VLAN
- Associate VLAN 60 to the primary VLAN, VLAN 100.

For more details on creating secondary VLAN, see Creating Secondary VLAN and Associating to Primary VLAN.

Step 4

Assign ports, which are connected to the Web servers, to the community VLAN 50.

Step 5

Assign ports, which are connected to the DNS servers, to the isolated VLAN 60.

Step 6

Configure the port that connects to the Firewall as a promiscuous port and map the secondary VLAN 50 and VLAN 60 to this promiscuous port. For more details, see Configuring Promiscuous Ports.

After you configure the promiscuous port, the secondary VLANs appear in the Mapped VLANs table.

You have configured promiscuous port and mapped both secondary VLANs to the primary VLAN 100.

If you want to map only the community VLAN 60, you must check the configurations, and map the other isolated VLANs.

Check the Select to Unmap check box and click Apply to unmap the isolated VLAN from primary VLAN. Community VLAN 60 is unmapped from the primary VLAN.
Verifying Configuration

To verify the configuration for this scenario:

**Step 1**
Either:
- Select **Configuration > Topology**.

Or
- Select **Monitor > Monitoring Tools > Topology Services**.

The Topology Services Main Window appears.

**Step 2**
From the Tree View in the Topology Services Main window, verify whether the new PVLANs are listed under DMZ VTP domain in transparent mode.

Primary VLAN 100 is listed as a subfolder under the DMZ domain and the secondary VLAN under the Primary VLAN subfolder. Note that the icon for PVLANs is different from the icon for normal VLANs.

**Step 3**
Generate VLAN Report for DMZ domain.

**Step 4**
Verify whether the new primary VLAN and secondary VLANs are listed. The associated primary VLAN is also listed for the secondary VLANs.

**Step 5**
To confirm that the PVLAN configuration is functioning, you can:
- **a.** Run a trace between the Web servers. The resultant traces must be successful.
- **b.** Run a trace between any Web server and the DNS. The resultant trace must fail.
- **c.** Run a trace between the DNS servers.
CHAPTER 12

Configuring Virtual Routing and Forwarding (VRF)

Using LMS, you can perform end-to-end VRF configurations in an enterprise network. You can perform the VRF Configurations using the following configuration workflows:

- Configuring VRF
- Editing VRF
- Extend VRF
- Deleting VRF

You can assign multiple VLANs to a single VRF instance using Edge VLAN Configuration workflow. To view and manage VRF configuration jobs, see Using VRF Lite Job Browser.

This section also details the following:

- Scalability Limits
- Pre-requisites

Scalability Limits

In an Enterprise network, LMS is tested to support the configuration of 32 VRFs with VRF configuration supported in 550 devices in your network. However, at a given time, you can select up to 20 devices and configure VRF using the Create, Edit and Extend VRF workflow.

Pre-requisites

The pre-requisites to perform VRF configurations are:

1. The device must be managed by LMS.
2. The device must either be L2/L3 or an L3 device
3. The device must have the necessary hardware support. For more information on hardware support, see http://www.cisco.com/en/US/products/sw/cscowork/ps563/products_device_support_tables_list.html

   If the device hardware is not supported then the device will be classified as Other devices
4. If a device does not support MPLS VPN MIB, it is classified as a Capable device.
5. VTP Server must be support MPLS VPN MIB. If the VTP Server does not support MPLS VPN MIB, LMS will not manage VTP Clients.
Configuring VRF

VRF configurations comprises workflows used to create, edit, extend, delete and assign Edge VLAN to VRF. The VRF Create wizard enables you to create new VRF instances on the selected devices.

To navigate through the Configuration workflows, click **Back** or **Next**. To exit the Configuration workflow, click **Cancel**.

This section explains the **Device Selector**.

**Device Selector**

To configure VRF on the devices, the devices are selected using the Device Selector. The Device Selector in all the configuration workflows displays the devices that satisfy the following condition:

- Layer2/Layer3 devices
- Layer3 devices

To create VRF, the VRF Creation wizard directs you through:

1. Create VRF
2. Interface Mapping to VRF
3. Routing Protocol Configuration
4. Summary of VRFs to be Configured

Create VRF

In the Create VRF workflow, you can select the Layer2/Layer3 or Layer 3 devices from the Distribution Layer or the Core Layer. At a given time, you can select up to 20 devices and configure VRF on the selected devices.

After selecting the devices, you can provide following details of VRF: VRF Name, Route Distinguisher and description of VRF that helps you identify the VRF that you have created.

In order to understand the workflows while configuring VRF, consider the topology as shown in **Figure 12-1** to demonstrate various stages involved in the VRF creation process. The topology includes devices from Distribution Layer and Core Layer.
Chapter 12 Configuring Virtual Routing and Forwarding (VRF)

Figure 12-1 LMS Topology

Here, the devices selected are 10.77.241.2 and 10.77.241.4. The interface connecting the two devices is a routed interface.

If you select only one device, the VRF creation prompts you to exit the Create VRF wizard, without mapping any interface to the VRF created on the selected device.

To provide end-to-end virtualization for the selected devices, you must virtualize the interfaces connecting devices selected. An interface can be mapped to a VRF in the Interface Mapping to VRF workflow.

To map an interface to the VRF created (virtualize an interface), you must select at least two devices in the VRF creation wizard.

Only users with Network Administrator privileges can create VRFs.
To create VRF:

**Step 1**  
Select **Configuration > Workflows > VRF-lite > Create VRF**.  
The Create VRF page appears.

**Step 2**  
Enter the details as mentioned below:

<table>
<thead>
<tr>
<th><strong>Table 12-1</strong></th>
<th><strong>Settings in Create VRF</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Window Element</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| Device Selector | The Device Selector displays the devices under the following groups:  
- All Devices - Represents VRF Supported devices managed by LMS.  
- Device Type Groups - Represents the devices that are grouped as Routers, Switches and Hubs, and Unknown Device Type.  
- User Defined Groups - Represents the devices that are in the user-defined groups.  
The Device Selector enables you to search and select the devices on which VRF is to be configured.  
Select the devices using the Device Selector.  
Check the checkbox to select the device in the groups listed and click **Select**.  
If you select only one device, the VRF creation wizard is completed without mapping any interface to the VRF created on the selected device.  
To map an interface to the VRF created, you must select at least two devices in the VRF creation wizard.  
See *Inventory Management with Cisco Prime LAN Management Solution 4.2* for information on how to use the Device Selector.  |
| VRF Name | Name of the VRF to be created. Valid values are alphanumeric characters. This field is mandatory.  |
| Route Distinguisher (RD) | Value used to distinguish routes configured in a VRF. Valid values are numeric characters in the format X:Y.  
The valid values for X are autonomous numbers. X can take values from 1 to 65535 or an IP Address.  
The valid values for Y are numeric values. Y can take values from 1 to 65535. For example X:Y is in the form 32:66 or 10.10.10.10:22.  
Note: You must enter a unique value for each VRF that is configured.  |
| Description | Description of VRF to be created. Valid values are alphanumeric characters.  
With no entry, the default description provided by LMS is “VRF Created by LMS”  |
| Finish | Click **Finish** to create VRF on the selected devices without interface mapping.  |
Step 3 Click Next.
The Interface Mapping to VRF window appears. For information on Interface Mapping to VRF, see Interface Mapping to VRF.

Interface Mapping to VRF

The Interface Mapping to VRF window displays the Source and the Destination devices selected using Device Selector. The page also displays a list of links in the form of rows.

This section contains:

- Current Mode
- Preferred Virtual Interfaces
- Native VLAN

The Interface Mapping to VRF window is used to map an interface to a VRF. The links displayed are the interfaces connecting a Source device to the Destination device. The mapping is performed from the devices in the Distribution Layer and Core Layer.

Current Mode
The current mode is the existing mode of an interface connecting any two selected devices. The current mode of an interface can be either a Switched or Routed mode.

Preferred Virtual Interfaces
In the Interface Mapping to VRF page, while you are assigning an interface to a VRF, you are prompted to create preferred virtual interfaces on the device. LMS suggests a preferred virtual interface, in scenarios where the current mode cannot be considered for configuring VRF.

The preferred virtual interfaces decide the type of virtual interface to be created, to virtualize an interface that connects the selected devices while you create VRF. The preferred virtual interfaces are based on the family of the selected devices.

The preferred virtual interface type is a part of the metadata XML file. The metadata XML file is used as a repository to store information on the device types and their associated metadata while creating VRF.

LMS has defined the following preferred virtual interfaces for the devices belonging to:

- Cat3k and Cat4k family, SVI is the preferred virtual interface
- Cat 6k and Router category, Sub-interface is the preferred virtual interface

Consider an example where two devices are selected. The virtual interfaces are created based on the current mode.

Note
The interfaces that are virtualized using VRF-lite must be Layer 3 interfaces.

In the Interface Mapping to VRF page, an interface is virtualized based on the current mode of the interface.
The Interface Configuration modes are mentioned in the Table 12-2.

### Table 12-2 Interface Configuration Modes

<table>
<thead>
<tr>
<th>Current Mode</th>
<th>Trunk is configured</th>
<th>Preferred Mode</th>
<th>LMS Configures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switched</td>
<td>Yes</td>
<td>SVI</td>
<td>SVI</td>
</tr>
<tr>
<td>Switched</td>
<td>Yes</td>
<td>SI</td>
<td>SVI</td>
</tr>
<tr>
<td>Switched</td>
<td>No</td>
<td>SVI</td>
<td>Trunk, SVI</td>
</tr>
<tr>
<td>Routed ¹</td>
<td>N/A</td>
<td>SVI</td>
<td>Trunk, SVI</td>
</tr>
<tr>
<td>Routed ²</td>
<td>N/A</td>
<td>SI</td>
<td>SI</td>
</tr>
<tr>
<td>Routed with Sub-interface configured</td>
<td>N/A</td>
<td>SI</td>
<td>SI. LMS configures with current mode</td>
</tr>
<tr>
<td>Routed with Sub-interface configured</td>
<td>N/A</td>
<td>SVI</td>
<td>SI. LMS configures with current mode</td>
</tr>
</tbody>
</table>

1. Interface is in Routed mode and the Sub-interface is not configured.
2. Interface is in Routed mode and the Sub-interface is not configured.

### Native VLAN

In the Interface mapping to VRF page, when you configure the VRF details on an interface, the VRF configurations might affect the global configurations in some scenarios. Therefore, Native VLANs are used for the global configuration traffic.

Consider the source device as 10.77.241.4 with source interface as Gi 1/1 and the destination device as 10.77.241.2 with destination interface as Gi 1/1 as shown in Figure 12-2.
Scenario 1: If both source and destination interfaces are in routed mode, Trunk cannot be configured on the interfaces. To configure Trunk, LMS converts the routed port of the destination interface to switch port. If a free VLAN exists, VNM converts the free VLAN to Native VLAN.

<table>
<thead>
<tr>
<th>Source Interface IP with port mode</th>
<th>Is Trunk</th>
<th>Preferred Mode</th>
<th>Sub-interface configured</th>
<th>Destination Interface IP with port mode</th>
<th>Is Trunk</th>
<th>Preferred Mode</th>
<th>Sub-interface configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.77.241.4, Routed</td>
<td>False</td>
<td>SI</td>
<td>Yes</td>
<td>10.77.241.2, Routed</td>
<td>False</td>
<td>SVI</td>
<td>No</td>
</tr>
</tbody>
</table>

Note: The IP Address provided for the source and the destination interface must be within the same network. For example: If the source interface IP Address is 10.10.10.2, then the destination interface IP Address must be configured as 10.10.10.3.
## Configuring VRF

### Step 1

In the Interface Mapping to VRF window, enter the details as in Table 12-4:

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VRF Details</strong></td>
<td><strong>VRF Name</strong> Name of the VRF to be created.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td><strong>Source Device Name</strong> Displays the Source Device name as in Device Credentials and Repository (DCR). Click the arrow icon to view or hide details of the interfaces that are a part of the Source device.</td>
</tr>
<tr>
<td><strong>Checkbox</strong></td>
<td><strong>Interface</strong> Interface connecting the Source device.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td><strong>IP Address</strong> Source interface IP Address. Valid IP values are the IPv4 Addresses. This field is blank if the source physical interface is not configured with an IP Address. If you newly configure an IP Address, the corresponding network IP Address must be advertised. You must advertise the IP Address by manually updating the Commands field in the Routing Protocol Configuration page.</td>
</tr>
<tr>
<td><strong>Destination</strong></td>
<td><strong>Device Name</strong> Displays the Destination Device name as entered in Device Credentials and Repository (DCR).</td>
</tr>
<tr>
<td></td>
<td><strong>Interface</strong> Interface connecting the Destination device.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td><strong>IP Address</strong> Destination interface IP Address. Valid IP values are the IPv4 Addresses. If the destination physical interface is not configured with an IP Address, this field is blank. If you newly configure an IP Address, the corresponding network IP Address must be advertised. You must advertise the IP Address by manually updating the Commands field in the Routing Protocol Configuration page.</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td><strong>Subnet Mask</strong> Subnet mask of the interface</td>
</tr>
</tbody>
</table>
| **is Trunk** | **is Trunk** Provides the status of the Trunk configuration on the associated physical interface. The following status is displayed:  
   - Not Applicable — In some scenarios, Trunk configuration is not required to configure VRF  
   - True — Trunk is configured on the associated physical interface  
   - Create — Trunk is not configured on the associated physical interface. Click **Create** to create a Trunk. |
| **VLAN ID** | **VLAN ID** VLAN ID on which VRF is configured. VLAN ID is auto-generated. The allowed range is from 1 to 4095. You can edit VLAN ID. |
Step 2  Click Next.

The Routing Protocol Configuration window appears.

For information on Routing Protocol Configuration, see Routing Protocol Configuration.

Warning Messages

In the Create VRF workflow, when you assign an interface to a VRF, in the following scenarios, the Warning messages displayed are:

**Table 12-5  Information on Warning Messages**

<table>
<thead>
<tr>
<th>Warning Message</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>One link is not configured as Trunk</td>
<td>Trunk is not configured on the selected physical interfaces displayed in the Interface Mapping to VRF window. You cannot assign VRF to the non-trunk interfaces.</td>
</tr>
</tbody>
</table>
| Some of the selected devices are isolated | Reasons for warning about isolated devices are: 
  • Devices selected are not in series:
    At least one or more devices selected are not connected in series, so the unconnected devices get isolated. You can view these device details in Topology (Layer 2 View). 
  or 
  • Devices with no physical connection:
    At least one or more selected devices is not physically connected. These devices are isolated device. You can view these device details in Topology (Unconnected View). 
You cannot assign VRF to interfaces for isolated devices. |

Routing Protocol Configuration

The Routing Protocol Configuration window is used to configure the Routing protocol to the selected devices on which VRF is configured.

By default, the Routing Protocol information from the global configuration for OSPF and EIGRP protocols is displayed.
Static Route Configuration

LMS currently supports the following Routing Protocols: OSPF and EIGRP. You can enter the static route configuration using the Configuration Icon in the Routing Protocol Configuration page.

Command Syntax

```
ip route vrf vrfname Destination IP Address Subnet Mask Router IP Address
```

For example:

```
ip route vrf Red 172.16.30.0 255.255.255.0 172.16.20.2
```

To configure static route directly using a device, you must enter the command as mentioned in the Command Syntax in the configuration mode.

---

Step 1

In the Routing Protocol Configuration window, enter the details as given in Table 12-6:

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device name to which routing protocol is associated.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the device.</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>You can configure the routing protocols on the VRF-configured devices.</td>
</tr>
<tr>
<td>View Global</td>
<td>Displays the VRF configuration and the global configuration details of the device name. You cannot edit these details.</td>
</tr>
</tbody>
</table>

Routing Protocols listed are the protocols present in global Configuration details.

**View Global**

Display the VRF configuration and the global configuration details of the device name.

**Commands**

Display the commands used to configure routing protocol configuration on the VRF to be created.

**Configuration Icon**

Enables you to edit the commands displayed in the Commands field.

**Restore Default**

Restores Protocol configuration and clear edited Commands details to default global configuration values.

**Finish**

Enables you to finish the Create VRF workflow without viewing the commands used to deploy the VRF Configurations in the Summary page.

Upon clicking finish, a job is created to deploy the VRF Configuration details to the selected devices.

---

Step 2

Click Next

The Summary page appears. For information on Summary, see Summary of VRFs to be Configured.
Summary of VRFs to be Configured

The Summary page summarizes the VRF and the Protocol configuration details to be deployed on the devices selected.

This section contains:

- Sample Summary
- Understanding VRF Configurations for Create VRF

Note

Upon successful completion of Create VRF workflow, LMS triggers the Data Collection process. After the Data Collection process is complete, LMS initiates the VRF Collection process.

The Sample Summary summarizes the VRF configuration details on the devices 10.77.241.2 and 10.77.241.4, connected by an interface Gi1/1. For more information, see Figure 12-2.

A sample of the summary is displayed below.

Sample Summary

Device: 10.77.241.2

ip vrf Green
  description Green VRF
  rd 60:70
vlan 4
  name Vlan_4
vlan 3000
  name VLANforGreenVRF
interface Vlan4
  ip address 20.20.20.1 255.255.255.252
  no shutdown
interface Gi1/1
  switchport trunk native vlan 4
  switchport trunk allowed vlan add 4
  switchport trunk allowed vlan add 3000
  no shutdown
interface VLAN3000
  ip vrf forwarding GreenVRF
  ip address 20.20.20.1 255.255.255.252
  no shutdown
router eigrp 10
  address-family ipv4 vrf GreenVRF
    autonomous-system 10
    network 10.0.0.0
    network 20.0.0.0
    auto-summary
eigrp router-id 10.77.241.2
eigrp stub connected summary
  exit-address-family

Device: 10.77.241.4

ip vrf GreenVRF
  description Green VRF
  rd 60:70
interface Gi1/1
  no switchport
  interface Gi1/1.1
encapsulation dot1Q 3000
ip vrf forwarding GreenVRF
ip address 20.20.20.2 255.255.255.252
no shutdown

router eigrp 10
   address-family ipv4 vrf GreenVRF
      autonomous-system 10
      network 10.0.0.0
      network 20.0.0.0
      auto-summary
      eigrp router-id 10.77.241.2
      eigrp stub connected summary
   exit-address-family

Understanding VRF Configurations for Create VRF

The following VRF configuration details are deployed on the selected devices and corresponding interfaces. The description of the VRF configuration details is given in Table 12-7.

Table 12-7 Create VRF Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device device name</td>
<td>Name of the selected device</td>
</tr>
<tr>
<td>ip vrf vrf-name</td>
<td>Allows you to enter VRF configuration mode and assigns a VRF name</td>
</tr>
<tr>
<td>description vrf-name</td>
<td>Provides description of the VRF created</td>
</tr>
<tr>
<td>rd route-distinguisher</td>
<td>Creates a VPN route distinguisher</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Allows you to enter the interface configuration mode and specify the Layer 3 interface to be associated with the VRF. The interface can be a routed port or SVI.</td>
</tr>
<tr>
<td>encapsulation dot1Q vlan-identifier</td>
<td>Allows you to define the encapsulation format as IEEE 802.1Q and specify the VLAN identifier. The VLAN identifier takes values ranging from 1 to 4095.</td>
</tr>
<tr>
<td>ip vrf forwarding vrf-name</td>
<td>Associates a VRF with an interface or sub-interface</td>
</tr>
<tr>
<td>ip address ip-address mask</td>
<td>Configure IP Address on an interface or sub-interface.</td>
</tr>
<tr>
<td>no shutdown</td>
<td>Enables an interface.</td>
</tr>
<tr>
<td>no switchport</td>
<td>Converts Layer 2 switch port interface to a Layer 3 routed physical interface</td>
</tr>
</tbody>
</table>

Step 1 Click Finish
A job is created to deploy the VRF configuration details to the selected devices. A confirmation message appears with the Job ID in the Information dialog box.
For example, if you create VRF Red, the message appears, Successfully created job for confirmation deployment 1051

Step 2 Click Job ID to check status of the Create VRF Configuration Job in the Information dialog box.
Step 3

Click **OK** in the Info dialog box.

To view the VRF configuration job status, go to **Configuration > Job Browsers > VRF Lite**. See Using VRF Lite Job Browser.

---

**Note**

To exit the VRF Create wizard without deploying the VRF details on the devices selected, click **Cancel**.

---

### Editing VRF

Edit VRF enables you to edit the VRF details on the devices participating in a VRF.

The Edit VRF workflow is used to edit the following details:

- IP Address of the interface connecting the devices that are a part of the selected VRF
- VLAN ID and VLAN Name
- Routing Protocol Configuration
- Exclude an interface that is a part of the selected VRF

Only users with Network Administrator privileges can edit VRF details.

To edit VRF details of the VRF configured devices, the VRF Edit wizard directs you through:

1. Interface Mapping to VRF in Edit VRF
2. Routing Protocol Configuration in Edit VRF
3. Summary of Edit VRF

To edit VRF:

**Step 1**

Select **Configuration > Workflows > VRF-lite > Edit VRF**.

The Edit VRF page appears. Table 12-8 describes the fields on the Edit VRF page.

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VRF Details</strong></td>
<td></td>
</tr>
<tr>
<td>VRF Name</td>
<td>Shows the list of VRFs as a drop-down list. You can edit the VRF by selecting the VRF from the drop-down list.</td>
</tr>
<tr>
<td>Route Distinguisher (RD)</td>
<td><em>Display only.</em> Shows the RD value of the selected VRF in the format X:Y. For more information on RD, see Route Distinguisher (RD).</td>
</tr>
<tr>
<td>Description</td>
<td><em>Display only.</em> Description of the selected VRF. You cannot edit the description.</td>
</tr>
<tr>
<td>Device Selector</td>
<td></td>
</tr>
</tbody>
</table>
Step 2  Click Next
The Interface Mapping to VRF window appears.

For information on Interface Mapping to VRF, see Interface Mapping to VRF in Edit VRF.

Consider the devices selected for Edit VRF workflow are: source device 10.77.241.4 with source interface as Gi 1/1 and the destination device as 10.77.241.2 with destination interface as Gi 1/1 as shown in Figure 12-2.

### Interface Mapping to VRF in Edit VRF

The Interface Mapping to VRF window displays a list of links connecting the devices that are selected in the Edit VRF page and are participating in the VRFs to be edited.

The link details are:

- The links displayed, can either be virtualized with the selected VRF or unvirtualized. You can use the Interface checkbox to deselect a link. This unvirtualizes a virtualized link.

  The corresponding negate command is displayed in the Summary of Edit VRF page indicating that the SI or SVI has been removed. You must manually update the negate command for the routing protocols in the Commands in Edit VRF workflow.

- If both interfaces on either side of a link, are virtualized with a VRF, the Interface Mapping to VRF page displays the values of VLAN, Switch Virtual Interfaces (SVIs) or Sub-Interface (SIs) IP address and so on.

---

**Table 12-8 Edit VRF Settings**

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Selector | Device Selector displays pre-selected devices, participating in the selected VRF. The Device Selector displays the devices under the following groups:  
  - All Devices - Represents VRF Configured devices  
  - Device Type Groups - Represents the devices that are grouped as Routers, Switches and Hubs, and Unknown Device Type  
  - User-defined Groups - Represents the devices that are in the user-defined groups.  

  The Device Selector enables you to search and select the devices on which VRF must be configured to edit the VRF functionality. Select the checkbox to select the device in the groups listed and click Select.  

  You must select at least two devices to edit the virtualization of the link connecting devices participating in the selected VRF. For more information on the devices listed, see Device Selector. |

*Note* The Device Selector does not display the devices that are not managed by LMS.

---

Configuration Management with Cisco Prime LAN Management Solution 4.2
If a link is virtualized only on one side of the interface, the same VLAN is used to virtualize the interface on the other end of the link. LMS application will not use a new VLAN. You can edit the VLAN details in this page.

The Interface Mapping to VRF window is used to map an interface to a VRF. The mapping is performed from the Distribution layer to the Core layer. It also provides information on the Source and the Destination devices associated with a link.

In the Interface Mapping to VRF in Edit VRF page, while assigning an interface to a VRF, LMS suggests preferred virtual interfaces to be created on the device. For more information, see Preferred Virtual Interfaces.

### Step 1

In the Interface Mapping to VRF window, enter the details as given in Table 12-9:

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VRF Details</strong></td>
<td><strong>Source</strong></td>
</tr>
<tr>
<td>VRF Name</td>
<td><em>Display only.</em> Name of the VRF selected.</td>
</tr>
<tr>
<td>Source Device Name</td>
<td>Displays the Source Device name as entered in Device Credentials and Repository (DCR).</td>
</tr>
<tr>
<td></td>
<td>Click the arrow icon to view or hide SIs or SVIs that are a part of the source device, participating in the VRF selected.</td>
</tr>
<tr>
<td>Checkbox</td>
<td>To assign an SI or SVI to a VRF, check the check box against the SVIs or SIs listed under the device name to which they are connected.</td>
</tr>
<tr>
<td></td>
<td>When you uncheck the checkbox to deselect a link to unvirtualize a virtualized link, the corresponding Negate command appears in the Summary of Edit VRF page.</td>
</tr>
<tr>
<td></td>
<td>You must manually update the negate command for the routing protocols in the Commands in Edit VRF workflow.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td>IP Address</td>
<td>If the interface is virtualized with a configured IP Address, it displays an SI or SVI. You can edit the IP Address. Valid IP values are the IPv4 Addresses. This field will be empty if the source physical interface is not configured. If you configure an IP Address newly, you must advertise the corresponding network IP Address by manually updating the Commands in Edit VRF field.</td>
</tr>
<tr>
<td>Device Name</td>
<td><em>Display only.</em> Shows the Destination Device name as it appears in the Device Credentials and Repository (DCR).</td>
</tr>
<tr>
<td>Interface</td>
<td><em>Display only.</em> Shows the name of the SVIs or SIs in the Destination device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>If the interface is virtualized with a configured IP Address, it displays an SI or SVI. You can edit the IP Address. Valid IP values are the IPv4 Addresses. This field will be empty if the source physical interface is not configured. If you configure an IP Address newly, you must advertise the corresponding network IP Address by manually updating the Commands in Edit VRF field.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Displays the subnet mask of the IP Address of SVI or SI.</td>
</tr>
</tbody>
</table>
Editing VRF

Step 2
Click Next

The Routing Protocol Configuration window appears.

For information on Routing Protocol Configuration, see Routing Protocol Configuration in Edit VRF.

Routing Protocol Configuration in Edit VRF

The Routing Protocol Configuration window displays details of the configured Routing protocols. These protocols are associated to the individual devices that you have selected. VRF is configured on these devices.

The details of the routing protocol running in the global configuration are also displayed.

Step 1
In the Routing Protocol Configuration window, enter the details as given in Table 12-10.
Table 12-10  Routing Protocol Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Protocol</td>
<td>You can configure the Routing protocols on VRF-configured devices. The drop-down list displays the routing protocols running on the selected device. LMS supports following routing protocols: • OSPF • EIGRP Routing Protocols listed are the protocols in global configuration details.</td>
<td>You can choose the desired routing protocol.</td>
</tr>
<tr>
<td>View Global</td>
<td>Displays the global routing protocol configuration details of the device name. You cannot edit these details.</td>
<td>Click View Global to view the global configuration details.</td>
</tr>
</tbody>
</table>
Step 2  Click Next

The Summary page appears.

For information on Summary, see Summary of Edit VRF.

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands</td>
<td>Displays the commands used to configure routing protocol configuration on the VRF to be edited.</td>
<td>You cannot enter a value in this field. To edit the command details: Click Configuration Icon. The newly configured IP Address for SIs or SVIs entered in the Interface Mapping to VRF in Edit VRF page, must be advertised using this field. To edit the command details: 1. Click Configuration Icon and enter the IP Address to be advertised. Valid IP values are the IPv4 Addresses. 2. Click the tick mark to save the changes. 3. Click the close mark to close without saving the changes.</td>
</tr>
<tr>
<td>Configuration Icon</td>
<td>Enables you to edit the commands displayed in the Commands field.</td>
<td>Click Configuration Icon to edit the Commands field details. Or To enter Static Route Configuration, click Configuration Icon, delete the commands displayed in the commands field and enter the commands mentioned in the Command Syntax.</td>
</tr>
<tr>
<td>Restore Default</td>
<td>Restores the edited Routing Protocol configuration details to the configuration values computed in the Edit VRF workflow.</td>
<td>Click Restore Default to restore VRF Configuration details to default Global values.</td>
</tr>
</tbody>
</table>
Chapter 12  Configuring Virtual Routing and Forwarding (VRF)

Summary of Edit VRF

The Summary page provisions you with the VRF and the Protocol configuration details to be deployed to the selected devices.

This section contains Sample Summary for Edit VRF.

Note

Upon successful completion of Edit VRF workflow, LMS triggers the Data Collection process. After the Data Collection process is complete, LMS initiates the VRF Collection process.

The Sample Summary summarizes the VRF configuration details on the devices 10.77.241.2 and 10.77.241.4, connected by an interface Gi1/1. For more information, see Figure 12-2.

A sample of the summary is displayed below.

Sample Summary for Edit VRF

Device: 10.77.241.2

ip vrf Green
  description Green VRF
  rd 60:70
vlan 4
  name Vlan_4
vlan 3000
  name VLANforGreenVRF
interface Vlan4
  ip address 20.20.20.1 255.255.255.252
  no shutdown
interface Gi1/1
  switchport trunk native vlan 4
  switchport trunk allowed vlan add 4
  switchport trunk allowed vlan add 3000
  no shutdown
interface VLAN3000
  ip vrf forwarding GreenVRF
  ip address 20.20.20.1 255.255.255.252
  no shutdown

router eigrp 10
  address-family ipv4 vrf GreenVRF
    autonomous-system 10
    network 10.0.0.0
    network 20.0.0.0
    auto-summary
    eigrp router-id 10.77.241.2
    eigrp stub connected summary
  exit-address-family
Device: 10.77.241.4

ip vrf GreenVRF
  description Green VRF
  rd 60:70
interface Gi1/1
  no switchport
  interface Gi1/1.1
    encapsulation dot1Q 3000
    ip vrf forwarding GreenVRF
    ip address 20.20.20.2 255.255.255.252
    no shutdown
Extend VRF

Extend VRF enables you to extend the VRF functionality across the network. You can extend VRF configuration details by selecting the neighbor devices of the VRF-configured devices in a network.

Only the following users have privileges to extend VRF details: Network Administrator, System Administrator and Super Admin.

To extend VRF functionality to other devices, the VRF Extend wizard directs you through:

1. Extend VRF
2. Interface Mapping to VRF in Extend VRF
3. Routing Protocol Configuration in Extend VRF
4. Summary of Extend VRF
To extend VRF:

**Step 1**

Select **Configuration > Workflows > VRF-lite > Extend VRF**.

The Extend VRF page appears. Table 12-11 describes the Extend VRF page.

### Table 12-11  Settings in Extend VRF

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VRF Details</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VRF Name</td>
<td>Name of the VRF selected.</td>
<td>You can select the VRF from the VRF Name drop-down list.</td>
</tr>
<tr>
<td>Route Distinguisher (RD)</td>
<td>Displays the RD value of the VRF entered while creating a VRF. Note: You must enter a unique value for each VRF that is configured. For more information on RD, see Route Distinguisher (RD).</td>
<td>Displays the RD value of the VRF selected in the format X:Y. You can edit the RD value. The edited RD value is applied only to the new devices that were added while extending the VRF.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the description of the VRF entered while creating a VRF.</td>
<td>Displays the description of the VRF selected. You can edit the description. The edited description is applied only to the new devices that were added while extending the VRF.</td>
</tr>
</tbody>
</table>
Extend VRF

Chapter 12 Configuring Virtual Routing and Forwarding (VRF)

12-22

Configuration Management with Cisco Prime LAN Management Solution 4.2
OL-25941-01

Table 12-11 Settings in Extend VRF (continued)

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Selector</td>
<td>Device Selector displays all the devices, except the devices participating in the selected VRF. It does not display any device that is configured with the VRF selected. The Device Selector also displays the devices under the following groups: • All Devices—Devices which are not participating in the selected VRF • Device Type Groups—Devices that are grouped as Routers, Switches and Hubs, and Unknown Device Type • User-defined Groups—Represents the devices that are in the user-defined groups. The Device Selector enables you to search and select the devices on which VRF must be configured to extend the VRF functionality. See Inventory Management with Cisco Prime LAN Management Solution 4.2 for information on how to use the Device Selector.</td>
<td>Select the devices using the Device Selector. Click the checkbox to select the device in the groups listed and click Select.</td>
</tr>
</tbody>
</table>

Note

The Device Selector does not display the devices that are not managed by LMS.

Step 2 Click Next.

The Interface Mapping to VRF window appears.

For information on Interface Mapping to VRF, see Interface Mapping to VRF in Extend VRF.

In Extend VRF, consider the devices selected are 10.77.241.4 and 10.77.241.6. For more information, see Figure 12-3.
Interface Mapping to VRF in Extend VRF

The Interface Mapping to VRF window displays a list of links that connect the devices. These are the devices that you have selected using Device Selector in the Extend VRF window.

The links displayed are:

- Links that connect the devices selected in Device Selector (in Extend VRF page)
- Links that connect the devices selected in Device Selector (in Extend VRF page) and the L2 neighboring VRF-configured device that is not selected in Device Selector (in Extend VRF page)
  - If the links associated with the L2 neighboring device are configured with the selected VRF, only the link is displayed.
  - If the neighbor device is not configured with the selected VRF and it is not selected in Device Selector, the device is not displayed in the Interface Mapping to VRF page.

Note the following about links:

- If both interfaces on either side of a link are not virtualized with a VRF, the Interface Mapping to VRF page displays the values of VLAN, SI or SVI, IP address configured.
Extend VRF

- If a link is virtualized using a VLAN on one side of the interface, the same VLAN is used to virtualize the interface on the other side of the link. LMS will not use a new VLAN. You can edit the VLAN details in this page.

While running you cannot exit the extend VRF workflow by clicking Finish in the Interface Mapping to VRF window.

The Interface Mapping to VRF window is used to map an interface to a VRF. The mapping is performed from the Distribution layer to the Core layer. It also provides information on the Source and the Destination devices associated with a link.

In the Interface Mapping to VRF in Extend VRF page, while assigning an interface to a VRF, LMS suggests preferred virtual interfaces to be created on the device. For more information, see Preferred Virtual Interfaces.

### Step 1
In the Interface Mapping to VRF window, enter the details as given in Table 12-12:

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VRF Name</td>
<td>Name of the VRF selected.</td>
<td>You cannot edit this field.</td>
</tr>
<tr>
<td>Source</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Device Name</td>
<td>Displays the Source Device name as entered in Device Credentials and Repository (DCR).</td>
<td>Click the arrow icon to view or hide details of the SIs or SVIs that are a part of the source device and participating in the VRF selected.</td>
</tr>
</tbody>
</table>
| Checkbox       | Allows you to select or deselect an SVI or SI that must be assigned to a VRF. | • To select, check against the SVIs or SIs listed under the device name to which they are connected.  
Or  
• To deselect, uncheck against the SVIs or SIs listed under the device name to which they are connected. |
| Interface      | Switch Virtual Interfaces (SVIs) or Sub-Interface (SIs) name in the source device. | Display only. |
| IP Address      | If the interface is virtualized, with IP Address configured, it displays an SI or SVI. You can edit the IP Address. This field is empty if the source physical interface is not configured. If you newly configure an IP Address, the corresponding network IP Address must be advertised. You must advertise the IP Address by manually updating the Commands in Extend VRF field. | Enter the IP Address. Valid IP values are the IPv4 Addresses. |
Table 12-12  Settings in Interface Mapping to VRF in Extend VRF

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Displays the Destination Device name as entered in Device Credentials and Repository (DCR).</td>
<td>Display only.</td>
</tr>
<tr>
<td>Interface</td>
<td>Switch Virtual Interfaces (SVIs) or Sub-Interface (SIs) name in the Destination device.</td>
<td>Display only.</td>
</tr>
<tr>
<td>IP Address</td>
<td>If the interface is virtualized, with IP Address configured, it displays an SI or SVI. You can edit the IP Address. This field is empty if the source physical interface is not configured. If you newly configure an IP Address, the corresponding network IP Address must be advertised. You must advertise the IP Address by manually updating the Commands in Extend VRF field.</td>
<td>Enter the IP Address. Enter the IP Address of the</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask of IP Address of SVI or SI</td>
<td>Enter the subnet mask</td>
</tr>
<tr>
<td>is Trunk</td>
<td>Provides the status of the Trunk configuration on the associated physical interface. The following status is displayed:  - True — Trunk is configured on the associated physical interface  - Create — Trunk is not configured on the associated physical interface.</td>
<td>To configure Trunk, click Create hyperlink. After clicking Create, Trunk is created.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>VLAN Name on which VRF is configured. VLAN Name is auto-generated.</td>
<td>You can edit VLAN Name.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN ID on which VRF is configured. VLAN ID is auto-generated or configured.</td>
<td>You can edit VLAN ID.</td>
</tr>
</tbody>
</table>

Step 2  Click Next.
The Routing Protocol Configuration window appears.
For information on Routing Protocol Configuration, see Routing Protocol Configuration in Extend VRF.
Routing Protocol Configuration in Extend VRF

The Routing Protocol Configuration window displays details of the configured Routing protocols. These protocols are associated to the individual devices that you selected. VRF is configured on these devices. Details about the Routing protocol running in the global configuration table are also displayed.

**Step 1**
In the Routing Protocol Configuration window, enter the details as given in Table 12-6:

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device name to which routing protocol is associated.</td>
<td>Display only.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the device.</td>
<td>Display only.</td>
</tr>
</tbody>
</table>
| **Routing Protocol** | You can configure the routing protocols on VRF-configured devices. The drop-down list displays the routing protocols running on the device selected. LMS supports following routing protocols:  
  - OSPF  
  - EIGRP  
  Routing Protocols listed are the protocols present in global configuration details. | You can choose the Routing protocol that you want. |
| View Global          | Displays the VRF configuration and the global configuration details of the device name. You cannot edit these details. | Click View Global to view the Global Configuration details. |
| **Commands in Extend VRF** | Displays the commands used to configure routing protocol configuration on the VRF to be extended. | You cannot enter a value in this field. To edit the command details:  
The newly configured IP Address for SIs or SVIs entered in the Interface Mapping to VRF in Extend VRF page, must be advertised using this field. Valid IP values are the IPv4 Addresses  
To edit the command details, Click Configuration Icon and enter the IP Address to be advertised. After entering the details, click the tick mark to save the changes.  
Click Configuration Icon and click the tick mark to save the changes. |
Extend VRF

Step 2  Click Next.

The Summary window appears.

For information on Summary, see Summary of Extend VRF.

---

**Summary of Extend VRF**

The Summary window displays the VRF and the Protocol configuration details to be deployed on the selected devices.

This section contains:
- Sample Summary for Extend VRF
- Understanding VRF Configurations for Extend VRF

Upon successful completion of Extend VRF workflow, LMS triggers the Data Collection process. After the Data Collection process is complete, LMS initiates the VRF Collection process.

The Sample Summary summarizes the VRF configuration details on the devices 10.77.241.4 and 10.77.241.6. For more information, see Figure 12-3.

A sample of the summary is displayed below.

**Sample Summary for Extend VRF**

Device: 10.77.241.4

vlan 5
  name Vlan_5
interface Gi1/3
  switchport trunk allowed vlan add 5
interface Vlan5
  ip vrf forwarding GreenVRF
  ip address 5.5.5.1 255.255.255.252
  no shutdown
Extend VRF

To extend VRFs to selected devices and corresponding interfaces, the VRF configuration details are deployed on the selected devices and corresponding interfaces. To understand the VRF configuration details edited, see Understanding VRF Configurations for Create VRF.

**Step 1** Click **Finish**.

A job is created to deploy the VRF configurations details to the selected devices. A confirmation message appears with the Job ID in the Information dialog box.

For example, if you extend VRF Red, the message appears, *Successfully created job for confirmation deployment.1052*

**Step 2** Click **Job ID** to check status of the Job in the Info dialog box.

**Step 3** Click **OK** in the Information dialog box.

To view the VRF configuration job status, go to **Configuration > Job Browsers > VRF Lite**. See Using VRF Lite Job Browser.
Deleting VRF

Delete VRF workflow is used to delete the VRFs present on your network.

The Delete VRF workflow enables you to:

- Delete VRF from the selected devices
- Delete virtual interfaces that are virtualized by the VRF of the selected device
- Delete virtualized virtual interfaces from the devices, at the other end of the physical interface that connects the selected device.

For example, Device A with virtual interface (Gig5/1.1) is connected to Device B with virtual interface (Gig4/1.1). (Assume that the virtual interfaces of both devices are virtualized with the selected VRF.)

If you select Device A using Device Selector, Device B will be on the other end of the physical interface that is connected to Device A. In this case, the virtual interface(Gig5/1.1) on Device A, and virtual interface(Gig4/1.1) on Device B will be deleted.

You cannot delete Layer2 VLANs using the Delete VRF feature.

- Delete internal VLANs created for Sub-Interfaces (SIs)

The following users have the privilege to delete VRF: Network Administrator and Super Admin. The user privileges mentioned is applicable for local mode only.

To delete VRF:

Step 1

Select Configuration > Workflows > VRF-lite > Delete VRF.

The Delete VRF: VRF and Device Selection page appears. Table 12-14 details the Delete VRF: VRF and Device Selection page.

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VRF Details</strong></td>
<td></td>
</tr>
<tr>
<td>VRF Name</td>
<td>Shows the list of VRFs as a drop-down list. You can delete the VRF by selecting the VRF from the drop-down list.</td>
</tr>
<tr>
<td>Route Distinguisher (RD)</td>
<td><em>Display only.</em> Shows the RD value of the selected VRF in the format (X:Y). For more information on RD, see <a href="#">Route Distinguisher (RD)</a>.</td>
</tr>
<tr>
<td>Description</td>
<td><em>Display only.</em> Description of the selected VRF. You cannot edit the description.</td>
</tr>
</tbody>
</table>

**Table 12-14** Delete VRF: VRF and Device Selection
Step 2  Click Next.

The Summary window appears.

For information on Summary, see Delete VRF - Summary.

### Delete VRF - Summary

The Summary window summarizes the commands that will be deployed on the devices to withdraw participation in a VRF.

This section contains:

- Sample Summary for Delete VRF
- Understanding VRF Configurations for Delete VRF

**Note**

Upon successful completion of Delete VRF workflow, LMS triggers the Data Collection process. After the Data Collection process is complete, LMS initiates the VRF Collection process. The VRF Collection process initiated depends on the settings provided in Admin. See *Administration of Cisco Prime LAN Management Solution 4.2* for more information.

The Sample Summary summarizes the VRF configuration details on the devices 10.77.241.4 and 10.77.241.6. For more information, see Figure 12-3.

A sample of the summary is displayed below.

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Selector | Device Selector displays VRF-configured devices with selected VRF.  
The Device Selector displays the devices under the following groups:  
- All Devices - Represents VRF Configured devices  
- Device Type Groups - Represents the devices that are grouped as Routers, Switches and Hubs, and Unknown Device Type  
- User-defined Groups - Represents the devices that are in the user-defined groups.  
The Device Selector enables you to search and select the devices on which VRF functionality must be deleted.  
Select the checkbox to select the device in the groups listed.  
For more information on the devices listed, see Device Selector. |

<table>
<thead>
<tr>
<th>Table 12-14 Delete VRF: VRF and Device Selection</th>
</tr>
</thead>
</table>
Sample Summary for Delete VRF
Device: 10.77.241.4

    no interface Vlan5
    no ip vrf GreenVRF

Device: 10.77.241.6

    no interface Vlan5
    no ip vrf GreenVRF

Understanding VRF Configurations for Delete VRF
The VRF configuration details pushed in the devices is explained in Table 12-15.

Table 12-15  Delete VRF Configuration details

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device device name</strong></td>
<td>Name of the device</td>
</tr>
<tr>
<td>no interface interface-id</td>
<td>Removes the interface_id from device name. For example, vlan 5 will be removed from device IP 10.77.241.6.</td>
</tr>
<tr>
<td>no ip vrf vrf-name</td>
<td>Deletes the VRF from the device</td>
</tr>
</tbody>
</table>

To delete VRF, present on the selected devices, Click **Finish** in the Summary page.
A job is created to delete the VRF configurations details from the selected devices. A confirmation message appears with the Job ID in the Information dialog box.
To view the VRF configuration job status, go to **Configuration > Job Browsers > VRF Lite**. See Using VRF Lite Job Browser.

Edge VLAN Configuration

In an Enterprise network, end-to-end virtualization is achieved by associating a VRF instance with an SVI to map VLANs to different logical or physical VPN connections.

The Edge VLAN Configuration workflow allows you to map the Access VLANs to a VRF instance there by providing end-to-end virtualization. The Access VLANs are mapped to single VRF instance by assigning it to existing Switch Virtual Interface (SVI) or new SVIs created at the Distribution Layer.

A VRF instance is associated with an Switch Virtual Interface (SVI) to map VLANs to different logical or physical VPN connections.

**Note**
You can associate at most one SVI with a VLAN.

The following users have the privilege to assign Edge VLAN to VRF: Network Administrator and Super Admin. These user privileges apply only to the local mode.

The Edge VLAN Configuration wizard directs you through:

5. VLAN to VRF Mapping
6. Edge VLAN Configuration Summary
To perform Edge VLAN Configuration:

**Step 1**
Select **Configuration > Workflows > VRF-lite > Edge VLAN Configuration**.

The Edge VLAN Configuration: VRF and Device Selection page appears. *Table 12-16* details the Edge VLAN Configuration: VRF and Device Selection page.

*Table 12-16  Edge VLAN Configuration: VRF and Device Selection*

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF Details</td>
<td></td>
</tr>
<tr>
<td>VRF Name</td>
<td>Shows the list of VRFs as a drop-down list. Select the VRF from the drop-down list.</td>
</tr>
<tr>
<td>Route Distinguisher (RD)</td>
<td><em>Display only.</em> Shows the RD value of the selected VRF in the format X:Y. For more information on RD, see Route Distinguisher (RD).</td>
</tr>
<tr>
<td>Description</td>
<td><em>Display only.</em> Description of the selected VRF. You cannot edit the description.</td>
</tr>
<tr>
<td>Device Selector</td>
<td></td>
</tr>
</tbody>
</table>
| Device Selector | Device Selector displays VRF-configured devices with selected VRF. The Device Selector displays the devices under the following groups:  
  - All Devices - Represents VRF Configured devices  
  - Device Type Groups - Represents the devices that are grouped as Routers, Switches and Hubs, and Unknown Device Type  
  - User-defined Groups - Represents the devices that are in the user-defined groups.  
The Device Selector enables you to search and select the devices. Select the checkbox to select the device in the groups listed. For more information on the devices listed, see Device Selector. |

**Step 2**
Click **Next**
The Edge VLAN Configuration: VLAN to VRF Mapping page appears.
For information on VLAN to VRF Mapping, see **VLAN to VRF Mapping**.
VLAN to VRF Mapping

The Edge VLAN Configuration: VLAN to VRF Mapping page is used to map the Access VLANs to a VRF instance thereby providing an end-to-end virtualization. You can assign Edge VLAN to a VRF by associating it to a Switch Virtual Interface (SVI).

The Edge VLAN Configuration: VLAN to VRF Mapping page is used to:

1. Configure SVI for new or already existing VLANs in the Distribution Layer
2. Allow VLANs in available trunk in Access Layer
3. Configure Layer 3 features

The devices selected in Edge VLAN Configuration: Select Devices page are the devices from the Distribution Layer.

The Edge VLAN Configuration: VLAN to VRF Mapping page displays a list of Switch Virtual Interfaces (SVIs) that are

- Virtualized with the VRF selected
- Unfertilized

This section contains:

- **Trunk Configuration**
- **Layer 3 Features**

The Edge VLAN Configuration: VLAN to VRF Mapping page includes the following icons:

- **Existing VLAN icon:** Used to display existing VLANs (VLAN Name) on the device.
- **Configurations icon:** Used to perform Trunk and Layer 3 feature configuration.

Upon clicking the Configurations icon, the Trunk Configuration tab is selected by default and the Available Trunks page appears.

**Step 1**

The Edge VLAN Configuration: VLAN to VRF Mapping window appears. The window displays the name of the selected VRF in the Edge VLAN Configuration: Select Devices page. In this window, enter the details as given in Table 12-17.

**Table 12-17  Details of VLAN to VRF Mapping**

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VRF Details</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VRF Name: Selected VRF</td>
<td>Name of the VRF selected.</td>
<td>Display only.</td>
</tr>
<tr>
<td><strong>Device Details</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Name (Hyperlink)</td>
<td>Represents the device selected in the Device Selector.</td>
<td>Click the arrow icon to view or hide details of the SVIs that are a part of the device name.</td>
</tr>
<tr>
<td></td>
<td>Device name of the device is displayed as a hyperlink.</td>
<td>If you right-click the Device name hyperlink, it displays Add SVI option. Click Add SVI option to add an SVI.</td>
</tr>
</tbody>
</table>
Chapter 12 Configuring Virtual Routing and Forwarding (VRF)

Table 12-17 Details of VLAN to VRF Mapping

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Represents a Switch Virtual Interface that is the logical Layer 3 interface on a switch. It displays the multiple VLANs that are carried by the physical interface. The corresponding VLAN ID and VLAN Name is populated in this page. You can view the status of the interface. It displays a tick mark if the status is up and cross mark if the status is down.</td>
<td>- Enter the SVI value. Valid values of SVI ranges from 2 to 4096. Or - Select existing VLANs on your network by clicking the icon. If the existing VLAN Name is displayed in this field, you can edit this field. Edited entries will overwrite the existing VLAN Name. If the VLAN value entered is not in your network, LMS creates VLAN.</td>
</tr>
<tr>
<td>Checkbox</td>
<td>Allows you to virtualize or un-virtualize SVIs using the selected VRF.</td>
<td>- To virtualize an interface, check against the SVIs listed under the Device Name - To un-virtualize, un-check an interface that is already virtualized with a VRF</td>
</tr>
<tr>
<td>Existing VLAN icon</td>
<td>When you click this icon, the Existing VLAN Selector page appears. This page displays the existing VLANs on the device. You can also search existing VLANs by entering the VLAN Name in the Search field. The VLANs displayed do not have an SVI/SI in the selected device.</td>
<td>Select the desired VLAN. Upon selecting the VLAN, the corresponding VLAN Name and VLAN ID is populated in the VLAN ID and VLAN Name field.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the SVI. Enter the IP Address. Valid IP values are the IPv4 Addresses</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask of the SVI. Enter the Subnet mask</td>
<td></td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN ID to be assigned to a VRF. Valid values of VLAN ID ranges from 1 to 4094.</td>
<td>Enter the VLAN ID. You cannot edit this field.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>VLAN Name to be assigned to a VRF. Enter the VLAN Name.</td>
<td></td>
</tr>
<tr>
<td>Configurations</td>
<td>Enables you to perform the following configurations to be associated to the corresponding SVI: Trunk and Layer 3 feature configuration. Click the Edge Interface Configuration icon to configure Trunk and Layer 3 features. For more information, see Trunk Configuration and Layer 3 Features.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 12  Configuring Virtual Routing and Forwarding (VRF)

Trunk Configuration

The Available Trunks page displays the trunks available in the selected device. It also displays the device that are neighbors to the selected device. If no trunk is available in the selected device, the Available Trunks page is blank.

The VLANs in any corresponding, existing or newly created SVIs will be allowed on all the trunk interfaces, that are selected in the Trunk Configuration page. The values displayed in the Trunk Configuration page are not fetched from the selected devices.

Step 2  In the Trunk Configuration page, enter the details as given in Table 12-18.

Table 12-18  Settings of Trunk Configuration

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Trunks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface Name</td>
<td>Interface name on which Trunk exist.</td>
<td>Display only.</td>
</tr>
<tr>
<td>Neighbor Name</td>
<td>Neighbor device to the selected device.</td>
<td>Select the desired trunk in which VLAN needs to be allowed and click <strong>Apply</strong>. The Trunk configuration details entered are saved. The VLANs in the corresponding SVI will be allowed on all the trunk interfaces that are selected in the Trunk Configuration page.</td>
</tr>
</tbody>
</table>

Layer 3 Features

Upon clicking the Layer 3 Features tab, the Layer 3 Feature page appears which enables you to configure the following Protocols and DHCP Server details for any corresponding, existing or newly created SVIs. The values displayed under Layer 3 Features tab are not fetched from the selected devices.

- HSRP: Hot Standby Router Protocol
- VRRP: Virtual Router Redundancy Protocol
- GLBP: Gateway Load Balancing Protocol

Note  The layer 3 features details are not fetched from the devices.

Step 3  In the Layer 3 Feature Configuration page, enter the details as given in Table 12-18.
Table 12-19 Settings of Layer 3 Feature Configuration

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 3 Redundancy Protocol</td>
<td>Select Type Represents the Redundancy protocol types.</td>
<td>Select the desired Redundancy protocol Type.</td>
</tr>
<tr>
<td></td>
<td>HSRP : Hot Standby Router Protocol</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VRRP : Virtual Router Redundancy Protocol</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GLBP: Gateway Load Balancing Protocol</td>
<td></td>
</tr>
<tr>
<td>Group Number</td>
<td>Represents the group number of the protocol.</td>
<td>Enter the Standby Group Number.</td>
</tr>
<tr>
<td></td>
<td>A valid group number is an integer. Valid range values for corresponding Redundancy Protocols is as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• HSRP : 0 - 4095</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VRRP : 1 - 255</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• GLBP : 0 - 1023</td>
<td></td>
</tr>
<tr>
<td>Virtual Router IP Address</td>
<td>IP Address of the Virtual Router at the edge.</td>
<td>Enter the Virtual Router IP Address.</td>
</tr>
<tr>
<td></td>
<td>Valid IP values are the IPv4 Addresses.</td>
<td>Valid IP values are the IPv4 Addresses.</td>
</tr>
<tr>
<td>DHCP Server IP Address</td>
<td>IP Address of the DHCP Server</td>
<td>Enter the DHCP Server IP Address and click Apply. Valid IP values are the IPv4 Addresses. After applying the Layer 3 Features configuration details, the values are saved. Click Close. The Edge VLAN Configuration: VLAN to VRF Mapping page appears.</td>
</tr>
</tbody>
</table>

After entering the Trunk and Layer 3 Features, a new row is added on the Edge VLAN Configuration: VLAN to VRF Mapping page appears. You can enter the details in the new row to create an SVI for newly created VLAN.

**Step 4** Click Next

The Edge VLAN Configuration: Summary page appears.

For information on Summary, see Edge VLAN Configuration Summary.
Edge VLAN Configuration Summary

The Edge VLAN Configuration: Summary page summarizes the VRF configuration details to be deployed to the selected devices.

This section contains:

- Sample Summary for Edge VLAN Configuration
- Understanding Edge VLAN Configuration Details

Note
Upon successful completion of Edge VLAN Configuration workflow, LMS triggers the Data Collection process. After the Data Collection process is complete, LMS initiates the VRF Collection process.

The Sample Summary summarizes the VRF configuration details on the device 10.77.241.2. For more information, see Figure 12-2.

A sample of the summary is displayed below.

Sample Summary for Edge VLAN Configuration
Device: 10.77.241.4

```bash
vlan 3
  name VLAN0003
interface VLAN3
  ip vrf forwarding GreenVRF
  ip address 10.77.22.3 255.255.255.2
  no shutdown
glbp 1 ip 10.77.22.23
  ip helper-address 255.255.255.0
```

Understanding Edge VLAN Configuration Details
The following VRF configuration details are pushed in the selected devices. The description of the Edge VLAN Configuration details is given in Table 12-20.

**Table 12-20 Edge VLAN Configuration details**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip vrf forwarding vrf-name</code></td>
<td>Enters VRF configuration mode and assigns a VRF name</td>
</tr>
<tr>
<td><code>description vrf-name</code></td>
<td>Provides description of the VRF created</td>
</tr>
<tr>
<td><code>ip address vrf-name</code></td>
<td>Associates a VRF with an interface or sub-interface</td>
</tr>
<tr>
<td><code>no shutdown</code></td>
<td>Converts Layer 2 switch port interface to a Layer 3 routed physical interface</td>
</tr>
<tr>
<td><code>glbp</code></td>
<td>Enables IEEE 802.1Q encapsulation of traffic on a specified sub-interface in virtual LANs. IEEE 802.1 Q is a standard protocol for interconnecting multiple switches and routers, and for defining VLAN topologies.</td>
</tr>
<tr>
<td><code>ip helper-address</code></td>
<td>Used to enable an interface</td>
</tr>
</tbody>
</table>

To assign VLANs on the selected interfaces, to a VRF, click **Finish** in the Edge VLAN Configuration: Summary page.
A job is created to assign edge VLAN to the selected VRF. A confirmation message appears with the Job ID in the Information dialog box.

To view the VRF configuration job status, go to Configuration > Job Browsers > VRF Lite. See Using VRF Lite Job Browser.
Using VRF Lite Job Browser

The VRF Lite Configuration Jobs browser enables you to view the status of all VRF configuration jobs. VRF configuration jobs are the jobs that are created for the VRF configuration workflows like Create, edit, extend and delete VRF as well as Edge VLAN Configuration jobs.

The job details like the job ID, the job type, the job description, the job owner, the time the job is scheduled to run at, the time of job completion, the schedule type, the job status, run status can be viewed here. Table 12-21 describes the fields in the VRF Lite Configuration Jobs browser.

To access the VRF Lite Configuration Jobs browser, select **Configuration > Job Browsers > VRF Lite**. The VRF Lite Configuration Jobs browser page appears.

You can manage the VRF configuration jobs using the VRF Lite Configuration Jobs browser.

### Note
View the Permission Report (Reports > System > Users > Permission) to check whether you have the required privileges to perform this task.

The VRF Lite Configuration Jobs browser is used to perform the following:

- **View**—Used to launch reports. See **View**.
- **Stop**—Stop a scheduled or running job. See **Stop Job**.
- **Retry**—Retry a job. See **Retry Job**.
- **Delete**—Delete a job. See **Delete Job**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique ID assigned to the VRF configuration job when it is created.</td>
</tr>
<tr>
<td></td>
<td>Clicking the Job ID hyperlink provides a report page with the job details of the job.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Type of VRF configuration job such as Create VRF, Edit VRF, Extend VRF, Delete VRF and Edge VLAN Configuration.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the job provided by the job creator.</td>
</tr>
<tr>
<td>Owner</td>
<td>User who created the job.</td>
</tr>
<tr>
<td>Scheduled At</td>
<td>Date and time the job was scheduled at.</td>
</tr>
<tr>
<td>Completed At</td>
<td>Date and time the job was completed at.</td>
</tr>
</tbody>
</table>
Using VRF Lite Job Browser

Chapter 12 Configuring Virtual Routing and Forwarding (VRF)

### Table 12-21  VRF Lite Configuration Jobs Browser

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Status</td>
<td>Job states include:</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Waiting for approval</td>
</tr>
<tr>
<td></td>
<td>• Scheduled (pending)</td>
</tr>
<tr>
<td></td>
<td>• Succeeded</td>
</tr>
<tr>
<td></td>
<td>• Succeeded with Info</td>
</tr>
<tr>
<td></td>
<td>• Failed</td>
</tr>
<tr>
<td></td>
<td>• Crashed</td>
</tr>
<tr>
<td></td>
<td>• Cancelled</td>
</tr>
<tr>
<td></td>
<td>• Suspended</td>
</tr>
<tr>
<td></td>
<td>• Rejected</td>
</tr>
<tr>
<td></td>
<td>• Missed Start</td>
</tr>
<tr>
<td></td>
<td>• Failed at Start</td>
</tr>
<tr>
<td>Schedule Type</td>
<td>Specifies the type of schedule for the job:</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs once at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>• Daily—Runs daily at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly—Runs weekly on the day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Monthly—Runs monthly on the day of the month and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs immediately.</td>
</tr>
<tr>
<td>Status</td>
<td>Provides the status of the current jobs. The status of the current jobs is displayed as succeeded or failed.</td>
</tr>
</tbody>
</table>

### View

Use to launch the respective report of the VRF configuration job selected in the VRF Lite Configuration Jobs Browser page.

### Stop Job

You can stop a scheduled or running job from the VRF Lite Configuration Jobs Browser.

Select the job and click **Stop**. You are prompted for a confirmation before the job is stopped. You can select only one job to stop at a given time.
Delete Job
You can delete a VRF configuration job from the VRF Lite Configuration Jobs Browser.
Select the job and click **Delete**. You are prompted for a confirmation before the job is deleted. You can select more than one job to delete.

Retry Job
You can retry a VRF configuration job related to VRF configuration from the VRF Lite Configuration Jobs Browser. You can retrieve only failed jobs. Select the job and click **Retry**. You are prompted for a confirmation before retrying the job. You can select only one job to be retried at a given time.
Viewing Topology Services

Topology Services is an application that enables you to view and monitor your network including the links and the ports of each link.

Topology Services display the network topology of the devices discovered by LMS through Topology Maps. Besides these Maps, the application includes numerous reports that helps you to view the physical and logical connectivity in details.

To launch Topology Services, either:

- Select Configuration > Topology from the menu.
- Or
  - Select Monitor > Monitoring Tools > Topology Services from the menu.

You must install the Java plug-in to access Topology Services from a client. If you are prompted to install the Java plug-in, download and install it using the installation screens.

See Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.2 for more information.
CLI Utilities

LMS provides Command Line Interface (CLI) support. The CLI utilities that are supported by LMS are:

- CWCLI
- Performance Tuning Tool
- syslogConf.pl Utility
- Software Management CLI Utility

CWCLI

CiscoWorks Command Line Framework (CWCLI) is the interface or framework through which application functionality is provided.

The following are the `cwcli` applications:

- `cwcli config` is the configuration command-line tool. `cwcli netconfig` command lets you use NetConfig from the command line.
- `cwcli export` is a command line tool that also provides servlet access to inventory, configuration and change audit data. This can be used for generating inventory, configuration archive, and change audit data for devices in LMS.
- `cwcli inventory` is a Device Management application command line tool. This tool can be used for checking the device credentials, exporting the device credentials. You can also view the devices and delete the devices.
- `cwcli invreport` is a CiscoWorks command line tool which allows you to run previously created Inventory Custom Reports and also system reports. The output is displayed in the Comma Separated Value (CSV) format.
- `cwcli netshow` is a command line tool that lets you use NetShow features from the command line. You can use the `cwcli netshow` commands to view, browse, create, delete, and cancel NetShow jobs and Command Sets.

This appendix contains the following sections:

- Overview: CLI Framework (cwcli)
- Overview: cwcli config Command
- Overview: cwcli netconfig Command
- Overview: cwcli export Command
• Overview: cwcli inventory Command
• Overview: cwcli invreport Command
• Overview: cwcli netshow Command

You can set the debug mode for CLIFramework and ConfigCLI in the Log Level Settings dialog box (Admin > System Preferences > Loglevel Settings).

Overview: CLI Framework (cwcli)

CLI Framework (cwcli) is a Command-Line Interface. This interface provides application-related functionality.

The CLI Framework supports the following tasks:
• Parsing the command line for the applications.
• Easy logging and messaging capabilities
• Authentication and authorization for individual applications
• Remote access support.

This section contains:
• cwcli Global Arguments
• Remote Access

SYNOPSIS

The command line syntax is as follows:

cwcli application command GlobalArgs AppSpecificArguments

• application specifies one or more LMS applications that use the framework. For example, config, export, inventory, invreport, and netconfig.
• command specifies which core operations are to be performed for a particular service.
• GlobalArgs specifies arguments common for all CLI. For example, username, password, log, debug, etc.
• AppSpecificArguments are the additional parameters required for each core command.

You should enter the application name immediately after cwcli and the command name, after the application name. All other GlobalArgs arguments can be specified in any order.

Apart from the applications, Global args (-u user, -p password, -l logfile, -m email, -d debuglevel) framework also supports two generic commands. They are:
• -v—Version of the CLI interface.
• -help—All the applications that can be invoked using the framework.

SYNTAX

cwcli -v
cwcli -help
**cwcli Global Arguments**

The following table shows the `cwcli config` command arguments you can specify with all commands.

<table>
<thead>
<tr>
<th>cwcli arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-u userid</code></td>
<td>User ID. Field is required.</td>
</tr>
</tbody>
</table>
| `-p password`   | It is the password for the specified User ID. If you enter the password at the command line, a message appears:  
* Warning * The `-p` option is highly insecure and *not* recommended. See `-u` option for more details. |
| `-device devicename or device_list` | Device Name of the device added into DCR. You can use comma separated displaynames and wildcard character `%`. For example, if there are two devices with names Rtr12 and Rtr13, Rtr% will display both the devices. To use all the devices, use `-device %`. |
| `-view view_list` | If the data needs to be generated for all the devices in a specific group, you can use the `-view` argument. You can use this argument to generate data for devices in all device views including system-defined groups and user-defined groups. You can enter multiple group name separated using a comma. For view name, you have to enter the fully qualified path as in the Group Administration window. To separate the path you must use forward slash only. For example, `-view="/RME@ciscoworks_servername/All Devices"` |
| `-ipaddress address` | Device IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated. You cannot use this option with `-device, -view, or -input`. Also, you cannot specify wildcard characters. |
| `-l logfile` | Must be a relative name. By default ConfigCLI.log and cli.log files are used, located at:  
• `NMSROOT\log` (On Windows)  
• `/var/adm/CSCOpx/log` (On Solaris and Soft Appliance)  
If the relative name is specified then the log messages are logged into the file specified. The file is created under the log directory, mentioned above. For example, `cwcli config export -u alpha -p beta -device % -l export.log`. In this case, export.log is created under the log directory mentioned above. |
| `-m email` | Email address to mail the command output to. You can enter single or comma separated email IDs. |
| `-d debuglevel` | Enables debugging to command-line tool. Specifies debugging verbosity. Default is least verbose. |
Appendix A      CLI Utilities

CWCLI

Note
-d and -l arguments are supported for backward compatibility. Select Admin > System > Debug Settings > Config and Image Management Debugging settings > CLI Framework to set debug levels.

When using wildcards, you must use the percent sign (%), not an asterisk (*), as shown in the following examples:
%device (lists all devices that end with the suffix ‘device’)
dev% (lists all devices that start with the prefix ‘dev’)
% (lists all devices LMS manages)

Remote Access

CLI framework (cwcli) offers remote access facilities to allow you to invoke cwcli commands from the client in the same way as they run on the LMS server.

The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to run any command:
For post-request,
http://lms-server:lms-port/rme/cwcli payload XML file
For get request,
http://lms-server:lms-port/rme/cwcli?command=cwcli config commandname -u user -p BAse64 encoded pwd -args1 arg1value...

Note
Use <arg> and <argval> tags when the argument is a file.

The contents of the payload xml file is as follows.
<payload>
 <command>
  cwcli config export -u admin -p <Base64Encoded pwd> -device 1.1.1.1 -xml
 </command>
 <arg>
 </arg>
 <arg-val>
 </arg-val>
</payload>

For example to run the cwcli config import comand payload.xml is as follows:
<payload>
 <command>
  cwcli config import -u admin -p <Base64Encoded pwd> -device 10.77.240.106
 </command>
 <arg>

<table>
<thead>
<tr>
<th>cwcli arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help</td>
<td>Displays usage information.</td>
</tr>
<tr>
<td>-input</td>
<td>Text file containing arguments for each device.</td>
</tr>
</tbody>
</table>
The Remote Access servlet creates a temporary file with the contents specified between the arg-val tags for the import command. On the server the command is run as
\[ \text{cwcli config import} \ -u \text{admin} \ -p \text{Base64Encoded pwd} \ -d \text{device} \ 10.77.240.106 \ -f \text{tempfile}\]
Here, the tempfile contains the configuration of the device that you want to import.

For example,
\[ \text{perl samplescript.pl http(s)://lms-server:lms-port/rme/cwcli/payloadXML}\]
To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

**Note**
For the secure mode (HTTPS) the port number is 443. The default port for LMS server in HTTP mode is 1741.

**Sample Script to Invoke the Servlet**
```perl
#!/opt/CSCOpx/bin/perl
use LWP::UserAgent;
$temp = $ARGV[0] ;
$fname = $ARGV[1] ;
print " argv[0} = $ARGV[0] , fname = $fname 
",
open (FILE,"$fname") || die "File open Failed $!");
while { <FILE> }
    { $str .= $_ ;
        while { <FILE> }
            { $str .= $_ ;
                #print $str ;
                url_call($temp);
                #-- Activate a CGI:
                sub url_call
                {
                    my ($url) = @_; my $ua = new LWP::UserAgent;
                    $ua->timeout(1000); # you can set timeout value depending on number of devices
                    my $hdr = new HTTP::Headers 'Content-Type' => 'text/html';
                    my $req = new HTTP::Request ('GET', $url, $hdr);
                    $req->content($str);
                    print "It comes here \n";
                    my $res = $ua->request ($req);
```
my $result;
#    print "It comes here too \n";
if ($res->is_error)
{
    print "ERROR : ", $res->code, ", ": ", $res->message, ";\n";
    $result = '\';
    if ($res->message =~ /read timeout/)
    {
        print "ERROR:Timeout has occured. Increase the timeout value in samplescript.pl.\nFor example, if the devices managed in network is more than 1k, increase the timeout value to 5000.";
    }
    }
else {
    $result = $res->content;
    if($result =~ /Authorization error/)
    {
        print "Authorization error\n";
    }
    else {
        print "\n$result" ;
    }
    }
}

Setting CWCLIFILE Environment Variable

You can store your username and password in a file and set a variable CWCLIFILE that points to the file. This helps you to avoid the -p argument, which will reveal the password in clear text in CLI.

You should maintain this file and control access permissions to prevent unauthorized access.

If CWCLIFILE is set only to filename instead of full path, cwcli framework looks for the current working directory.

If you use the -p argument, even after setting the CWCLIFILE variable, the password is taken from the command line instead of CWCLIFILE. This is not secure and usage of this argument is not recommended.

The password must be provided in the file in the following format:

username password

where username and password are the LMS login credentials. The delimiter between the username and password is a single space.

You must enter comma as the delimiter if the password is blank. Otherwise, cwcli framework will fail to validate the password.

Example to run the cwcli command with the CWCLIFILE file:

On Windows, at the command prompt enter:

C:\Program Files\CSCOpx\bin>set CWCLIFILE=D:\ciscoworks\password.txt
C:\Program Files\CSCOpx\bin>cwcli export changaudit -u admin -view "/RME@ciscoworksservername\Normal Devices"

Where the file, password.txt contains the username and password for LMS server.
Overview: cwcli config Command

The `cwcli config` command-line tool performs the following core functions on one or more devices and the configuration archive:

- Moves configuration files from the configuration archive to one or more devices.
- Transfers the configuration files from devices to the archive if the configuration running on a device is different from the latest archived version.
- Imports configuration files from the file system and pushes them to one or more devices, which updates the configuration archive.
- Merges the startup configuration files with the running configuration files.
- Copies the running configuration files to the startup configuration files.
- Copies a configuration file to the startup configuration files.
- Copies the difference between a configuration file and the running configuration to the running configuration files. This makes the configuration in the file available on the running configuration.
- Reboots running devices to load a running configuration with its startup configuration.

In addition, `cwcli config` performs the following core functions on the configuration archive:

- Exports configurations from the archive to the filesystem.
- Compares any two configuration files in the archive based on version or date.
- Deletes configurations older than a specified date from the configuration archive.

This section contains:

- Using the cwcli config Command for Batch Processing
- Getting Started With cwcli config
- Uses of cwcli config
- Remote Access
- Running cwcli config
- cwcli config Command Parameters
- Parameters For All cwcli config Commands
- cwcli config Syntax Examples
- cwcli config Core Arguments
- Examples of cwcli config
- cwcli config Command Man Page
- Arguments
- cwcli config Subcommand Man Pages

Using the cwcli config Command for Batch Processing

In addition to using the graphical-based device configuration functions, you can use the `cwcli config` command-line utility to perform batch processing tasks on the configuration archive, devices, or on both.

For more details see these sections:

- Running cwcli config
• cwcli config Core Arguments
• Examples of cwcli config

On platforms other than Windows 2000, all files created by cwcli config are owned by casuser. They belong to the same group as the user (casuser) who created the files, and have read-write access for both casuser and the group.

Note
Your login determines whether you can use this argument.

Getting Started With cwcli config

cwcli config is a command-line tool. This tool is like an interface between the user and the device and the configuration archive.

Generally, the configuration archive automatically registers modifications to the device's configuration in archived, version-based files. Over time, multiple configurations of a device accumulate in the archive. Typically, the latest version is the configuration running on the device.

Uses of cwcli config

With cwcli config, you can:

• Device and Archive Updates
  Modify a device's running configuration. You can allow personnel of your organization to modify the device's configuration without explicitly providing them with Telnet access to the device.

• Deleting Configurations
  Delete unwanted versions of the configuration file from the archive. This is a command-line variant of the UI purge feature.

• Comparing Configurations
  Generate 'diffs' of different configuration versions of the same device to find out what modifications were made. This is a command-line counterpart for GUI-based reports.

Device and Archive Updates

Whenever you use cwcli config to update the running configuration of the device, the tool also archives the newly written configuration to the archive, bypassing the auto-detection mechanism.

Getting a Version of the Device Configuration

To obtain a version of the device's configuration from the device, modify it, and then write it back to the device. You use two features of cwcli config to do this.

1. Use the export command to obtain a copy of the desired configuration version file.
2. Edit and deploy it on the device using the import function. If the update succeeds, import also archives the configuration in the archive as the latest version.

Example:

cwcli config export -u user -p pass -device zebra.domain.com -version 3 -f zebraconf
version 3 of device zebra's configuration has been obtained from the device. It is available in the file zebraconf. You must edit the file and make the necessary modifications.

cwcli config import -u user -p pass -device zebra.domain.com -f zebraconf

The edited file is written back to the device and archive. If there were five configurations originally, a sixth one is now added.

If you want to update the running config on the device, and are certain that the latest archived version is the same as the running config, then you can obtain the latest version as follows:

cwcli config export -u user -p pass -device zebra.domain.com -f zebraconf

the latest version is copied to file zebraconf.

After writing the edited configuration to the device, you might want to reboot the device. You can do this automatically from cwcli config by using the -reboot argument to the import command:

cwcli config import -u user -p pass -device zebra.domain.com -f zebraconf -reboot

In addition, you might want to write file zebraconf to both the running as well as the startup configuration. To do this, enter the following command:

cwcli config export -u user -p pass -device zebra.domain.com -f zebraconf -save

Reverting to Earlier Configuration Version

For running configuration, use either compare or export to decide, which version to revert to.

For VLAN configuration, look into the Configuration Version Report for the device to find the versions for which VLAN configuration is also archived. Then use put to deploy the desired version.

The put function gets the requested version from the archive, writes it to the device. For Running configuration, it archives it as the latest version of that device.

Example:

cwcli config put -u user -p pass -device zebra.domain.com -version 3

version 3 of device zebra's configuration is extracted from the archive and written to the device. It is also stored in the archive as the latest version.

Example:

cwcli config put -u user -p pass -device zebra.domain.com -version 3 -filetype vlan

version 3 of device zebra's vlan configuration is extracted from the archive and written to the device.

Like import, the put function allows you to reboot the device using the -reboot argument, and to update the startup configuration using the -save argument.

Writing Startup Configuration to Running Configuration

To write the startup configuration of the device to its running configuration. Use the start2run function of cwcli config to retrieve the startup configuration from the device, and then write it back to the device's running configuration. The new running configuration is archived as the latest version.

Example:

 cwcli config start2run -u user -p pass -device zebra.domain.com

To ensure that the running configuration on the device is stored in the archive, that is, synchronize the archive with the device. Use the get function to do so.

Example:

 cwcli config get -u admin -p admin -device zebra.domain.com
The running configuration of device zebra is retrieved from the device and archived as the latest version, only if there is a need to do so. However, if the running configuration does not differ from the latest archived version, then the archival does not take place.

Configuration updates can be performed on multiple devices at once. For more details see “Running cwcli config on Multiple Devices” section on page A-11.

Deleting Configurations

Use the `delete` function of `cwcli config` to delete unwanted versions from the archive, to conserve disk space, and to reduce visual clutter on reports.

Example:

```
cwcli config delete -u user -p pass -device zebra.domain.com -version 2 5
```

All versions between and including 2 and 5 are removed from the archive. There is also a time-stamp based variant.

Comparing Configurations

Use the `compare` function to compare any two versions of the archived configuration files of one or more devices. The compare function also lists down the entire configuration changes based on the timestamp.

Example:

```
cwcli config compare -u user -p pass -device zebra.domain.com -version 2 5
```

cwcli config can only compare the archived configuration files. The compliance report is stored in the job directories.

Remote Access

`cwcli config` uses remote access facilities offered by the CLI framework to allow you to invoke the `cwcli config` commands from the client in the same manner they would run them on the LMS server.

The name of the servlet is `/rme/cwcli`.

All the command can be run remotely.

**Note**

For the secure mode (HTTPS) the port number is 443. The default port for LMS server in HTTP mode is 1741.

Running cwcli config

The `cwcli config` command is located in the following directories, where `install_dir` is the directory in which LMS is installed:

- On Solaris and Soft Appliance systems, `NMSROOT/bin`. The default directory is `/opt/CSCOpx`
- On Windows systems, `NMSROOT\bin`

    The default install directory is `C:\Program Files`.

If you install LMS on Windows on an NTFS partition, only users in the administrator or casuser group can access `cwcli config`.

Users with read-write access to the `CSCOpx\files\archive` directory and the directories under that can also use `cwcli config`.
Running cwcli config on Multiple Devices

You can run `cwcli config` simultaneously on multiple devices. Details vary from command to command. This section describes how to apply import on multiple devices. Details of multiple-device syntax for other commands are described under the DESCRIPTION in the man page.

The commands, such as `put`, `import`, `write2run` and `write2start` accept only one device on the command line. If you want to apply the command to multiple devices, enter the names of those devices and any arguments in a text file.

For example, assume that you want to deliver the configuration file `serviceconf` to devices, antelope and rhino. Also assume that you want to reboot rhino. The command line of `cwcli config` is as follows:

```
cwcli config import -u admin -p admin -input device-list -m root@netcontrol.domain.com
```

You do not want the output of the command to go to stdout. Instead, you want it to be mailed to the superuser at host netcontrol.

Device-list is a text with the following contents:

```
# comments start with a leading hash symbol. Write serviceconf to rhino and # antelope. reboot antelope.
-device rhino.domain.com -f serviceconf
-device antelope.domain.com -f serviceconf -reboot
# end of input file device-list
```

Additional Information

The examples in this man page are not comprehensive. There are many other scenarios in which `cwcli config` can be used.

For example, if you want to modify the running configuration on the device, without using the latest archived version, considering the latest may not be the same as the running configuration. You can apply the `get` command and then export and import. Various combinations of the features can be used.

You can also use `cwcli config` in UNIX cron jobs to schedule config updates in advance.

Also, the output generated by `cwcli config` can be logged to a file and sent to any recipient through email. A host of additional arguments can be applied on other commands.

cwcli config Command Parameters

Using the `cwcli config` commands you can manipulate, deploy and archive your device configuration files.

- Using the Compare Command
- Using the Delete Command
- Parameters For All cwcli config Commands
- cwcli config Syntax Examples

Using the Compare Command

When you specify the `compare` command, both `-version` and `-date` are optional.

- If you do not specify `-version` or `-date`, the latest configuration is compared with the previous version.
• If you do specify **-version** or **-date**, and the value you enter is the latest version or date, that configuration is compared with the previous version.
Using the Delete Command

When you specify the `-date` command, you must specify `-version` or `-date`.

If you specify only one date, all versions archived up and including that date are deleted.

To delete a version archived on a particular date, specify two dates that are the same date as the archived version date. The latest two versions of configuration can never be deleted from the archive. Be careful while using the `delete` command.

Parameters For All `cwcli config` Commands

The `-d` and `-l` arguments are supported for backward compatibility.

In LMS, select `Admin > System > Debug Settings > Config and Image Management Debugging settings > ConfigCLI` to set debug levels.

When using wildcards, you must use the percent sign (%), not an asterisk (*), as shown in the following examples:

```%
%device
dev%
%device%
```

The following table lists the `cwcli config` command-specific arguments and which commands you can use the arguments with:

<table>
<thead>
<tr>
<th>cwcli config arguments</th>
<th>Applicable Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-baseline</code></td>
<td>createdeployparamfile, directbaselinedeploy</td>
<td>Specifies the name of the Baseline template for which the parameter file has to be created.</td>
</tr>
</tbody>
</table>
| `-date`                | compare, delete    | • Compare  
  – If you specify one date, the latest configuration version is compared with the most recently archived version on that particular date.  
  – If you specify two dates, the most recently archived version of the first date is compared with the most recently archived version of the second date.  
• Delete  
  – If you specify one date, all versions archived up to this date are deleted.  
  – If you specify two dates, all versions archived between and on those dates are deleted. |
<p>| <code>-enable_pass</code>         | import, put, write2run, write2start, run2start, start2run, deploycomplianceresults, compareanddeploy, reload | Specifies execution mode Base64 encoded Password for connecting to device. |</p>
<table>
<thead>
<tr>
<th>cwcli config arguments</th>
<th>Applicable Commands</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-filename`            | `export, import`   | Specifies fully qualified pathname of configuration file to import to or export from.  
• If you do not specify this argument, the current working directory is assumed.  
• If you do not specify this argument when importing or exporting a single device configuration, default filename, devicename.cfg, in the current working directory is assumed.  
The `-filename` argument applies only to single devices. To perform the operation on multiple devices, you must specify the `-input` argument. |
| `-input inputlist`     | Applicable to all commands except `compareanddeploy, createdeployparamfile, deploycomplianceresults, and directbaselinedeploy.` | You must enter `-input inputlist` to run commands, such as `put` and `import`, on multiple devices.  
The parameter, `inputlist` is a text file containing arguments for each device. A line starting with `#` is treated as a comment.  
For example, an input list file might look like this:  
```  
#comment line  
-version version [-save] [-reboot] device_name  
-version version [-save] [-reboot] device_name  
```
| `-jobid`               | `createdeployparamfile` | Used to specify the job identifier of the previously run `comparewithbaseline` job. |
| `-l`                   | `createdeployparamfile, directbaselinedeploy` | Specifies the file to log the results of the command. |
| `-listonly`            | `write2run`          | Displays difference between the latest running configuration for device in configuration archive and new configuration that is generated, without downloading changes. |
| `-m`                   | `createdeployparamfile, directbaselinedeploy` | Specifies an email address to send the results of the command. |
| `primary_pass`         | `import, put, write2run, write2start, run2start, start2run, deploycomplianceresults, compareanddeploy, reload` | Specifies primary user name for connecting to device. |
| `-primary_user`        | `import, put, write2run, write2start, run2start, start2run, deploycomplianceresults, compareanddeploy, reload` | Specifies primary user name for connecting to device. |
| `-reboot`              | `import, put`        | After successfully pushing a configuration to a device, device reboots. By default the device does not reboot.  
For IOS devices, you must also specify `-save` to avoid losing configuration changes when rebooting. |
<p>| <code>-save</code>                | <code>import, put</code>        | Applies to Cisco IOS devices only. Performs a write memory after pushing the configuration. The default is no write memory. |</p>
<table>
<thead>
<tr>
<th>cwcli config arguments</th>
<th>Applicable Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-timeout</td>
<td>import, put, write2run, write2start, run2start, start2run, comparewithbaseline, deploycompliancresults, compareanddeploy, get, reload</td>
<td>Specifies the duration of the interval in seconds between two successive polling cycles. Configuration Archive is polled according to the interval specified to retrieve and display the job results.</td>
</tr>
<tr>
<td>-version version</td>
<td>compare, delete, export, put</td>
<td>• For put and export, you can specify one version of the configuration in the archive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For compare, you can specify two versions, which are compared with each other.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you specify only one version, that is compared with latest archived version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For delete, if you specify one version, that version is deleted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you specify two versions, all versions in between and including those version are deleted.</td>
</tr>
</tbody>
</table>

**cwcli config Syntax Examples**

The following examples demonstrate the `cwcli config` command syntax. Square brackets ([ ]) indicate arguments. A pipe (|) acts as a delimiter. This means that only one of the listed entries can be specified.

---

**Note**

Make sure you first use the `cwcli config` command in a test environment before running the command in production. This is to avoid any loss of data when a device is rebooted or a configuration is overwritten.

The following command extracts the running configurations from all devices:

```
cwcli config get -u user -p password -device %
```

The following command exports the configuration of all the devices from the archive and puts the configuration into the file, devicename.cfg. This is the default file name because `-f` is not specified:

```
cwcli config export -u user -p password -device %
```

If there is more than one device in the default view All, you see an error message because the `export` command does not accept multiple device names on the command line. You must specify the `-input` argument to run the `export` command on more than one device.
The following table shows more syntax examples:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Syntax</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>no arguments</td>
<td><code>cwcli config -u user -p password [-v -help]</code></td>
<td>If you do not specify arguments, cwcli config shows command usage (-help)</td>
</tr>
<tr>
<td>compare</td>
<td>`cwcli config compare -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-device list] [-view name] [-ipaddress list] {-version version1 [version2]</td>
<td>Specify versions to compare using -version or -date argument. When specifying a date, use format mm/dd/yyyy. If you do not specify a date or a version, the latest two archived configurations are compared.</td>
</tr>
<tr>
<td>compareanddeploy</td>
<td>`cwcli config compareanddeploy -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-device list] [-view name] [-ipaddress list] { -version version1 [version2]</td>
<td>Creates a job that compares the given Baseline template with the latest version of the configuration for a device and downloads the configuration to the device if there is non-compliance.</td>
</tr>
<tr>
<td>comparewithbaseline</td>
<td>`cwcli config comparewithbaseline -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-device list] [-view name] [-ipaddress list] { -version version1 [version2]</td>
<td>Creates a job that compares the given Baseline template with the latest version of the configuration for a device. In case of non-compliance, the non-compliant commands are displayed.</td>
</tr>
<tr>
<td>delete</td>
<td>`cwcli config delete -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-device list] [-view name] [-ipaddress list] { -version version1 [version2]</td>
<td>Deletes the specified device configuration from the archive. Use -date or -version argument to specify configurations to delete. If you specify two dates, all configurations archived between those dates are deleted. If you specify two versions, all configurations between and including the versions are deleted.</td>
</tr>
<tr>
<td>deploycomplianceresults</td>
<td>`cwcli config deploycomplianceresults -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-device list] [-view name] [-ipaddress list] { -version version1 [version2]</td>
<td>Creates a job that uses the previously executed comparewithbaseline job to get the non-compliance commands and create a job. It replaces the parameters in the non-compliant commands with the values from the data file. The commands are then downloaded to ensure compliance with the baseline configuration.</td>
</tr>
<tr>
<td>export</td>
<td>`cwcli config export -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-device list] [-view name] [-ipaddress list] { -version number} [-f filename] [-version</td>
<td>Retrieves a configuration version for a device from the archive and writes it to a file. Exported configurations are named devicename.cfg if -f argument is not used.</td>
</tr>
</tbody>
</table>
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Syntax</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>import</td>
<td>`cwcli config import -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-device displayName] [-ipaddress address] [-f filename] [-save</td>
<td>-reboot] [-input argumentFile]`</td>
</tr>
<tr>
<td>listversions</td>
<td><code>cwcli config listversions -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-device list] [-view name] [-device displayName] [-viewname] [-ipaddress list] -baseline</code></td>
<td>Lists the versions of the configuration archived for a device on the main branch or the Baseline templates applicable to a device.</td>
</tr>
<tr>
<td>put</td>
<td>`cwcli config put -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-device displayName] [-ipaddress address] [-version number] [-config 1</td>
<td>2] [-save</td>
</tr>
<tr>
<td>run2start</td>
<td><code>cwcli config run2start -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-device list] [-view name] [-device list] [-view name] [-ipaddress list] [-input argumentFile][-timeout seconds] [-primary_user primary user name] [-primary_pass Base64 encoded primary password] [-enable_pass Base64 encoded enable password]</code></td>
<td>Creates a job that overwrites the startup configuration of device with running configuration. Specify multiple devices with <code>-device</code> argument by separating each device name with comma or with <code>-input</code> argument, which takes filename containing the multiple devices as an argument.</td>
</tr>
<tr>
<td>Argument</td>
<td>Syntax</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>start2run</td>
<td>cwcli config start2run -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-device list] [-view name] [-config 1</td>
<td>2] [-input argumentFile][-timeout seconds] [-primary_user primary user name] [-primary_pass Base64 encoded primary password] [-enable_pass Base64 encoded enable password]</td>
</tr>
<tr>
<td>write2run</td>
<td>cwcli config write2run -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-ipaddress list] [-f filename] [-config 1</td>
<td>2] [-listonly] [-input argumentFile][-timeout seconds] [-primary_user primary user name] [-primary_pass Base64 encoded primary password] [-enable_pass Base64 encoded enable password]</td>
</tr>
</tbody>
</table>
### Appendix A      CLI Utilities

#### CWCLI

<table>
<thead>
<tr>
<th>Argument</th>
<th>Syntax</th>
<th>Notes</th>
</tr>
</thead>
</table>
You can specify a filename by using the `-input` argument.  
The input file should be of this format:  
`-device 1.1.1.1,2.2.2.2,3.3.3.3 -filetype vlan`  
or  
`-filetype vlan -device 1.1.1.1,2.2.2.2,3.3.3.3`  
The `-filetype` should be either `vlan`, `running` or `startup`.  
If `-filetype` is not specified, then running will be taken as the default filetype value.  
The output contains device name, time of last config collection, and the filetype separated by comma. |
You can specify a filename by using the `-input` argument.  
The input file should be of this format:  
`-device 1.1.1.1,2.2.2.2,3.3.3.3 -filetype vlan`  
or  
`-filetype vlan -device 1.1.1.1,2.2.2.2,3.3.3.3`  
The `-filetype` should be either `vlan`, `running` or `startup`.  
If `-filetype` is not specified, then running will be taken as the default filetype value.  
The output contains device name, time of last attempt, and the filetype separated by comma. |

### cwcli config Core Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| compare  | Compares last two configurations in archive, specific configuration versions, or configuration changes based on a specified date.  
To run this command on multiple devices, specify `-device` argument or `-input` argument. |
| delete   | Deletes configurations older than specified date or version from archive.  
To run this command on multiple devices, specify `-device` argument or `-input` argument. |
| export   | Retrieves latest configuration from archive and writes it to specified file.  
To run this command on multiple devices, specify `-input` argument. |
## CWCLI

<table>
<thead>
<tr>
<th>cwcli config Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>get</strong></td>
<td>Pulls configuration from device to configuration archive if configuration is different from latest archived configuration. To run this command on multiple devices, specify -device argument or -input argument.</td>
</tr>
<tr>
<td><strong>import</strong></td>
<td>Imports configuration from specified file and pushes it to devices. To run this command on multiple devices, specify -input argument.</td>
</tr>
<tr>
<td><strong>put</strong></td>
<td>Pushes configuration files from the configuration archive to device based on version. To run this command on multiple devices, specify -input argument.</td>
</tr>
<tr>
<td><strong>reload</strong></td>
<td>Reboots devices to reload running configuration with startup configuration. To run this command on multiple devices, specify -device argument or -input argument.</td>
</tr>
<tr>
<td><strong>run2start</strong></td>
<td>Overwrites startup configuration with running configuration. To run this command on multiple devices, specify -device argument or -input argument.</td>
</tr>
<tr>
<td><strong>start2run</strong></td>
<td>Merges startup configuration with running configuration. To run this command on multiple devices, specify -device argument or -input argument.</td>
</tr>
<tr>
<td><strong>write2run</strong></td>
<td>Downloads difference between latest running configuration for the device in configuration archive with configuration in file specified by -f argument. To run this command on multiple devices, specify -input argument.</td>
</tr>
<tr>
<td><strong>write2start</strong></td>
<td>Erases the contents of the device’s startup configuration and writes the contents of the given file as the device’s new startup configuration. To run this command on multiple devices, specify -input argument.</td>
</tr>
<tr>
<td><strong>collectiondate</strong></td>
<td>Displays the last config collection date for the devices. To run this command on multiple devices, specify -device argument or -input argument.</td>
</tr>
<tr>
<td><strong>accessdate</strong></td>
<td>Displays the last config collection attempt date for the devices. To run this command on multiple devices, specify -device argument or -input argument.</td>
</tr>
</tbody>
</table>

### Examples of cwcli config

The following `cwcli config` command retrieves configurations for all devices in the LMS home_routers domain and stores the configurations in Sybase:

```
cwcli config get -u adam -p max -view home_routers
```

where home_routers is a device view.

The following `cwcli config` command reads inputfile and, for each device listed, pushes the appropriate configuration to that device:

```
cwcli config import -U adam -P max -input /tmp/inputfile
```

### cwcli config Command Man Page

This man page is also accessible from the command line of a LMS server installed on a UNIX system.

To view the man page, add the path install_dir/CSCOpx/man to the MANPATH variable. Then you can enter the command man `cwcli config` from any directory.
You can also access man pages for each `cwcli config` command by entering the command `man cwcl-command`, where command is the command name (for example, `export`). The man pages for each subcommand are also available in this help system.

**NAME**

cwcli config LMS command line interface for the device configuration archive

**SYNOPSIS**

cwcli config command [-arg1 [arg1Value] -arg2 [arg2Value] -argN [argNValue]]
cwcli config -help

**DESCRIPTION**
cwcli config is a LMS command line tool that allows you to access the configuration archive or configurations on devices. You can use `cwcli config` to update, export, and import configurations on devices and in the archive. You can also compare configurations and delete old configurations.

To get a list of supported commands, run the command

cwcli config -help

or

cwcli config?

Help on each command can be obtained in the following manner:

cwcli config command -help

For example:

cwcli config export -help

Additionally, man pages are available on UNIX installations for individual commands. To view the man page for any command, enter:

`man cwcl-command`

For example:

`man cwcl-export`
Arguments

Many of the arguments are common across all commands. These arguments can be broadly classified as those that are expected by every command (function independent) and those that are specific to the context of a command.

- Mandatory Arguments
- Function-independent Arguments
- Function-dependant Arguments
- Function-specific Arguments
- Common Arguments
- Command Arguments

Mandatory Arguments

You must use the following arguments with all commands.

- `u userid`
  Specifies the LMS username. You must define an environment variable `cwcli CWCLIFILE` with value set to a filename, which will contain the corresponding password.

  The file has to be maintained by you. You can control the access permissions of this file to prevent un-authorized access. `cwcli config` looks for current working directory if `cwcli CWCLIFILE` is set to only file name instead of full path.

  If `-u` argument is used along with `-p` argument, the password is taken from the command line instead of `cwcli CWCLIFILE`. This is not secure and usage of this argument is not recommended.

  The password must be provided in the file in the following format:

  `username password`

  Where username is the LMS user name given in command line. The delimiter between username and password is single blank space. You must provide the delimiter if the password is blank.

  Otherwise, `cwcli config` will not validate the password. The password file can contain multiple entries with different user names. The password of the first match is considered in case of duplicate entries.

  See Setting CWCLIFILE Environment Variable for more details.

Function-independent Arguments

You can use the following arguments without any commands:

- `help`
  When run with the `-help` argument, `cwcli config` displays a list of all supported commands and a one-line description of the command.

- `v`
  When run with the `-v` argument, `cwcli config` displays `cwcli config` version information.

Function-dependant Arguments

You can use the following arguments only with commands:

- `p password`
  Specifies the password for the LMS username.
Warning

SECURITY WARNING: If -p password is used, the password is read from the command line instead of cwcli CWCLIFILE. This is highly insecure and *not* recommended. See -u argument for more details. See Setting CWCLIFILE Environment Variable for more details.

-d debuglevel
Sets the debug level based on which debug information is printed. debuglevel is a numeric value between 1 and 5.

-f filename
Specifies the name of the file to which the retrieved configuration is written. If not specified, devicename.cfg is assumed.

-l logfile
Logs the results of the cwcli config command to the specified log filename.

-m mailbox
Mails the results of the cwcli config command to the specified email address.

Function-specific Arguments

You can use the following arguments only with specific commands:

-baseline
Used with the compareanddeploy, deploycomplianceresults, listversions, createdeployparamfile, directbaselinedeploy, or comparewithbaseline function, specifies the name of the Baseline template that is compared with the latest configuration version of the device. If there are commands in the baseline configuration file that are not compliant with the latest configuration of the device in the archive, they are downloaded to the device.

Note
The Baseline template must not contain any parameters for the command to succeed.

-date date1 date2
Used with the compare or delete command, specifies the configuration date(s) to compare or delete. Use the format mm/dd/yyyy.

-device name
Used with the export, import, or put function, specifies the name of the device. You can specify a wildcard, %, in the device name to match any device(s) that have the same textual pattern.

-device list
Used with the get, start2run, compare, compareanddeploy, comparewithbaseline, deploycomplianceresults, listversions, put, run2start, start2run, write2run or delete commands

Specifications the list of device names separated by commas. You can specify a wildcard, %, in the device list to match device(s) that have the same textual pattern.

-ipaddress list
Used with the get, start2run, compare, compareanddeploy, comparewithbaseline, deploycomplianceresults, listversions, put, run2start, start2run, write2run or delete commands.
Specifies IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated.

You cannot use this option with -device, -view, or -input. Also, you cannot specify wildcard characters.

-filename
Used with the directbaselinedeploy, export, import, write2run or write2start function, specifies the name of the file to which the configuration from archive should be exported to. Used with the import function, specifies the name of the file that contains the configuration to import.

Note -f argument must not be specified when -view or -device % is used. If used, the given file will be overwritten with the configuration retrieved for other devices.

-listonly
Used with the write2run function, lists the differences between the running configuration and the specified configuration file.

-reboot
Used with the import or put function, reboots the device after the configuration has been written to the device.

-save
Used with the import or put function, saves the configuration written to the device to the device's memory.

-timeout
Used with the compareanddeploy, deploycomplianceresults, import, put, run2start, start2run, write2run or comparewithbaseline function, specifies the duration of the interval in seconds between two successive polling cycles.

-version number
Used with the export function, specifies the configuration version to retrieve from the archive. Used with the put function, specifies the configuration version to load from the archive and push to the device.

-version version1 version2
Used with the compare or delete function, specifies the configuration version(s) to compare or delete.

-view name
Specifies the device view where the device name specified with -device argument is located. If -device argument is not specified, performs the operation on all devices in the view. More details are described in the -view Argument Usage section later in this man page.

-xml
Creates an XML file with the name of the device containing the configuration retrieved.
Input List File Format

For commands that do not accept multiple device names on the command line, such as put, import, and export, you can create an input list file that contains a list of devices to perform the operation on.

The contents of the input list file are a sequence of lines. Each line specifies a device name and the arguments to apply to that device. The arguments must be specific to the function. You cannot include view names in the input list file. You must specify view names on the command line. You can include comments in the input list file by starting the each commented line with #.

Input List File Example:

For the command

cwcli config put -u userid -p password -view myView -input ~/todo_list

An example of the input list file ~/todo_list is # Comment line.

-version 3 -reboot -device enm-2501.cisco.com
-version 2 -save -device enm-4500.cisco.com

-view Argument Usage

If both -device and -view are specified, the devices in that view and the devices specified against -device are considered.

For example, assume that -view has two devices D1 and D2 and D3 is specified against -device, then all the three devices D1, D2 and D3 are considered.

-view Argument Usage Examples:

Search for a device in a specified view:

cwcli config export -u admin -p admin -view myView -device myDevice

cwcli config Subcommand Man Pages

Each cwcli config command has a man page. You can access these man pages from the command line of a LMS server installed on a UNIX system.

To view the man pages, add the path:

install_dir/CSCOpx/man to the MANPATH variable.

Then you can enter the command

man cw- command

where command is the command name. For example, export.

This topic contains the man pages for the following cwcli config subcommands:

- compare
- comparewithbaseline
- compareanddeploy
- delete
- deploycomplianceresults
- export
- get
**Appendix A      CLI Utilities**

- import
- put
- reload
- run2start
- start2run
- write2run
- write2start
- listversions
- createdeployparamfile
- directbaselinedeploy
- collectiondate
- accessdate

**compare**

**Name**

cwcli config compare – CiscoWorks  
cwcli config compare function

**Syntax**

cwcli config compare -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-device list | -view name | -device list -view name | -ipaddress list] { -version version1 [version2] | -date date1 [date2] }
cwcli config compare -help

**Description**

**compare** lists the differences between versions of a device configuration. You can specify the versions to be compared by using the **-version** argument or the **-date** argument.

- If you specify the **-version** argument with only one version number, that version is compared with the latest archived configuration of the device.
- If you specify the **-date** argument with only one date, the configuration version with that date is compared with the latest archived configuration. When specifying a date, use the format mm/dd/yyyy.
- If you do not specify either a date or a version, the latest two archived configurations are compared. You can specify multiple devices by separating each device name with a comma.

The output of the Compare function can be interpreted as follows:

- Lines preceded by `+' sign signify those occurring only in the first version but not in the latter.
- Lines preceded by `-' sign signify those occurring only in the latter version but not in the first.
- Lines preceded by `<' and `>' connote those which are present in both files but differ from each other.
### compareanddeploy

**Name**
cwcli config compareanddeploy – CiscoWorks compare and download configuration with Baseline template function.

**Syntax**
cwcli config compareanddeploy -help

**Description**
compareanddeploy creates a job that compares the given Baseline template with the latest version of the configuration for a device and downloads the configuration to the device if there is non-compliance. If you specify the -baseline argument, the name of the Baseline template is compared with the latest configuration version of the device and later downloaded to the device if there are any commands in the baseline config file which are not compliant with the latest configuration of the device in the archive. The Baseline template must not have any parameters for the command to succeed.

### comparewithbaseline

**Name**
cwcli config comparewithbaseline - CiscoWorks compare configuration with Baseline template function.

**Syntax**
cwcli config comparewithbaseline -help

**Description**
comparewithbaseline creates a job that compares the given Baseline template with the latest version of the configuration for a device. If you use the -baseline argument, the name of the Baseline template is compared with the latest configuration version of the device.

### delete

**Name**
cwcli config delete – CiscoWorks cwcli config delete function

**Syntax**
cwcli config delete -help

**Description**
delete deletes the specified device configuration from the archive. You can use the -date argument or the -version argument to specify which configurations to delete.
- If you specify two dates, all configurations archived between those two dates are deleted.
- If you specify only one date, all configurations up to and including the configuration archived on that date are deleted.
- If you specify two versions, all configurations between and including the two versions are deleted.
- If you specify only one version, the configuration corresponding to that version is deleted.
deploycomplianceresults

Name | `cwcli config deploycomplianceresults` - CiscoWorks deploy command with baseline function.
--- | ---

deploycomplianceresults

Description | `deploycomplianceresults` uses the previously run `comparewithbaseline` job to get the non-compliance commands and creates a job after replacing the parameters if any in the non-compliance commands with the values from the data file and then downloads those commands to ensure the compliance with the baseline config.

If you specify the `-baseline` argument, the name of the Baseline template which will be compared with the latest configuration version of the device.

export

Name | `cwcli config export` - CiscoWorks `cwcli config`'s `export` function.
--- | ---

description | `export` retrieves the configuration specified by the `-version` argument, for the device specified by -device and/or -view argument, from the archive and writes it to the file specified by the `-f` argument.

- If you do not specify a version number, the latest configuration of the device from the archive is retrieved.
- If you do not specify a file name, a file named devicename.cfg is created. To run this command against multiple devices, you must specify the `-input` argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of the `cwcli config` man page.

get

Name | `cwcli config get` - CiscoWorks `cwcli config` get function
--- | ---
Syntax | `cwcli config get` -u `userid` -p `password` [-d `debuglevel`] [-m `email`] [-l logfile] [-filetype `running`|`startup`|`runningstartup`] [-device `list` | -view `name` | -device `list` -view `name` | -ipaddress `list`]

description | `get` retrieves the running configuration from the device(s), specified by the -device and/or -view argument, and pushes it to the configuration archive if the running configuration is different than the latest version in the archive.

For devices that support vlan configuration like CatIOS devices, the vlan configuration is also fetched and archived along with running-configuration.

However, if a new version of the running configuration is not archived, the vlan configuration fetched, overwrites the previously archived vlan configuration for the latest version of running configuration in the archive. You can run the get function against multiple devices by separating each device name with a comma.
import

<table>
<thead>
<tr>
<th>Name</th>
<th>cwcli config import – CiscoWorks cwcli config import function</th>
</tr>
</thead>
<tbody>
<tr>
<td>cwcli config import -help</td>
<td></td>
</tr>
</tbody>
</table>

Description

import retrieves the configuration from a file specified by the -f argument, and pushes it to the device specified by the -device and/or the -view argument, adding to the device's running configuration.

• If you do not specify a file name, a file named device name.cfg is used. You can specify the -save and -reboot arguments, which operate the same as for the put argument.

To run the import argument against more than one device, you must specify the -input argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of cwcli config(1).

The configuration archive might be updated after you specify the import argument if the loaded configuration is different from the latest configuration in the archive.

put

<table>
<thead>
<tr>
<th>Name</th>
<th>cwcli config put – CiscoWorks cwcli config put function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>cwcli config put -u userid -p password [-d debuglevel] [-m email] [-l logfile] [ -device name</td>
</tr>
<tr>
<td>cwcli config put -help</td>
<td></td>
</tr>
</tbody>
</table>

Description

put retrieves the configuration specified by -version from the configuration archive and pushes it to the device specified by the -device and/or -view argument

The -filetype can be used to specify the type of configuration viz running/vlan configuration. By default, the running configuration is considered

• In case of running configuration, the archived running configuration is merged with the running configuration on the device unless you specify -save, in which case, the archived configuration is also written to the device's memory.

• In case of vlan configuration, the archived vlan configuration overwrites that on the device. The vlan configuration will not come into effect until the device is rebooted. You can specify -reboot to reboot the device after the configuration (running/vlan) is pushed to the device.

To run the put command on more than one device at a time, you must use the -input argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of cwcli config(1).
### Configuration Management with Cisco Prime LAN Management Solution 4.2

#### Appendix A

#### CLI Utilities

**reload**

<table>
<thead>
<tr>
<th>Name</th>
<th>cwcli config reload – CiscoWorks cwcli config reload function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>cwcli config reload -u userid -p password [-d debuglevel] [-m email][-l logfile] [-device list] [-view name] [-device list -view name] [-ipaddress list] [-input argumentFile] [-timeout seconds] [-primary_user primary user name] [-primary_pass Base64 encoded primary password] [-enable_pass Base64 encoded enable password]</td>
</tr>
<tr>
<td>Description</td>
<td>reload reboots the device(s), specified by the -device and/or -view argument, resulting in the running configuration being loaded with its startup configuration. You can specify multiple devices with the -device argument by separating each device name with a comma.</td>
</tr>
</tbody>
</table>

**run2start**

<table>
<thead>
<tr>
<th>Name</th>
<th>cwcli config run2start – CiscoWorks cwcli config run2start function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>run2start overwrites the startup configuration of any device(s), specified by the -device and/or -view argument, with its running configuration. You can specify multiple devices with the -device argument by separating each device name with a comma or with the -input argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of cwcli config(1).</td>
</tr>
</tbody>
</table>

**start2run**

<table>
<thead>
<tr>
<th>Name</th>
<th>cwcli config start2run – CiscoWorks cwcli config start2run function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>start2run merges the running configuration of any device(s), specified by the -device and/or -view arguments, with its startup configuration to give a new running configuration. You can specify multiple devices with the start2run argument by separating each device name with a comma or with the -input argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of cwcli config(1).</td>
</tr>
</tbody>
</table>
### write2run

<table>
<thead>
<tr>
<th>Name</th>
<th><code>cwcli config write2run</code> - CiscoWorks cwcli config write2run function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`cwcli config write2run -u userid -p password [-d debuglevel][-m email][-l logfile] { -device name [-ipaddress address] -f filename [-config 1</td>
</tr>
</tbody>
</table>
| Description | **write2run** compares the latest running configuration for the device in the configuration archive with the configuration in the file specified by the `-f` argument to generate a new configuration that is downloaded to the device, so that the end result is that the configuration specified in the file is available on the running configuration of the device.  
If `-listonly` is specified, the difference between the latest running configuration for the device in the configuration archive and the new configuration that is generated is listed on the display, but no configuration is downloaded to the device.  
To run this command against multiple devices, specify the `-input` argument, which takes a file name as an argument.  
The contents of the file must be similar to those described in the Input List File Format section of `cwcli config(1)`.  
**CAVEAT**  
This command is not 100% reliable in that it may not successfully overwrite the running configuration. This is due to the dependency on the underlying Diff API, which generates the configuration difference to be downloaded to the device to make the running configuration on the device same as the one specified in the file (by the `-f` argument). |

### write2start

<table>
<thead>
<tr>
<th>Name</th>
<th><code>cwcli config write2start</code> - CiscoWorks cwcli config write2start function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`cwcli config write2start -u userid -p password [-d debuglevel][-m email][-l logfile] { -device name [-ipaddress address] -f filename [-config 1</td>
</tr>
</tbody>
</table>
| Description | **write2start** erases the contents of the device's startup configuration and then writes the contents of the given file as the device's new startup configuration. If you do not specify a file name, it prints an error message and exits.  
To run this command against multiple devices, you must specify the `-input` argument, which takes a file name as its argument.  
The contents of the file must be similar to those described in the Input List File Format section of `cwcli config(1)`.) |
### listversions

**Name**
cwcli config listversions – CiscoWorks cwcli config listversions function

**Syntax**
cwcli config listversions -u userid -p password [-d debuglevel] [-m email][-l logfile] [-device name | -view name | -device name -view name | -ipaddress list] [-baseline][ -input argumentFile]
cwcli config listversions -help

**Description**
Listversions (specified by "listversions") lists the different versions of configuration files archived in the archival system. If you use the -baseline argument, only the names of the Baseline templates are displayed.
You can choose a template and use it inline with the comparewithbaseline and compareanddeploy commands.

### createdeployparamfile

**Name**
cwcli config createdeployparamfile - CiscoWorks cwcli config createdeployparamfile function.

**Syntax**
cwcli config createdeployparamfile -u userid -p password [-d debuglevel] [-m email][-l logfile][-jobid comparewithbaseline jobid] [-baseline baselinefile] [-t parameterfile]
cwcli config createdeployparamfile -help

**Description**
createdeployparamfile creates a parameter file if the Baseline template containing the parameters is specified. You can use the -jobid argument to specify the job identifier of the previously executed comparewithbaseline job. You can choose a template with the -baseline argument and specify the name of the Baseline template for which the parameter file has to be created.

### directbaselinedeploy

**Name**
cwcli config directbaselinedeploy - CiscoWorks cwcli config directbaselinedeploy function

**Syntax**
cwcli config directbaselinedeploy -u userid -p password [-d debuglevel] [-m email][-l logfile] [-baseline baselinefile] [-substitute parameterfile] [-t timeout seconds] [-primary_user primary user name] [-primary_pass Base64 encoded primary password] [-enable_pass Base64 encoded enable password]
cwcli config directbaselinedeploy -help

**Description**
directbaselinedeploy creates a job that downloads the given Baseline template after retrieving the values of the parameters in the template from the given parameter file. You can use the -timeout argument to specify the duration of the interval in seconds between the two successive polling cycles.
You can use the -baseline to specify the name of the Baseline template which will be compared with the latest configuration version of the device and later downloaded to the device if there are any commands in the baseline config file which are not compliant with the latest configuration of the device in the archive. You can use the -substitute to substitute the values from the XML parameter file for the parameters specified in the template.
### Collection Date

**Name**  | `cwcli config collectiondate` - CiscoWorks `cwcli config collectiondate` function
---|---
**Syntax**  | `cwcli config collectiondate -u userid -p password [-a debuglevel] [-m email] [-l logfile] [-filetype running|startup|vlan] [-input argumentFile] { -device list -view name | -ipaddress list }`
`cwcli config collectiondate -help`
**Description**  | `collectiondate` displays the last config collection date for the devices. The output contains device name, time of last config collection, and the filetype separated by comma.

### Access Date

**Name**  | `cwcli config accessdate` - CiscoWorks `cwcli config accessdate` function
---|---
**Syntax**  | `cwcli config accessdate -u userid -p password [-a debuglevel] [-m email] [-l logfile] [-filetype running|startup|vlan] [-input argumentFile] { -device list -view name | -ipaddress list }`
`cwcli config accessdate -help`
**Description**  | `accessdate` displays the last config collection attempt date for the devices. The output contains device name, time of last attempt, and the filetype separated by comma.

## Overview: cwcli netconfig Command

The `cwcli netconfig` command lets you use NetConfig from the command line. This section contains `cwcli netconfig Remote Access`.

**Caution**

The `cwcli netconfig` command does not validate the command arguments you use or the configuration commands that you run using it. If you enter incorrect commands you can misconfigure or disable the devices on which the job runs.

### Running the cwcli netconfig Command

To use the `cwcli netconfig` command, you must be able to run the cwcli command, and you must have permissions to use the Adhoc system-defined task. For more details see topic in the section.

The command syntax is:

```
cwcli netconfig Sub_command Common_arguments Command_arguments
```

The subcommands and arguments are described in the following sections:

- Subcommands (see Subcommands)
- Common Arguments (see Common Arguments)
- Command Arguments (see Command Arguments)
Subcommands

Subcommands specify the action the command performs. Valid values for the subcommands are:

<table>
<thead>
<tr>
<th>Sub Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>createjob</td>
<td>Creates job.</td>
</tr>
<tr>
<td>deletejob</td>
<td>Deletes jobs.</td>
</tr>
<tr>
<td>canceljob</td>
<td>Cancels jobs.</td>
</tr>
<tr>
<td>jobdetails</td>
<td>Lists job details.</td>
</tr>
<tr>
<td>jobresults</td>
<td>Lists job results.</td>
</tr>
<tr>
<td>listjobs</td>
<td>Lists jobs.</td>
</tr>
<tr>
<td>import</td>
<td>Imports user-defined tasks in XML format.</td>
</tr>
<tr>
<td>export</td>
<td>Exports user-defined tasks in XML format.</td>
</tr>
<tr>
<td>listtasks</td>
<td>Lists the NetConfig user-defined tasks.</td>
</tr>
</tbody>
</table>

Common Arguments

Common arguments specify parameters that apply to all subcommands. Valid values for common_arguments are:

<table>
<thead>
<tr>
<th>Command Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u user</td>
<td>Enter valid CiscoWorks username.</td>
<td>None</td>
</tr>
<tr>
<td>-p password</td>
<td>Enter password for username.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for more details.</td>
<td></td>
</tr>
</tbody>
</table>

Command Arguments

Command arguments specify parameters that apply only to specific subcommands.

The conventions followed are:

- Arguments in [ ] are optional. For optional arguments, if you do not specify a value the default value that has been set by the administrator using the NetConfig UI, will become applicable.
- Arguments in { } denote that you must provide one argument from each group of arguments in curly braces ({}), that is separated by vertical bars (|).
- Arguments suffixed with + denote that you can enter multiple values separated with spaces.
- Values that contain spaces need to be entered within “ ”. For example, the job description that you provide when you use a the createjob command should be entered within “ ”.

Valid values for command_arguments are described in the following table:
### Sub Command | Command Argument | Description | Usage Notes
--- | --- | --- | ---
createjob | | Defines devices to be configured. Jobs can run only one device category (IOS, Catalyst, Content Engine (CE), or Content Service Switch (CSS)). Do not enter devices of multiple categories.

<table>
<thead>
<tr>
<th>Sub Command</th>
<th>Command Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>createjob</td>
<td>`-device comma_separated_device_names</td>
<td>Defines devices to be configured. comma_separated_device_names is list of device names.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sub Command</th>
<th>Command Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>createjob</td>
<td>`-devicefile devicelist_filename</td>
<td>Defines devices to be configured. comma_separated_device_names is list of device names.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sub Command</th>
<th>Command Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>createjob</td>
<td>`-view device_view_name</td>
<td>Defines devices to be configured. comma_separated_device_names is list of device names.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sub Command</th>
<th>Command Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>commandlist_filename</td>
<td>Defines configuration commands to be used.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sub Command</th>
<th>Command Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>{-mode {config</td>
<td>enable}</td>
<td>You can specify the command file path, the command mode, the rollback file and the name of the user-defined task.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sub Command</th>
<th>Command Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>{-rollbackfile rollback_cmdlist_filename</td>
<td>Defines the rollback configuration commands for the job.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sub Command</th>
<th>Command Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>{-taskname : &quot;User defined task name&quot;}</td>
<td>Specifies the user-defined task name within quotes.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sub Command</th>
<th>Command Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>{-description : &quot;job_description&quot;}</td>
<td>Enter the description for the job you are creating. &quot;job_description&quot; is the description you specify, for the job that you are creating. Enter this value within quotes.</td>
<td></td>
</tr>
<tr>
<td>Sub Command</td>
<td>Command Argument</td>
<td>Description</td>
<td>Usage Notes</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>`[-schedule: MM/dd/yyyy:HH:mm:ss</td>
<td>schedule` defines time and date job will run.</td>
<td>MM is month (01 to 12). DD is day of month (01 to 31). YYYY is year (Example: 2004). HH is hours, mm is minutes, and ss is seconds in 24-hour time. If you do not specify the schedule type, the job will be an immediate job.</td>
</tr>
<tr>
<td></td>
<td>`-schedule_type: once</td>
<td>weekly</td>
<td>monthly</td>
</tr>
<tr>
<td></td>
<td><code>-policyfile policy_filename</code></td>
<td>Defines job policies using a job policy file. You can specify job policies using combination of <code>-policyfile</code> argument and other optional arguments, however, you can specify each argument only once in command. <code>policy_filename</code> is path to job policy file. Can be a full pathname or filename in local directory.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>-makercomments: &quot;maker comments&quot;</code></td>
<td>Comments from the job creator, to the job approvers, if job approval is enabled for the job. Enter your comments within quotes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>-mkemail: maker email id</code></td>
<td>E-mail ID of the job creator, for approval notifications, if approval is enabled for the job. None.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`-execution: Sequential</td>
<td>Parallel`</td>
<td>Configures the job execution property, whether the jobs should be run sequentially or in parallel. None.</td>
</tr>
<tr>
<td></td>
<td><code>-startup: Copy running config to startup policy</code></td>
<td>Select to cause the configuration job to write the running configuration to the startup configuration on each device after configuration changes are made successfully. None.</td>
<td></td>
</tr>
<tr>
<td>Sub Command</td>
<td>Command Argument</td>
<td>Description</td>
<td>Usage Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>deletejob</td>
<td>-id job_id+</td>
<td>This subcommand allows you to delete one or more NetConfig jobs.</td>
<td>job_id+ specifies the ID of the job on which to act. You can specify multiple job IDs separated by spaces or commas.</td>
</tr>
<tr>
<td>canceljob</td>
<td>-id job_id</td>
<td>This subcommand allows you to cancel a NetConfig job from the command line.</td>
<td>job_id specifies ID of job on which to act.</td>
</tr>
<tr>
<td>jobdetails</td>
<td>-id job_id+</td>
<td>Allows you to view details of one or more NetConfig jobs from the command line.</td>
<td>You can specify multiple job ID separated by spaces or commas.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[-version]</td>
<td></td>
<td>Select to cause the job to be considered a failure when the most recent configuration version in the Configuration Archive is not the same as the configuration that was running when you created the job.</td>
<td>-sync argument should be provided if this policy is selected. This argument causes the job to archive the running configuration before making configuration changes.</td>
</tr>
<tr>
<td>[-email]</td>
<td>[Job Notification email ids ]</td>
<td>Specify the email addresses to which the configuration job will send status notices.</td>
<td>Separate multiple addresses with commas.</td>
</tr>
<tr>
<td>[-sync]</td>
<td></td>
<td>Select to cause the job to archive the running configuration before making configuration changes.</td>
<td>None.</td>
</tr>
<tr>
<td>[-failure]</td>
<td>“Stop on failure”</td>
<td>“Ignore failure and continue”</td>
<td>“Rollback device and stop”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[-primary_user]</td>
<td>Primary User name -primary_pass: “Primary password” ]</td>
<td>Primary username for connecting to the device.</td>
<td>Enter the primary password within quotes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Primary password for connecting to the device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[ -enable_pass: “Execution mode Password” ’]</td>
<td>Password for running commands in the execution mode, on the device.</td>
<td>Enter the execution mode password within quotes.</td>
<td></td>
</tr>
<tr>
<td>Sub Command</td>
<td>Command Argument</td>
<td>Description</td>
<td>Usage Notes</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>jobresults</td>
<td>[ -id job_id+ ]</td>
<td>Specifies ID of job on which to act.</td>
<td>You can specify multiple job ID separated by spaces or commas.</td>
</tr>
<tr>
<td></td>
<td>[ -details ]</td>
<td>Specifies full details of job results to be displayed.</td>
<td>Not specifying details will display only the summary of job execution result.</td>
</tr>
<tr>
<td>listjobs</td>
<td>[ -status {A(ll)</td>
<td>R(unning)</td>
<td>C(ompleted)</td>
</tr>
<tr>
<td>import</td>
<td>{-taskfile User-defined task file}</td>
<td>User-defined task filename in XML format.</td>
<td></td>
</tr>
<tr>
<td>export</td>
<td>{-task+ User-defined task name}</td>
<td>Name of the user-defined task to be exported.</td>
<td>You can specify multiple tasks separated by spaces or commas.</td>
</tr>
<tr>
<td></td>
<td>{-dest file export location}</td>
<td>Path of the destination location to which the exported user-defined task file is to be copied.</td>
<td></td>
</tr>
<tr>
<td>listtask</td>
<td></td>
<td>Lists the NetConfig user-defined tasks.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Examples**

**Example 1**

The command

```
cwcli netconfig createjob -u username -p password -devicefile devicefile -commandfile command.file -failure Ignore failure and Continue -startup
```

creates a NetConfig job with the following characteristics:

- Devices mentioned in `devicefile` will be configured.
- Commands in file `command.file` will run.
- Job will continue if it fails to successfully configure a device.
- Each device's running configuration will be copied to startup as soon as the device is successfully configured.
- Job will run immediately because the `-schedule` argument is not specified.
Example 2

The command

```
cwcli netconfig createjob -u username -p password -devicefile devicefile -commandfile command.file -policyfile policyfile
```

creates a NetConfig job with the following characteristics:

- Devices listed in the file `devicefile` will be configured.
- Commands in the file `command.file` will run.
- The file `policyfile` contains job policy arguments that determine the job policy.

Understanding cwcli netconfig Input Files

Several types of text files are available for you to use as input for the `cwcli netconfig` command and the `-createjob` subcommand. You can also use the command list type as input for user-defined tasks.

<table>
<thead>
<tr>
<th>File Type</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device list</td>
<td>Lists devices on which job will run. It lists one device on each line.</td>
<td>Use with <code>-devicefile</code> argument. Job can run only one device category (IOS, or Catalyst). Do not list devices of multiple categories.</td>
</tr>
<tr>
<td>Command list</td>
<td>Lists configuration commands that job will run; one command per line.</td>
<td>Use with <code>-commandfile</code> argument, or to add commands to a user-defined task.</td>
</tr>
<tr>
<td>Job policy</td>
<td>Lists of job policy arguments; one argument per line.</td>
<td>Use with <code>-policyfile</code> argument.</td>
</tr>
</tbody>
</table>

Examples

**Device List File**

```
-device device_display_name1
-device device_display_name2
-device device_display_name3
-device device_display_name4
```

**Command List File**

```
command1
command2
command3
command4
```

**Job Policy File**

This file configures the job to stop running if the job fails on a device, to write the running configuration to startup after configuration changes are made.

```
-failure Stop on Failure
-sync
```
cwcli netconfig Man Page Examples

On UNIX, you can view the complete man pages by setting the MANPATH to /opt/CSCOpx/man.

The following are some examples from the NetConfig man page:

**Examples**
Device List File Example
For the command
```
cwcli netconfig createjob -u userid -p password -devicefile c7000.dev -commandfile command.file
   -description "cwcli netconfig job" -mode config
```
An example of the device list file c7000.dev is
```
enm-7000-1.cisco.com
enm-7000-2.cisco.com
enm-7000-3.cisco.com
enm-7000-4.cisco.com
```

Command List File Example
For the command
```
cwcli netconfig createjob -u userid -p password -devicelist c7000-1,c7000-2 -commandfile command.file
   -description "cwcli netconfig job" -mode config
```
An example of the command file command.file is
```
snmp-server community public ro
snmp-server community private rw
```

Policy File Example
For the command
```
cwcli netconfig createjob -u userid -p password -devicefile c7000.dev -commandfile command.file -policyfile policy.in
   -description "cwcli netconfig job" -mode config
```
An example of the policy file policy.in is
```
-failure "Stop on failure"
-sync
-execution Parallel
```

User-defined Task XML file Example
```
<?xml version="1.0" encoding="UTF-8"?>
<Task name="SampleTASK">
   <Template mode="1" name="iproute" parameterized="false">
      <Commands>
         <cli>ip route 0.0.0.1 0.0.0.0 Ethernet0/0</cli>
         <cli>ip route 0.0.0.2 0.0.0.0 Ethernet0/0</cli>
         <cli>ip route 0.0.0.3 0.0.0.0 Ethernet0/0</cli>
      </Commands>
```

<cli>ip route 0.0.0.4 0.0.0.0 Ethernet0/0</cli>
<cli>ip route 0.0.0.5 0.0.0.0 Ethernet0/0</cli>
<cli>ip route 0.0.0.6 0.0.0.0 Ethernet0/0</cli>
</Commands>
<RollbackCommands>
<cli>no ip route 0.0.0.4 0.0.0.0 Ethernet0/0</cli>
<cli>no ip route 0.0.0.5 0.0.0.0 Ethernet0/0</cli>
</RollbackCommands>
<MDFIds>268438030,273153536,272819655</MDFIds>
</Template>
</Task>

cwcli netconfig Remote Access

You can also perform the cwcli netconfig tasks using the servlet. You will have to upload a payload XML file, which contains the cwcli netconfig command arguments and LMS user credentials.

You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the output either on the console or in the specified output file, if the credentials are correct and arguments are valid.

The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to run any command:

**For post request,**

```
perl samplepost.pl http://lms-server:lms-port/rme/cwcli payload_XML_file
```

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

```
perl samplepost.pl https://lms-server:lms-port/rme/cwcli payload_XML_file
```

The default port for LMS server in HTTPS mode is 443.

The schema for creating the payload file in XML format is:

```
<payload>
  <command>
    cwcli inventory commandname -u user -p BAsed64 encoded pwd -args1 arg1value...
  </command>
</payload>
```

To invoke the servlet using a script, see the Overview: cwcli invreport Command.

The script and the payload file should be residing in the client machine.

**For get request,**

```
http://<rme-server>:<rme-port>/rme/cwcli?command=cwcli netconfig commandname -u user -p BAsed64 encoded pwd -args1 arg1value...
```

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

```
https://lms-server:lms-port/rme/cwcli?command=cwcli netconfig commandname -u user -p BAsed64 encoded pwd -args1 arg1value...
```
The default port for LMS server in HTTPS mode is 443.
The Base64 encoded for “admin” is YWRtaW4=.
The URL encode for,
- Double quotes (") is %22
- Percentage sign (%) is %25

Overview: cwcli export Command

cwcli export is a command line tool that also provides servlet access to inventory, configuration and change audit data.
This can be used for generating inventory, configuration archive, and change audit data for devices in LMS.
This section contains:
- Using the cwcli export Command
- Running cwcli export changeaudit
- Running cwcli export config
- Running cwcli export inventory Command
- XML Schema for cwcli export inventory Data

Note
You cannot run this command for the devices that are in Conflicting or Suspended state.

This tool supports the following features:
- Generating change audit data in XML format
  The tool uses the existing Change Audit log data and generates the Change Audit log data in XML format.
  See Running cwcli export changeaudit for the usage and XML schema details
- Generating configuration data in XML format
  The tool uses existing configuration archive APIs and generates latest configuration data from the configuration archive in XML format.
  Elements in the XML file are created at the configlet level in the current configuration archive.
  Predefined rules that currently exist in the configuration archive are used to get the configlets data.
  See Running cwcli export config for the usage and XML schema details
- Generating inventory data in XML format
  The tool has servlet access and command line utilities that can generate inventory data for devices managed by the LMS server.
  See Running cwcli export inventory Command for the usage and XML schema details
The `cwcli export` command is located in the following directories, where `install_dir` is the directory in which LMS is installed:

- On UNIX systems, `/opt/CSCOpx/bin`
- On Windows systems, `install_dir\CSCOpx\bin`

The default install directory is `C:\Program Files`.

If you install LMS on an NTFS partition on Windows, only users in the administrator or casuser group can access `cwcli export`. Users with read-write access to the `CSCOpx\files\archive` directory and the directories under that can also use `cwcli export`.

You can also perform the `cwcli export` tasks using the servlet. You will have to upload a payload XML file, which contains the `cwcli export` command arguments and LMS user credentials.

You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the output either on the console or in the specified output file, if the credentials are correct and arguments are valid.

The name of the servlet is `/rme/cwcli`.

The following is the servlet to be invoked to run any command:

**For post request**,  

```
perl samplepost.pl http://lms-server:lms-port/rme/cwcli payload_XML_file
```

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use `https` protocol for secured connection.

```
perl samplepost.pl https://lms-server:lms-port/rme/cwcli payload_XML_file
```

The default port for LMS server in HTTPS mode is 443.

The schema for creating the payload file in XML format is:

```
<payload>
  <command>
    cwcli inventory commandname -u user -p BASE64 encoded pwd -args1 arg1value...
  </command>
</payload>
```

To invoke the servlet using a script, see the **Overview: cwcli invreport Command**.

The script and the payload file should be residing in the client machine.

**For get request**,  

```
http://lms-server:lms-port/rme/cwcli?command=cwcli export commandname -u user -p BASE64 encoded pwd -args1 arg1value...
```

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use `https` protocol for secured connection.

```
https://lms-server:lms-port/rme/cwcli?command=cwcli export commandname -u user -p BASE64 encoded pwd -args1 arg1value...
```

The default port for LMS server in HTTPS mode is 443.

The BASE64 encoded for “admin” is `YWRtaW4=`.

The URL encode for:

- Double quotes (" is `%22` and Percentage sign (%) is `%25`
Using the cwcli export Command

The command line syntax of the application is in the following format:

```
cwcli export command GlobalArguments AppSpecificArguments
```

- `cwcli export` is the CiscoWorks command line interface for exporting inventory/config/changeaudit details into XML format.
- `Command` specifies which core operation is to be performed.
- `GlobalArguments` are the additional parameters required for each core command.
- `AppSpecificArguments` are the optional parameters, which modify the behavior of the specific `cwcli export` core command.

The order of the arguments and arguments are not important. However, you must enter the core command immediately after `cwcli export`.

The following sections describe:

- The `cwcli export` commands (See `cwcli export Commands`)
- The mandatory and optional arguments (See `cwcli export Global Arguments`)
- The default archiving location (See `Archiving cwcli export Data in XML File`)

On UNIX, you can view the `cwcli export` man pages by setting the MANPATH to `/opt/CSCOpx/man`. The commands to launch the `cwcli export` man pages are:

- `man cwcli-export`—To launch the `cwcli export` command man page.
- `man export-changeaudit`—To launch the `cwcli export changeaudit` command man page.
- `man export-config`—To launch the `cwcli export config` command man page.
- `man export-inventory`—To launch the `cwcli export inventory` command man page.

**cwcli export Commands**

The following table lists the command part of the `cwcli export` syntax.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cwcli export changeaudit</code></td>
<td>Generates Change Audit log data in XML format.</td>
</tr>
<tr>
<td><code>cwcli export config</code></td>
<td>Generates configlets in XML format</td>
</tr>
<tr>
<td><code>cwcli export inventory</code></td>
<td>Generates Inventory data in XML format.</td>
</tr>
</tbody>
</table>

You must invoke the `cwcli export` command with one of the core commands specified in the above table. If no core command is specified, `cwcli export` can execute the `-v` or `-h` arguments only. Argument `-v` specifies the version of the `cwcli export` utility and argument `-h` (or null argument) displays the usage information of this tool.
cwcli export Global Arguments

The following describes the mandatory and optional global arguments for `cwcli export`:

<table>
<thead>
<tr>
<th>Global Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-u userid</code></td>
<td>Mandatory Specifies the LMS username.</td>
</tr>
<tr>
<td><code>-p password</code></td>
<td>Mandatory Specifies the password for the LMS username.</td>
</tr>
<tr>
<td></td>
<td>If you want to avoid the <code>-p</code> argument which will reveal the password in clear text in cli, you will have to store your username and password in a file and set a variable <code>cwcli CWCLIFILE</code> which points to the file.</td>
</tr>
<tr>
<td></td>
<td>You will have to maintain this file and control access permissions to prevent unauthorized access. <code>cwcli export</code> looks for current working directory if <code>cwcli CWCLIFILE</code> is set only to file name instead of full path.</td>
</tr>
<tr>
<td></td>
<td>If you use the <code>-p</code> argument, even after setting the <code>cwcli CWCLIFILE</code> variable the password is taken from the command line instead of <code>cwcli CWCLIFILE</code>. This is not secure and usage of this argument is not recommended.</td>
</tr>
<tr>
<td></td>
<td>The password must be provided in the file in the following format:</td>
</tr>
<tr>
<td></td>
<td>username password</td>
</tr>
<tr>
<td></td>
<td>where username is the LMS user name given in the command line. The delimiter between the username and password is single blank space.</td>
</tr>
<tr>
<td></td>
<td>You must enter the delimiter if the password is blank. Otherwise, <code>cwcli export</code> will fail to validate the password. The password file can contain multiple entries with different user names. The password that matches first is considered in case of duplicate entries.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If <code>-p password</code> is used, the password is read from the command line instead of <code>cwcli CWCLIFILE</code>. This is highly insecure and therefore not recommended.</td>
</tr>
<tr>
<td></td>
<td>See Setting CWCLIFILE Environment Variable for more details.</td>
</tr>
</tbody>
</table>

| `{ -device devicename | Mandatory |
| -view viewname | |
| -input inputfilename | |
| -ipaddress mgmt-ip-address } | |
|                  | Specifies the device name of the device that you have added in the Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices). You can enter multiple device name separated by a comma. You can use either wildcard or specific device(s) but not at the same time. |
|                  | The argument syntax used for `-device` argument may be a single device or a device list. Devices in a list are separated by a ','. The wild card symbol '%' may be used to specify a group of devices having a pattern. |
|                  | For example if a pattern `x%` is specified as a device in the list, then all the LMS devices that have names that start with x will be selected for this operation. |
### Global Arguments

<table>
<thead>
<tr>
<th>Argument and Optional Fields</th>
<th>Description</th>
</tr>
</thead>
</table>
| `{ -device devicename | -view viewname | -input inputfilename | -ipaddress mgmt-ip-address }` | Mandatory  
| `{ -device devicename | -view viewname | -input inputfilename | -ipaddress mgmt-ip-address }` | Mandatory  

If the data needs to be generated for all the devices in a specific group, you can use the `-view` argument. You can use this argument to generate data for devices in all device views including system-defined groups and user-defined groups.

You can enter multiple group name separated using a comma.

For view name, you have to enter the fully qualified path as in the Group Administration window. To separate the path you must use forward slash only.

For example, `-view "/RME@ciscoworks_servername/All Devices"`

You can create an input list file that contains a list of devices to perform the operation on. The contents of the input list file are a sequence of lines. Each line specifies a device name as entered in the Device and Credential Repository.

The arguments must be specific to the function. You cannot include group names in the input list file. You can include comments in the input list file by starting each commented line with `#`.

The input file should be of this format:

```
-device 1.1.1.1,2.2.2.2,3.3.3.3
```

or

```
-device 1.1.1.1
-device 2.2.2.2
-device 3.3.3.3
```

Specify the device IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated.

You cannot use this option with `-device`, `-view`, or `-input`. Also, you cannot specify wildcard characters.

```
-d debuglevel
```

Optional

`debug_level` is a number between 1 (the least information is sent to the debug output) and 5 (the most information is sent to the debug output). If you do not specify this argument, 4(INFO) is the default debug level.

```
-l logfile
```

Optional

Logs the results of the `cwcli export` command to the specified log file name. By default the command output will be displayed on the standard out.
**Archiving cwcli export Data in XML File**

By default, the data generated through `cwcli export` command is archived at the location:

<table>
<thead>
<tr>
<th>cwcli export Command</th>
<th>Location on LMS Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>changeaudit</code></td>
<td>On Solaris and Soft Appliance: <code>/var/admin/CSCOpx/files/rme/archive/YYYY-MM-DD-HH-MM-SS-changeaudit.xml</code></td>
</tr>
<tr>
<td></td>
<td>On Windows: <code>NMSROOT\files\rme\archive\YYYY-MM-DD-HH-MM-SS-changeaudit.xml</code></td>
</tr>
<tr>
<td><code>config</code></td>
<td>On Solaris and Soft Appliance: <code>/var/admin/CSCOpx/files/rme/cwconfig/YYYY-MM-DD-HH-MM-SS-MSMS-Device_Display_Name.xml</code></td>
</tr>
<tr>
<td></td>
<td>On Windows: <code>NMSROOT\files\rme\cwconfig\YYYY-MM-DD-HH-MM-SS-MSMSMS-Device_Display_Name.xml</code></td>
</tr>
<tr>
<td><code>inventory</code></td>
<td>On Solaris and Soft Appliance: <code>/var/admin/CSCOpx/files/rme/archive/YYYY-MM-DD-HH-MM-SS-inventory.xml</code></td>
</tr>
<tr>
<td></td>
<td>On Windows: <code>NMSROOT\files\rme\archive\YYYY-MM-DD-HH-MM-SS-inventory.xml</code></td>
</tr>
</tbody>
</table>

Where `NMSROOT` is the LMS installed directory.

You can also specify a directory to store the output. This application does not have a feature to delete the files created in the archive. You should delete the files when necessary.

While generating data through the servlet, the output will be displayed in the client terminal.
Running cwcli export changeaudit

Using this command you can export the Change Audit log data in the XML format.

The command syntax for cwcli export changeaudit is:

```shell
cwcli export changeaudit [-u username -p password -device devicenames] 
[- ipaddress mgmt-ip-address] 
[-f filename] 
[-from mm/dd/yyyy] ---> eg: 05/01/2004 
[-to mm/dd/yyyy] ---> eg: 05/06/2004 
[-app comma separated list of applications] 
[-cat comma separated list of categories]
```

Arguments in square brackets ([ ]) are optional; arguments in curly braces ({ }) are required. You must provide one argument from each group of arguments in curly braces ({ }) that is separated by vertical bars (|).

If you enter an argument which has space then use double quotes for that argument. For example for Software Management, you enter this as “Software Management”.

The following table describes the arguments that are specific to cwcli export changeaudit command. The other common arguments used by cwcli export are explained in Using the cwcli export Command.

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[-from mm/dd/yyyy]</td>
<td>Optional. Enter the from date. If you enter only -from date then the report will be generated from the date that you have specified, to the current date.</td>
</tr>
<tr>
<td>[-to mm/dd/yyyy]</td>
<td>Optional. Enter the from date. If you enter only -to date then the report will be generated from the date LMS has logged Change Audit record to the -to date that you have specified.</td>
</tr>
</tbody>
</table>
Appendix A      CLI Utilities

Arguments | Description
---|---
\[-app comma separated list of applications\] | Specify the application name. The supported applications are:
  - Archive Mgmt
  - ConfigEditor
  - CwConfig
  - ICServer
  - NetConfig
  - Software Management
If you do not specify the \[-app\] argument, then changes made by all applications is reported.

\[-cat comma separated list of categories\] | Specify the category name. The supported categories are:
  - CONFIG_CHANGE—Configuration changes on the device.
  - INVENTORY_CHANGE—Hardware changes on the device.
  - SOFTWARE_CHANGE—Software changes on the device.
If you do not specify the \[-cat\] argument, then changes made by all categories is reported.

**Note** If you do not enter \[-from\] and \[-to\] arguments, all the Change Audit records logged till the current date will be displayed.

The following sections describes:
- XML Schema for cwcli export changeaudit
- XML Schema for Configuration Management Application
- XML Schema for Software Management
- Usage Examples for cwcli export changeaudit Command

XML Schema for cwcli export changeaudit

The following is the schema used for exporting the change audit data in XML format.

```xml
<?xml version = "1.0" encoding = "UTF-8"?>
<!--Generated by XML Authority. Conforms to w3c http://www.w3.org/2000/10/XMLSchema-->  
<xsd:schema xmlns:xsd = "http://www.w3.org/2000/10/XMLSchema">  
  <xsd:element name = "changeRecord">  
    <xsd:complexType>  
      <xsd:sequence>  
        <xsd:element ref = "groupId"/>  
        <xsd:element ref = "category"/>  
        <xsd:element ref = "host"/>  
        <xsd:element ref = "user"/>  
        <xsd:element ref = "device"/>  
        <xsd:element ref = "connectionMode"/>  
        <xsd:element ref = "timestamp"/>  
        <xsd:element ref = "description"/>  
      </xsd:sequence>  
    </xsd:complexType>  
  </xsd:element>  
</xsd:schema>
```

Configuration Management with Cisco Prime LAN Management Solution 4.2

OL-25941-01 A-49
Detailed Description of changeaudit Schema

The table below describes elements in the changeaudit schema:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Type of the change. For example, configuration, inventory, or software.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the LMS application involved in the network change (Device Configuration, Inventory, or Software Management).</td>
</tr>
<tr>
<td>Host</td>
<td>Host device from which the user accessed the device or the host name of the LMS server.</td>
</tr>
<tr>
<td>User</td>
<td>Name of the person who performed the change. This is the name entered when the person logged in. It can be the name under which the LMS is running, or the name under which the Telnet connection is established.</td>
</tr>
<tr>
<td>Device</td>
<td>Network device on which the change occurred. The device name as entered in the Device and Credential Repository.</td>
</tr>
<tr>
<td>ConnectionMode</td>
<td>Connection mode through which the change was made, for example, Telnet, snmp, console, or LMS.</td>
</tr>
</tbody>
</table>
The following section describes the schema used by these application when you run the command `cwcli export changeaudit` with `-app` argument:

- Archive Mgmt, ConfigEditor, CwConfig, NetConfig
- Inventory Collection Service
- Software Management

### XML Schema for Configuration Management Application

The following XML schema is used by all Configuration Management application when you run the `cwcli export changeaudit` command with `-app` argument and the `-app` argument values as either Archive Mgmt, ConfigEditor, CwConfig, or NetConfig.

The schema file is:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE schema SYSTEM "http://www.w3.org/2001/XMLSchema.dtd">
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="ConfigDiff">
    <xs:annotation>
      <xs:documentation>Comment describing your root element</xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element name="OldConfig">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Command" maxOccurs="unbounded" />
            </xs:sequence>
            <xs:attribute name="Version" type="xs:integer" />
          </xs:complexType>
        </xs:element>
        <xs:element name="NewConfig">
          <xs:complexType>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```
Detailed Description of Configuration Management Schema

The table below describes elements in the Configuration Management schema.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Type of the change. For example, configuration, inventory, or software.</td>
</tr>
<tr>
<td>Host</td>
<td>Host device from which the user accessed the device or the host name of the LMS server.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application. For example, Archive Mgmt, NetConfig, etc.</td>
</tr>
<tr>
<td>User</td>
<td>Name of the person who performed the change. This is the name entered when the person logged in. It can be the name under which the LMS is running, or the name under which the Telnet connection is established.</td>
</tr>
<tr>
<td>Device</td>
<td>Network device on which the change occurred. The device name as entered in the Device and Credential Repository.</td>
</tr>
<tr>
<td>ConnectionMode</td>
<td>Connection mode through which the change was made, for example, Telnet, snmp, console, or LMS.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Date and time at which the application communicated the network change or when Change Audit saw the change record.</td>
</tr>
<tr>
<td>Summary</td>
<td>Description describing what caused the change. For example:</td>
</tr>
<tr>
<td>ConfigDiff</td>
<td>• FirstConfig, SecondConfig</td>
</tr>
<tr>
<td></td>
<td>• DeviceName—Network device on which the change occurred. The device name as entered in the Device and Credential Repository.</td>
</tr>
<tr>
<td></td>
<td>• Version—Configuration file version number.</td>
</tr>
<tr>
<td></td>
<td>• CommandDiff Polarity—Changes in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>• POSNEG—No change</td>
</tr>
<tr>
<td></td>
<td>• POSITIVE—Added new commands</td>
</tr>
<tr>
<td></td>
<td>• IGNORED—Ignored the commands</td>
</tr>
<tr>
<td></td>
<td>• NEGATIVE—Deleted the commands</td>
</tr>
</tbody>
</table>
XML Schema for Inventory Collection Service

The following XML schema is used by Inventory Collection Service application when you run the `cwcli export changeaudit` command with `-app` argument and the `-app` argument values as ICServer.

The schema file is:

```xml
<?xml version = "1.0" encoding = "UTF-8"?>
<xsd:schema xmlns:xsd = "http://www.w3.org/2000/10/XMLSchema">
  <xsd:element name = "InventoryChangeDetailRecord">
    <xsd:complexType>
      <xsd:sequence maxOccurs = "unbounded">
        <xsd:element ref = "Section"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name = "Section">
    <xsd:complexType>
      <xsd:sequence maxOccurs = "unbounded">
        <xsd:element ref = "Attributes"/>
      </xsd:sequence>
      <xsd:attribute name = "Name" type = "xsd:string"/>
      <xsd:attribute name = "Identity" type = "xsd:string"/>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name = "Attributes">
    <xsd:complexType>
      <xsd:all maxOccurs = "unbounded">
        <xsd:element ref = "Previous_value"/>
        <xsd:element ref = "Current_value"/>
        <xsd:element ref = "Action"/>
      </xsd:all>
    </xsd:complexType>
  </xsd:element>
</xsd:schema>
```

Detailed Description of Inventory Collection Service Schema

The table below describes elements in the Inventory Collection Service schema.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the physical and logical entities. The main physical entities are Chassis, Backplane, Card, CommunicationConnector, FlashDevice, FlashPartition, FlashFile, SoftwareIdentity, PhysicalMemory. The main logical entities are ManagedNetworkElement, LogicalModule, Port, MemoryPool, OSElement, IPProtocolEndpoin, IfEntry, AdditionalInformation. See Detailed Description of the Inventory Schema for further information.</td>
</tr>
<tr>
<td>Identity</td>
<td>Identifies the entity that has changed on the device. For example: If the Flash File name has changed then Identity will be Flash Device 2, Flash Partition 3.</td>
</tr>
</tbody>
</table>
The following XML schema is used by Software Management application when you run the `cwcli export changesAudit` command with `-app` argument and the `-app` argument values as Software Management.

The schema file is:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!-- edited with XMLSPY v2004 rel. 2 U (http://www.xmlspy.com) by Cisco -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="SwimHistoryRecord">
    <xs:annotation>
      <xs:documentation>Models a set of image changes on the device.</xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element name="JobID" type="xs:positiveInteger" minOccurs="0">
          <xs:annotation>
            <xs:documentation>ID of the Job in which the change happened</xs:documentation>
          </xs:annotation>
        </xs:element>
        <xs:element name="ImageChange" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="OldImage" type="Image" />
              <xs:element name="NewImage" type="Image" />
            </xs:sequence>
            <xs:attribute name="ID" type="xs:positiveInteger" use="required" />
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="Image">
    <xs:annotation>
      <xs:documentation>Models an Image.</xs:documentation>
    </xs:annotation>
    <xs:complexType name="Image">
      <xs:sequence>
        <xs:element name="Type"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

### Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AttributeName</td>
<td>Name of the different physical and logical entities. For example: In MemoryPool, the different entities are User, Free, PoolType. See <a href="#">Detailed Description of the Inventory Schema</a> for further information.</td>
</tr>
<tr>
<td>Previous_value</td>
<td>Value of the entity before the change occurred.</td>
</tr>
<tr>
<td>Current_value</td>
<td>Value of the entity after the change occurred.</td>
</tr>
</tbody>
</table>
| Action       | Type of change that has occurred on the device:  
  - Inserted— Added a new entity.  
  - Changed— Changed in the entity.  
  - Deleted— Deleted an entity. |

### XML Schema for Software Management

The following XML schema is used by Software Management application when you run the `cwcli export changesAudit` command with `-app` argument and the `-app` argument values as Software Management.

The schema file is:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!-- edited with XMLSpy v2004 rel. 2 U (http://www.xmlspy.com) by Cisco -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="SwimHistoryRecord">
    <xs:annotation>
      <xs:documentation>Models a set of image changes on the device.</xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element name="JobID" type="xs:positiveInteger" minOccurs="0">
          <xs:annotation>
            <xs:documentation>ID of the Job in which the change happened</xs:documentation>
          </xs:annotation>
        </xs:element>
        <xs:element name="ImageChange" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="OldImage" type="Image" />
              <xs:element name="NewImage" type="Image" />
            </xs:sequence>
            <xs:attribute name="ID" type="xs:positiveInteger" use="required" />
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="Image">
    <xs:annotation>
      <xs:documentation>Models an Image.</xs:documentation>
    </xs:annotation>
    <xs:complexType name="Image">
      <xs:sequence>
        <xs:element name="Type"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```
Detailed Description of Software Management Schema

The table below describes elements in the Software Management schema.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Type of the change. For example, configuration, inventory, or software.</td>
</tr>
<tr>
<td>Host</td>
<td>Host device from which the user accessed the device or the host name of the LMS server.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application. For example, Archive Mgmt, NetConfig, etc.</td>
</tr>
<tr>
<td>User</td>
<td>Name of the person who performed the change. This is the name entered when the person logged in. It can be the name under which the LMS is running, or the name under which the Telnet connection is established.</td>
</tr>
<tr>
<td>Device</td>
<td>Network device on which the change occurred. The device name as entered in the Device and Credential Repository.</td>
</tr>
<tr>
<td>ConnectionMode</td>
<td>Connection mode through which the change was made, for example, Telnet, snmp, console, or LMS.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Date and time at which the application communicated the network change or when Change Audit saw the change record.</td>
</tr>
<tr>
<td>Summary</td>
<td>Description describing what caused the change. For example, Software upgrade.</td>
</tr>
<tr>
<td>Job ID</td>
<td>Job ID for the Software Upgrade.</td>
</tr>
</tbody>
</table>
Example 1: To generate the Change Audit report for all applications and categories for a particular device group.

cwcli export changeaudit -u admin -p admin -view "/RME@ciscoworksservername/Normal Devices"

Example 2: To generate the Change Audit report for a specific application and category for a device in a given time frame

cwcli export changeaudit -u admin -p admin -device 10.6.8.6 -from 09/30/2004 -to 10/15/2004 -app "Archive Mgmt" -cat CONFIG_CHANGE

Example 3: To generate the Change Audit report in the given output file

cwcli export changeaudit -u admin -p admin -device % -f changeaudit.xml

Example 4: To generate the Change Audit using the cwcli get request

The password that you enter here must be in base64 encoded.

In this example,
- YWRtaW4= is the base64 encoded password for admin.
- %25 is the URL encode for “%”
- %2f is the URL encode for “_”
Enter this in your browser:

```
http://ciscowork_servername:1741/rme/cwcli?command=cwcli export changeaudit -u admin -p YWRtaW4= -device 10.7.3.8 -app %22Archive Mgmt%22 -cat %22CONFIG%2fCHANGE%22 -f changeaudit.xml
```

The output for this is written to the changeaudit.xml file. The changeaudit.xml file is located:

On Windows:

```
NMSROOT\MDC\tomcat
```

Where, **NMSROOT** is the LMS installed directory.

On Solaris and Soft Appliance:

```
NMSROOT/objects/dmgt
```

**Example 5: To generate the Change Audit report using cwcli post request method**

The password that you enter here must be in base64 encoded. In this example, `YWRtaW4=` is the base64 encoded password for admin.

The payload file, `changeaudit.xml` contains:

```
<payload>
  <command>
    cwcli export changeaudit -u admin -p YWRtaW4= -device 1.6.8.6 -from 09/30/2004 -app "Archive Mgmt" -cat CONFIG_CHANGE -view "/RME@CiscoWorks_servername/Pre-deployed" -f changeauditreport.xml
  </command>
</payload>
```

At the command prompt enter:

```
perl samplepost.pl https://LMS_Servername:443/rme/cwcli changeaudit.xml
```

To invoke the servlet using a script, see the **Overview: cwcli invreport Command**.

**SUMMARY**

```
Successful: export: changeauditreport.xml
<-- Processing complete -->
```

The output for this is written to the `changeauditreport.xml` file. The `changeauditreport.xml` file is located:

On Windows:

```
NMSROOT\MDC\tomcat
```

Where, **NMSROOT** is the LMS installed directory.

On Solaris and Soft Appliance:

```
NMSROOT/objects/dmgt
```
Running cwcli export config

Using this command you can retrieve the configuration data in the XML format specified by the schema. The Configlet Generator provides a wrapper over the existing Config Archive to retrieve configlets data for the selected device. The exported data contains the entire running configuration data.

The command syntax for cwcli export config is:


Arguments in square brackets ([ ]) are optional; arguments in curly braces ({ }) are required. You must provide one argument from each group of arguments in curly braces ({ }) that is separated by vertical bars (!).

If you enter an argument which has space then use double quotes for that argument.

The following table describes the argument that is specific to cwcli export config command. The other common arguments used by cwcli export are explained in Using the cwcli export Command.

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s 1</td>
<td>Optional. Displays the exported configuration file on the console. If you use this command, you can specify only one device. You cannot export the configuration files of multiple devices. To export the configuration files of multiple devices, either make multiple requests to the servlet, or get these files from the LMS server. Usage of this option: cwcli export config -u admin -p admin -device 10.22.33.44 -s 1</td>
</tr>
</tbody>
</table>

The output files depends on the number of devices specified. There are as many configuration XML output files as the number of devices. The output files are created under this location on LMS server:

On Solaris and Soft Appliance:
/var/adm/CSCOpx/files/rme/cwconfig/YYYY-MM-DD-HH-MM-SS-XXX-Device_Display_Name.xml

On Windows:
NMSROOT\files\rme\cwconfig\YYYY-MM-DD-HH-MM-SS-XXX-Device_Display_Name.xml

Where NMSROOT is the LMS installed directory.
XML Schema for cwcli export config

The following is the schema used for exporting the configuration data in XML format.

```xml
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="DeviceConfiguration">
    <xs:annotation>
      <xs:documentation>This has list of Configlets</xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Configlet" maxOccurs="unbounded" />
        <xs:element name="DeviceName" type="xs:string" />
        <xs:element name="DeviceFamily" type="xs:string" />
        <xs:element name="CreationTime" type="xs:date" />
        <xs:element name="Version" type="xs:string" />
        <xs:element name="Data" minOccurs="0" />
      </xs:sequence>
    </xs:complexType>
    <xs:element name="Configlet">
      <xs:annotation>
        <xs:documentation>Configlet can have subconfiglets</xs:documentation>
      </xs:annotation>
      <xs:complexType>
        <xs:sequence>
          <xs:element ref="Configlet" minOccurs="0" maxOccurs="unbounded" />
          <xs:element name="command" minOccurs="0" maxOccurs="unbounded" type="xs:string">
            <xs:complexType>
              <xs:simpleContent>
                <xs:extension base="xs:string">
                  <xs:attribute name="LineNo" />
                </xs:extension>
              </xs:simpleContent>
            </xs:complexType>
          </xs:element>
          <xs:element name="SubModeCommand" type="xs:string" minOccurs="0" />
        </xs:sequence>
      </xs:complexType>
      <xs:attribute name="Name" type="xs:string" use="required" />
    </xs:element>
  </xs:element>
</xs:schema>
```
Detailed Description of config Schema

The table below describes elements in the config schema:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Device device name as entered in the Device and Credential Repository.</td>
</tr>
<tr>
<td>Date</td>
<td>Date and time at which the configuration changes have occurred.</td>
</tr>
<tr>
<td>Version</td>
<td>Configuration file version.</td>
</tr>
<tr>
<td>Configlet name</td>
<td>Name of the configlet. The available configlets vary from device to device; the following are examples:</td>
</tr>
<tr>
<td></td>
<td>• SNMP displays SNMP configuration commands, for example, snmp-server community public RO.</td>
</tr>
<tr>
<td></td>
<td>• IP Routing displays IP routing configuration commands, for example, router abcd 100.</td>
</tr>
<tr>
<td></td>
<td>• Interface folder displays the different interface configuration commands, for example, Interface Ethernet0 and Interface TokenRing.</td>
</tr>
<tr>
<td></td>
<td>• Global displays global configuration commands, for example no ip address.</td>
</tr>
<tr>
<td></td>
<td>• Line con 0 displays configuration commands for line console 0.</td>
</tr>
<tr>
<td></td>
<td>• IP displays IP configuration commands, for example, ip http server.</td>
</tr>
</tbody>
</table>
Usage Examples for cwcli export config Command

This section provides some examples of usage for the cwcli export config command.

Example 1: To generate the config report for a particular device group

cwcli export config -u admin -p admin -view "/RME@ciscoworksservername/Normal Devices"

SUMMARY
========
Successful: ConfigExport:D:/PROGRA~1/CSCOpx/files/rme/cwconfig

The output folder will contain separate config file for every devices in the Normal Devices group.

Example 2: To generate the config report for the devices that are specified in the device input file

The input configdevices.txt contains these devices:
-device 10.22.33.44,10.22.33.55,1.1.1.1

cwcli export config -u admin -p admin -input configdevices.txt

Example 3: To generate the config using the cwcli get request

The password that you enter here must be in base64 encoded.

In this example,
• YWRtaW4= is the base64 encoded password for admin.
• %25 is the URL encode for “%”

Enter this in your browser:
http://ciscowork_servername:1741/rme/cwcli?command=cwcli export config -u admin -p YWRtaW4= -device %25

<!-- Processing Starts -->

SUMMARY
========
Successful: ConfigExport: D:/PROGRA~1/CSCOpx/files/rme/cwconfig

<!-- Processing complete -->

Example 4: To generate the Change Audit report using cwcli post request method

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

The payload file, config.xml contains:
<payload>
  <command>
cwcli export config -u admin -p YWRtaW4= -device 1.6.8.6
  </command>
</payload>

At the command prompt enter:
perl samplepost.pl https://LMS_Servername:443/rme/cwcli config.xml

<!-- Processing Starts -->
SUMMARY
==========
Successful: ConfigExport: D:/PROGRA~1/CSCOpx/files/rme/cwconfig
<!-- Processing complete -->
To invoke the servlet using a script, see the Overview: cwcli invreport Command.

Running cwcli export inventory Command

Using this command you can export inventory data in the XML format.
The command syntax for cwcli export inventory is:

```
cwcli export inventory [-u username -p password][-a debuglevel][-m mailid][-l logfile][-f filename]
```

The above command retrieves the inventory data in XML format specified by the schema. The -f parameter stores the output in the file specified by filename. If you have not specified the filename, the output is stored at the following location:

`PX_DATADIR\rme\archive\timestampinventory.xml` (On Solaris and Soft Appliance)

`PX_DATADIR\rme\archive\timestampinventory.xml` (On Windows)

Where `PX_DATADIR` is the NMSROOT/files directory and `NMSROOT` is the LMS installed directory.

The device name can also have a wild card symbol "%" to choose all devices with that particular name.

If the number of devices is large, the list of devices can be stored in an input file and the name of the input file can be given in the command line. The input argument cannot occur with the device or view arguments.

If the data needs to be generated for all the devices in a specific group, you can use the -view argument.
You can use this argument to generate data for devices in all device groups including system-defined groups and user-defined groups.

The following table describes the arguments that are specific to cwcli export inventory command. The other common arguments used by cwcli export are explained in Using the cwcli export Command.

<table>
<thead>
<tr>
<th>Global Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-hop hopdevice</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>Used to increase performance by using more memory. This indicates the number of devices to be worked upon at a time. By default, this value is 1.</td>
</tr>
</tbody>
</table>

Given below is the list of combinations, which could occur for the inventory command.

```
cwcli export inventory -u admin -p admin -f myinv.xml
cwcli export inventory -u admin -p admin -f myinv.xml -device device1
cwcli export inventory -u admin -p admin -device device%
```

```
cwcli export inventory -u admin -p admin -input inv.txt
```

```
cwcli export inventory -u admin -p admin -view "/RME@ciscoworksservername/Normal Devices"
```

```
cwcli export inventory -u admin -p admin -f myinv.xml -input inv.txt
```
To apply the `cwcli export` command on more than one LMS device you must use the format in the example given below. The parameter, inputlist, is a text file which will have the list of device names separated by a new line. A line starting with # will be treated as a comment.

Example:

```bash
#comment
-device device1,device2,device3
#comment
```

where device1, device2, and device3 are device displaynames.

XML Schema for cwcli export inventory Data

The following is the schema used for exporting the inventory data in XML format.

```xml
<?xml version = "1.0" encoding = "UTF-8"?>
<xs:schema xmlns:xs = "http://www.w3.org/2001/XMLSchema" elementFormDefault = "qualified" attributeFormDefault = "unqualified">
<!--This schema is based on the classes defined in Cisco Information Model V2.0 (CIMXV2.0) Each Device has Chassis and NetworkElement.
Chassis:
  Chassis contains a blackplane and multiple Cards. Each Card contains CommunicationConnectors and multiple daughter cards. Flash Devices reside on the Cards. NetworkElement:
  System Information, Interface Information and LogicalModules. LogicalModules contain OSElements and Logical Ports.
The element AdditionalInformation is meant to capture device specific details that are not part of the common schema. -->
<xs:element name = "InvDetails">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref = "SchemaInfo" minOccurs = "0" maxOccurs = "1"/>
      <xs:element ref = "RMEPlatform" minOccurs = "0" maxOccurs = "unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name = "SchemaInfo">
  <xs:complexType>
    <xs:sequence>
      <xs:element name = "RMEServer" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
      <xs:element name = "CreatedAt" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
      <xs:element name = "SchemaVersion" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name = "RMEPlatform">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref = "Cisco_Chassis" minOccurs = "0" maxOccurs = "unbounded"/>
      <xs:element ref = "Cisco_NetworkElement" minOccurs = "0" maxOccurs = "unbounded"/>
      <xs:element ref = "Cisco_ComputerSystemPackage" minOccurs = "0" maxOccurs = "unbounded"/>
      <xs:element ref = "Cisco_EnergyWise" minOccurs = "0" maxOccurs = "1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name = "Cisco_Chassis">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref = "InstanceID" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

Configuration Management with Cisco Prime LAN Management Solution 4.2
<xs:element name = "InstanceID" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "FlashDeviceType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Size" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NumberOfPartitions" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ChipCount" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Removable" type = "xs:boolean" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "Cisco_FlashPartition" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
<xs:restriction base="xs:string">
  <xs:enumeration value="nvRam"/>
  <xs:enumeration value="NVRAM"/>
  <xs:enumeration value="processorRam"/>
  <xs:enumeration value="RAM"/>
  <xs:enumeration value="ROM"/>
  <xs:enumeration value="FEPROM"/>
  <xs:enumeration value="BRAM"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:complexType>
<xs:element name = "Cisco_IPProtocolEndpoint">
  <xs:complexType>
    <xs:sequence>
      <xs:element name = "Address" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
      <xs:element name = "SubnetMask" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
      <xs:element name = "DefaultGateway" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
      <xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name = "Cisco_PEHasIfEntry">
  <xs:complexType>
    <xs:sequence>
      <xs:element name = "Cisco_IPProtocolEndpoint" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
      <xs:element name = "Cisco_IFEntry" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name = "Cisco_ComputerSystemPackage">
  <xs:complexType>
    <xs:sequence>
      <xs:element name = "Antecedent" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
      <xs:element name = "Dependent" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name = "Cisco_EnergyWise">
  <xs:complexType>
    <xs:sequence>
      <xs:element name = "InstanceID" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
      <xs:element name = "DomainName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
      <xs:element name = "Role" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
      <xs:element name = "Keyword" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name = "SoftwareIdentity">
  <xs:complexType>
    <xs:sequence>
      <xs:element name = "Classification" minOccurs = "0" maxOccurs = "1">
        <xs:simpleType>
          <xs:restriction base = "xs:string">
            <xs:enumeration value = "Firmware"/>
            <xs:enumeration value = "Software"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name = "VersionString" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
</xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
</xs:schema>
Detailed Description of the Inventory Schema

The inventory schema provides the structure for the inventory information exported from LMS. The schema divides inventory information into two groups:

- Physical Inventory
- Logical Inventory

The Physical Inventory contains the chassis information and related details for the device. The main elements in the schema for the physical inventory part are:

- Chassis (Cisco_Chassis)
- Backplane (Cisco_Backplane)
- Card (Cisco_Card)
- CommunicationConnector (Cisco_CommunicationConnector)
- FlashDevice (Cisco_FlashDevice)
- FlashPartition (Cisco_FlashPartition)
- FlashFile (Cisco_FlashFile)
- SoftwareIdentity (Cisco_SoftwareIdentity)
- PhysicalMemory (Cisco_PhysicalMemory)

The Logical Inventory part of the schema contains the details of the managed network element. The main elements in the schema for the logical inventory part are:

- ManagedNetworkElement (Cisco_NetworkElement)
- LogicalModule (Cisco_LogicalModule)
- Port (Cisco_Port)
- MemoryPool (Cisco_MemoryPool)
- OSElement (Cisco_OSElement)
- IPProtocolEndpoint (Cisco_IPProtocolEndpoint)
- IfEntry (Cisco_IfEntry)
- Additional Information

Chassis (Cisco_Chassis)

The Chassis class represents the physical elements that enclose other elements in the device and provide specific functions, such as a desktop, networking node, UPS, disk or tape storage, or a combination of these functions.

The following table describes the elements in Chassis:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceID</td>
<td>Unique identifier.</td>
</tr>
<tr>
<td>Model</td>
<td>Chassis model / Chassis ID.</td>
</tr>
<tr>
<td>Version</td>
<td>Hardware version of the chassis</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>Serial number associated with the chassis.</td>
</tr>
<tr>
<td>Type</td>
<td>Chassis type.</td>
</tr>
</tbody>
</table>
Chassis also contains the elements Card and Backplane.

**Backplane (Cisco_Backplane)**

Backplane is an instance of a backplane in a chassis. The following table describes the elements in Backplane:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BackplaneType</td>
<td>Type of backplane</td>
</tr>
<tr>
<td>Model</td>
<td>Model of the backplane</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>Serial number of the backplane</td>
</tr>
</tbody>
</table>

**Card (Cisco.Card)**

Card represents:

- A type of physical container that can be plugged into another card, motherboard, or hosting board
- A motherboard or hosting board in a chassis

This element includes any package capable of carrying signals and providing a mounting point for physical components such as chips, or other physical packages such as other cards. The following table describes the elements in Card:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceID</td>
<td>Card number. This is used to correlate with the logical part of the card.</td>
</tr>
<tr>
<td>Model</td>
<td>Model of the card.</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>Serial number of the card.</td>
</tr>
<tr>
<td>LocationWithinContainer</td>
<td>Number that indicates the physical slot number. This can be used as an index into a system slot table, irrespective of whether that slot is physically occupied or not.</td>
</tr>
<tr>
<td>PartNumber</td>
<td>Part number of the Hardware Component.</td>
</tr>
<tr>
<td>CardType</td>
<td>Type of the card (Card Type)</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive string used to describe the card.</td>
</tr>
<tr>
<td>OperationalStatus</td>
<td>Status of the card describing whether it is up or down</td>
</tr>
<tr>
<td>FWManufacturer</td>
<td>Manufacturer of the firmware</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Manufacturer of the hardware</td>
</tr>
<tr>
<td>NumberOfSlots</td>
<td>Number of slots in the card.</td>
</tr>
<tr>
<td>NoOfCommunicationConnectors</td>
<td>Number of ports in the card.</td>
</tr>
</tbody>
</table>
Apart from the elements described in the table above, the card element also contains reference to itself, which can represent a sub card. It also contains other elements such as CommunicationConnector and FlashDevice.

**CommunicationConnector (Cisco_CommunicationConnector)**

CommunicationConnector represents a physical port. The table below describes the elements in CommunicationConnector:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceID</td>
<td>Indicates the connector number for the chassis or system.</td>
</tr>
<tr>
<td>ConnectorType</td>
<td>Type of the physical port.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive string used to describe the card.</td>
</tr>
</tbody>
</table>

**FlashDevice (Cisco_FlashDevice)**

FlashDevice represents physical flash memory. Flash memory may reside on a PCMCIA card, line card, or any other type of card. FlashDevice may consist of one or more actual flash memory chips.

It also consists of reference to one or more flash partitions described in FlashPartition. The table below describes the elements in FlashDevice:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceID</td>
<td>FlashDevice sequence number to index the flash devices within the table of initialized FlashDevices.</td>
</tr>
<tr>
<td>InstanceName</td>
<td>Name of FlashDevice. This name is used to refer to the device within the system. Flash operations get directed to a device based on this name.</td>
</tr>
<tr>
<td>Size</td>
<td>Total size of FlashDevice. For a removable device, the size will be zero if the device has been removed.</td>
</tr>
<tr>
<td>NumberOfPartitions</td>
<td>Number of Flash partitions present in FlashDevice</td>
</tr>
<tr>
<td>ChipCount</td>
<td>Total number of chips within FlashDevice. This element provides information to a network management station on how much chip information to expect. It also helps the management station to check the chip index against an upper limit when randomly retrieving chip information for a partition.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of a FlashDevice. The description is meant to explain what FlashDevice is and its purpose.</td>
</tr>
<tr>
<td>Removable</td>
<td>Specifies whether FlashDevice is removable. Typically, only PCMCIA Flash cards are treated as removable. Socketed Flash chips and Flash SIMM modules are not treated as removable.</td>
</tr>
</tbody>
</table>

**FlashPartition (Cisco_FlashPartition)**

FlashPartition corresponds to the Cisco-flash-mib. The elements in FlashPartition are derived from the table of properties of ciscoFlashPartitionTable for each initialized flash partition.

When there is no explicit partitioning for a device, it is assumed that there is a single partition spanning the entire device exists. Therefore, a device always has at least one partition.
FlashPartition contains one or more FlashFileSystems as described in FlashFile. The table below describes the elements in FlashPartition.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceID</td>
<td>FlashPartition sequence number used to index FlashPartitions within the table for initialized FlashPartitions.</td>
</tr>
<tr>
<td>InstanceName</td>
<td>FlashPartition name used to refer to a partition by the system.</td>
</tr>
<tr>
<td>PartitionStatus</td>
<td>Status of the partition.</td>
</tr>
<tr>
<td>Upgrade</td>
<td>Upgrade information for the partition. This helps to download new files into the partition, and is needed when the PartitionStatus is run from flash.</td>
</tr>
<tr>
<td>NeedsErasure</td>
<td>Boolean parameter indicating whether the partition requires to be erased before any write operations can occur.</td>
</tr>
<tr>
<td>Size</td>
<td>FlashPartition size. It should be an integral multiple of ciscoFlashDeviceMinPartitionSize. If there is a single partition, this size will be equal to ciscoFlashDeviceSize.</td>
</tr>
<tr>
<td>FreeSpace</td>
<td>Free space within aFlashPartition.</td>
</tr>
<tr>
<td>FileCount</td>
<td>Number of files stored in the file system.</td>
</tr>
</tbody>
</table>

**FlashFile (Cisco_FlashFile)**

FlashFile manages the storage and organization of files on a Flash memory device. The table below describes the elements in FlashFile.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceID</td>
<td>FlashFile sequence number used to index within a FlashPartition directory table.</td>
</tr>
<tr>
<td>FileSize</td>
<td>Size of the file in bytes. This size does not include the size of the filesystem file header.</td>
</tr>
<tr>
<td>FileStatus</td>
<td>Status of a file. A file could be explicitly deleted if the file system supports such a user command. Alternatively, an existing good file would be automatically deleted if another good file with the same name were copied in. Deleted files continue to occupy prime space in flash memory. A file is marked as having an invalid checksum if any checksum mismatch was detected while writing or reading the file. Incomplete files (files truncated either because of lack of free space, or because of a network download failure) are also written with a bad checksum and marked as invalid.</td>
</tr>
<tr>
<td>Checksum</td>
<td>File checksum stored in the file header. This checksum is computed and stored when the file is written into Flash memory, and serves to validate the data written into Flash. Where the system generates and stores the checksum internally in hexadecimal form, checksum provides the checksum in a string form. Checksum is available for all valid and invalid-checksum files.</td>
</tr>
<tr>
<td>FileName</td>
<td>FlashFile name as specified by the user while copying the file to Flash memory. The name should not include the colon (:) character as it is a special separator character used to separate the device name, partition name, and the file name.</td>
</tr>
</tbody>
</table>
SoftwareIdentity (Cisco_SoftwareIdentity)

SoftwareIdentity provides the hardware and firmware version of the card. The table below describes elements in SoftwareIdentity.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification</td>
<td>Specifies whether the information is for hardware or firmware.</td>
</tr>
<tr>
<td>VersionString</td>
<td>Version information for software or firmware.</td>
</tr>
</tbody>
</table>

PhysicalMemory (Cisco_PhysicalMemory)

PhysicalMemory specifies the memory type and capacity of the device. The table below describes elements in PhysicalMemory.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MemoryType</td>
<td>Specifies the type of memory, that is whether RAM, ROM, or NVRAM.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Capacity in bytes.</td>
</tr>
</tbody>
</table>

ManagedNetworkElement (Cisco_NetworkElement)

ManagedNetworkElement is the entity that contains all logical parts of the device, which the users can configure (such as Logical Module, Port, Interfaces, Software Image details, and Memory Pool). The table below describes elements in ManagedNetworkElement.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceID</td>
<td>Index number assigned to the network element.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the network element. This description includes the full name and version identification of the system's hardware type, operating system, and networking software. The description can have only printable ASCII characters.</td>
</tr>
<tr>
<td>PrimaryOwnerName</td>
<td>Identification of the contact person for this managed node, and information on how to contact this person.</td>
</tr>
<tr>
<td>InstanceName</td>
<td>Administratively defined name for the network element.</td>
</tr>
<tr>
<td>PhysicalPosition</td>
<td>Physical location of the network element.</td>
</tr>
<tr>
<td>SysObjectId</td>
<td>Vendor's authoritative identification of the management subsystem contained in the element.</td>
</tr>
<tr>
<td>SysUpTime</td>
<td>Time in hundredths of a second since the network management portion of the element was last initialized.</td>
</tr>
<tr>
<td>OfficialHostName</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>NumberOfPorts</td>
<td>Number of ports in the network element.</td>
</tr>
</tbody>
</table>
LogicalModule (Cisco_LogicalModule)

LogicalModule is the logical device corresponding to a line card in the network device.

For example, a line card in a switch is an instance of LogicalModule, associated with the ManagedNetworkElement, in this case the switch. LogicalModule is not necessarily independently managed.

To represent a sub module, LogicalModule contains a reference to itself. It also contains Port and the OSElement. The table below describes the other elements in LogicalModule.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceID</td>
<td>Index that correlates the physical card and the logical module. This helps to correlate the physical card to logical card details.</td>
</tr>
<tr>
<td>ModuleNumber</td>
<td>Number assigned to the module by its parent ManagedNetworkElement.</td>
</tr>
<tr>
<td>ModuleType</td>
<td>Type or model of the module.</td>
</tr>
<tr>
<td>InstanceName</td>
<td>Name of the logical module.</td>
</tr>
<tr>
<td>EnabledStatus</td>
<td>Status of the module, that is whether it is up or down.</td>
</tr>
<tr>
<td>NumberOfPorts</td>
<td>Number of ports in the logical module.</td>
</tr>
</tbody>
</table>

Port (Cisco_Port)

Port is the logical representation of network communications hardware - a physical connector and the setup or operation of the network chips, at the lowest layers of a network stack.

For example, an Ethernet port on an Ethernet line card uses an instance of Port to represent its operational and logical properties. A port should be associated with either a LogicalModule or directly with a ManagedNetworkElement.

It also contains the element IPProtocolEndpoint. The table below describes the other elements in Port.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PortNumber</td>
<td>Number assigned to the port. Ports are often numbered relative to either a logical module or a network element.</td>
</tr>
<tr>
<td>PortType</td>
<td>Type of the port.</td>
</tr>
<tr>
<td>InstanceName</td>
<td>Name assigned to the port.</td>
</tr>
<tr>
<td>IfInstanceID</td>
<td>Index of the interface related to this port.</td>
</tr>
</tbody>
</table>
MemoryPool (Cisco_MemoryPool)

MemoryPool corresponds to entries to monitor entries. Each pool is a range of memory segregated by type or function. The table below describes the other elements in MemoryPool.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceName</td>
<td>Name assigned to the MemoryPool.</td>
</tr>
<tr>
<td>PoolType</td>
<td>Dynamic type value assigned to a dynamic MemoryPool. This is valid only when the PoolType attribute has the value Dynamic. MemoryPools can be divided into two groups Predefined Pools and Dynamic Pools. For dynamic pools, the PoolType is set to the dynamic value (65536) and the DynamicPoolType is set to an integer value used to distinguish the various dynamic pool types.</td>
</tr>
<tr>
<td>DynamicPoolType</td>
<td>This attribute holds the dynamic type value assigned to a dynamic memory pool. It is only valid when the PoolType attribute has the value Dynamic (65536).</td>
</tr>
<tr>
<td>AlternatePoolType</td>
<td>Indicates whether this MemoryPool has an alternate pool configured. Alternate pools are used for fallback when the current pool runs out of memory. If the value is set to zero, then this pool does not have an alternate. Otherwise the value is the same as the value of PoolType of the alternate pool.</td>
</tr>
<tr>
<td>IsValid</td>
<td>Indicates whether the other attributes in this MemoryPool contain accurate data. If an instance of this object has the value, False, (indicating an internal error condition), the values of the remaining objects in the instance may contain inaccurate information. That is, the reported values may be less than the actual values.</td>
</tr>
<tr>
<td>Used</td>
<td>Indicates the number of bytes from the MemoryPool that are currently in use by applications on the managed device.</td>
</tr>
<tr>
<td>Allocated</td>
<td>Indicates the number of bytes from the MemoryPool that are currently unused on the managed device.</td>
</tr>
<tr>
<td>Free</td>
<td>Indicates the largest number of contiguous bytes from the MemoryPool that are currently unused on the managed device.</td>
</tr>
</tbody>
</table>

OSElement (Cisco_OSElement)

OSElement represents the software element that is deployed to a network system and describes the software behind the operating system. The table below describes the other elements in OSElement.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceName</td>
<td>Name of the OS image.</td>
</tr>
<tr>
<td>Family</td>
<td>Family of the OS component.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the OS.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the OS image.</td>
</tr>
</tbody>
</table>
**IPProtocolEndpoint (Cisco_IPProtocolEndpoint)**

IPProtocolEndpoint contains the subnet mask and default gateway information corresponding to the management IP Address.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>IP address of this endpoint, formatted according to the convention as defined in the AddressType property of this class.</td>
</tr>
<tr>
<td>SubnetMask</td>
<td>Mask for the IP address of this element, formatted according to the convention as defined in the AddressType property of this class (e.g., 255.255.252.0).</td>
</tr>
<tr>
<td>DefaultGateway</td>
<td>Default gateway address.</td>
</tr>
</tbody>
</table>

**IfEntry (Cisco_IfEntry)**

IfEntry represents the contents of an entry in the ifTable as defined in RFC 1213.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceID</td>
<td>Index in the interface table defined in RFC 1213 for the entry containing the interface attributes of this object.</td>
</tr>
<tr>
<td>InstanceName</td>
<td>ifName attribute in the interface table defined in RFC 1213.</td>
</tr>
<tr>
<td>IfType</td>
<td>Interface type enumeration taken from the IANA definition of ifType.</td>
</tr>
<tr>
<td>IfSpeed</td>
<td>Estimate of the current bandwidth of the interface in bits per second. In cases, where the current bandwidth cannot be given, the nominal bandwidth should be specified.</td>
</tr>
<tr>
<td>IfAdminStatus</td>
<td>Desired state of the interface.</td>
</tr>
<tr>
<td>IfOperStatus</td>
<td>Current operational status of the interface.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the interface.</td>
</tr>
<tr>
<td>PhysicalAddress</td>
<td>Hardware address of the interface.</td>
</tr>
<tr>
<td>NetworkAddress</td>
<td>Network address of the interface.</td>
</tr>
</tbody>
</table>

**Additional Information**

AdditionalInformation is used to describe device specific information. It contains name and value attributes for elements specific to the device.

<table>
<thead>
<tr>
<th>Class</th>
<th>Element</th>
<th>AdditionalInformation Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Call Manager</td>
<td>Cisco_NetworkElement</td>
<td>ActivePhones, InActivePhones, ActiveGateways, InActiveGateways, CallManagerIndex, CallManagerName, CallManagerDescription, CallManagerVersion, CallManagerStatus</td>
</tr>
<tr>
<td></td>
<td>Cisco_Chassis</td>
<td>ApplicationPackageIndex, PackageManufacturer, Productname, Packageversion, Package SerialNumber</td>
</tr>
<tr>
<td>Class</td>
<td>Element</td>
<td>Additional Information Tag</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Cisco FastSwitch With_Module</td>
<td>Cisco_NetworkElement</td>
<td>FwdEngRev, BoardRev, SwitchPortNumber, SharedPortNumber, FirmwareSource</td>
</tr>
<tr>
<td></td>
<td>Cisco_FlashDevice</td>
<td>FlashBankStatus</td>
</tr>
<tr>
<td></td>
<td>Cisco_Card</td>
<td>InstanceID, ID</td>
</tr>
<tr>
<td>Cisco Firewall</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Cisco IPX-IGX-BPX</td>
<td>Cisco_Chip</td>
<td>InstanceName, Number</td>
</tr>
<tr>
<td></td>
<td>Cisco_Card</td>
<td>SecondarySwRev, slotIndex, RAMId, ROMId, BRAMId, BOOTId, LocationWithinContainer, SecondaryStatus</td>
</tr>
<tr>
<td></td>
<td>Cisco_Port</td>
<td>switchIfSlot, switchIfPort, SubPortNo, Status, Speed, PortType</td>
</tr>
<tr>
<td>Cisco LS1010 Switch</td>
<td>Cisco_Chip</td>
<td>Slot0 (Type), Slot1(Type), AvailableSlots</td>
</tr>
<tr>
<td></td>
<td>Cisco_NetworkElement</td>
<td>ConfigReg</td>
</tr>
<tr>
<td></td>
<td>Cisco_PhysicalMemory</td>
<td>NVRAMUsed, RomVersion</td>
</tr>
<tr>
<td>Cisco MGX</td>
<td>Cisco_Chip</td>
<td>Name, switchIfSlot, switchIfPort, SubPortNo, Status, Speed, PortType</td>
</tr>
<tr>
<td>Cisco Catalyst 3900 Switch</td>
<td>Cisco_Chip</td>
<td>ModuleCount, Configuration, SwitchCount</td>
</tr>
<tr>
<td></td>
<td>Cisco_Card</td>
<td>CiscoTsNumber, PermanentMAC, LocalMAC, CiscoTsModNumber, StackNo</td>
</tr>
<tr>
<td>Cisco Router 700 Series</td>
<td>Cisco_Chip</td>
<td>MACAddress, PortCount, Type</td>
</tr>
<tr>
<td>Cisco Router</td>
<td>Cisco_PhysicalMemory</td>
<td>NVRAMUsed, ROMVersion</td>
</tr>
<tr>
<td></td>
<td>Cisco_NetworkElement</td>
<td>Config</td>
</tr>
<tr>
<td>Cisco Catalyst IOS Switch</td>
<td>Cisco_Chip</td>
<td>MACAddress, PortCount, Type</td>
</tr>
<tr>
<td></td>
<td>Cisco_Card</td>
<td>FlashSize,FlashFree,FlashCard</td>
</tr>
<tr>
<td></td>
<td>Cisco_Chip</td>
<td>Config</td>
</tr>
<tr>
<td></td>
<td>Cisco_PhysicalMemory</td>
<td>NVRAMUsed, ROMVersion</td>
</tr>
<tr>
<td>Cisco Catalyst L2L3 Switch</td>
<td>Cisco_Chip</td>
<td>Slot0, Slot1, MACAddress, PortCount, Type</td>
</tr>
<tr>
<td></td>
<td>Cisco_NetworkElement</td>
<td>Config</td>
</tr>
<tr>
<td></td>
<td>Cisco_PhysicalMemory</td>
<td>NVRAMUsed, ROMVersion</td>
</tr>
<tr>
<td>Cisco VPN 3000 Concentrators</td>
<td>Cisco_Chip</td>
<td>PowerSupply1Type, PowerSupply2Type, RAMSize</td>
</tr>
<tr>
<td></td>
<td>Cisco_Card</td>
<td>LocationWithinContainer, CryptoHardwareType, SepState, DSPCodeVersion</td>
</tr>
<tr>
<td>Cisco Catalyst Switch</td>
<td>Cisco_Chip</td>
<td>PowerSupply1, PowerSupply2, MgmtType, BroadcastAddress, AvailableSlots</td>
</tr>
<tr>
<td></td>
<td>Cisco_Card</td>
<td>ModuleIndex, RedundantModule, ModuleSubType</td>
</tr>
<tr>
<td></td>
<td>Cisco_LogicalModule</td>
<td>moduleIndex,ModuleIPAddress</td>
</tr>
<tr>
<td>Cisco Optical Switches</td>
<td>Cisco_NetworkElement</td>
<td>RFUnitDetected, RFUnitID, RFUnitState, RFPeerUnitID, RFPeerUnitState, ActivateRF, ManualSwitchPermitted, StartupSyncStatus, RunningSyncStatus</td>
</tr>
<tr>
<td></td>
<td>Cisco_PhysicalMemory</td>
<td>NVRAMUsed</td>
</tr>
</tbody>
</table>
Overview: cwcli inventory Command

The cwcli inventory is a Device Management application command line tool. This tool supports the following features:

- You can check the specified device credentials for the devices.
- You can export device credentials of one or more devices in clear text.
- You can delete the specified devices.
- You can view the devices state.

The cwcli inventory command is located in the following directories, where install_dir is the directory in which LMS is installed:

- On Solaris and Soft Appliance systems, /opt/CSCOpx/bin
- On Windows systems, install_dir\CSCOpx\bin

  The default install directory is C:\Program Files.

This section contains:

- Using the cwcli inventory Command
- Running the cwcli inventory cda Command
- Running the cwcli inventory crmexport Command
- Running the cwcli inventory deletedevice Command
- Running the cwcli inventory getdevicestate Command

If you install LMS on an NTFS partition on Windows, only users in the administrator or casuser group can access cwcli inventory.

You can also perform the cwcli inventory tasks using the servlet. You will have to upload a payload XML file, which contains the cwcli inventory command arguments and LMS user credentials.

You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the output either on the console or in the specified output file, if the credentials are correct and arguments are valid.
The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to run any command:

**For post request,**

```
perl samplepost.pl http://lms-server:lms-port/rme/cwcli payload_XML_file
```

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

```
perl samplepost.pl https://lms-server:lms-port/rme/cwcli payload_XML_file
```

The default port for LMS server in HTTPS mode is 443.

The schema for creating the payload file in XML format is:

```
<payload>
<command>
cwcli inventory commandname -u user -p BAse64 encoded pwd -args1 arg1value...
</command>
</payload>
```

To invoke the servlet using a script, see the Overview: cwcli invreport Command.

The script and the payload file should be residing in the client machine.

**For get request,**

```
http://lms-server:lms-port/rme/cwcli?command=cwcli inventory commandname -u user -p BAse64 encoded pwd -args1 arg1value...
```

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

```
https://lms-server:lms-port/rme/cwcli?command=cwcli inventory commandname -u user -p BAse64 encoded pwd -args1 arg1value...
```

The default port for LMS server in HTTPS mode is 443.

The BAse64 encoded for “admin” is YWRtaW4=.

The URL encode for,

- Double quotes (") is %22
- Percentage sign (%) is %25

### Using the cwcli inventory Command

The command line syntax of the application is in the following format:

```
cwcli inventory command GlobalArguments AppSpecificArguments
```

The command line syntax of the application is in the following format:

```
cwcli export command GlobalArguments AppSpecificArguments
```

- `cwcli inventory` is the CiscoWorks command line interface for:
  - Checking the specified device credentials for the LMS devices.
  - Exporting device credentials of one or more LMS devices in clear text.
  - Deleting the specified LMS devices.
Viewing the LMS devices state.

- **Command** specifies which core operation is to be performed.
- **GlobalArguments** are the additional parameters required for each core command.
- **AppSpecificArguments** are the optional parameters, which modify the behavior of the specific `cwcli inventory` core command.

The order of the arguments and arguments are not important. However, you must enter the core command immediately after `cwcli inventory`.

The following sections describe:

- The `cwcli inventory` commands (See `cwcli inventory Commands`)
- The mandatory and optional arguments (See `cwcli inventory Global Arguments`)

On UNIX, you can view the `cwcli inventory` man pages by setting the MANPATH to `/opt/CSCOpx/man`. The man pages to launch the `cwcli inventory` are:

- `man cwinventory-cda` to launch the `cwcli inventory cda` command.
- `man cwinventory-delete` to launch the `cwcli inventory delete` command.
- `man cwinventory-export` to launch the `cwcli inventory export` command.
- `man cwinventory-state` to launch the `cwcli inventory getdevicestate` command

**cwcli inventory Commands**

The following table lists the command part of the `cwcli inventory` syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cwcli inventory cda</code></td>
<td>You can check the specified device credentials for the devices. See Running the <code>cwcli inventory cda Command</code></td>
</tr>
<tr>
<td><code>cwcli inventory crmexport</code></td>
<td>You can export device credentials of one or more devices in clear text. See Running the <code>cwcli inventory crmexport Command</code></td>
</tr>
<tr>
<td><code>cwcli inventory deletedevice</code></td>
<td>You can delete the specified devices. See Running the <code>cwcli inventory deletedevice Command</code></td>
</tr>
<tr>
<td><code>cwcli inventory getdevicestate</code></td>
<td>You can view the devices state. See Running the <code>cwcli inventory getdevicestate Command</code></td>
</tr>
</tbody>
</table>
cwcli inventory Global Arguments

The following describes the mandatory and optional global arguments for cwcli inventory:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u user</td>
<td>Enter a valid LMS username.</td>
<td>Mandatory.</td>
</tr>
<tr>
<td>-p password</td>
<td>Enter the password for the username.</td>
<td>Mandatory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can provide this as part of argument or you can enter the password when you get the password prompt. You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for more details.</td>
</tr>
<tr>
<td>{-device name</td>
<td>device name—Enter the Device Name of the device that you have added in the Device and Credentials database (Inventory &gt; Device Administration &gt; Add / Import / Manage Devices)</td>
<td></td>
</tr>
<tr>
<td>-view name}</td>
<td></td>
<td>Mandatory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You can enter multiple device list separated using a comma.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, if there are two devices with Device Names Rtr12 and Rtr13, using Rtr% will display both the devices.</td>
</tr>
<tr>
<td>{-device list</td>
<td>device list view name—Enter the Device Name and the Device Group name.</td>
<td></td>
</tr>
<tr>
<td>-view name}</td>
<td></td>
<td>Mandatory.</td>
</tr>
<tr>
<td>-ipaddress list</td>
<td>ipaddress list—Enter the device IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated.</td>
<td>Mandatory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You cannot use this option with -device, -view, or -input. Also, you cannot specify wildcard characters.</td>
</tr>
<tr>
<td>-d debug_level</td>
<td>Enter the debug level.</td>
<td>Optional.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>debug_level is a number between 1 (the least information is sent to the debug output) and 5 (the most information is sent to the debug output). If you do not specify this argument, 4(INFO) is the default debug level.</td>
</tr>
</tbody>
</table>
Running the cwcli inventory cda Command

You can use this command to check the following device credentials:

- SNMP Read Community String—SNMP version 2 read community string.
- SNMP Write Community String—SNMP version 2 write community string.
- SNMP Version 3—SNMP version 3 username and password.
- Telnet—Telnet username and password.
- Telnet Enable Mode User Name and Password—Telnet username and password in Enable mode.
- SSH—SSH username and password.
- SSH Enable Mode User Name and Password—SSH username and password in Enable mode.

You can update these credentials using Inventory > Device Administration > Add / Import / Manage Devices.

The command syntax for cwcli inventory cda is:

cwcli inventory cda -u userid -p password [-invoke | -status] [-credType credTypeList] [-device list | -device list -view name | -ipaddress list] [-d debuglevel] [-m email] [-help] [-l logfile]

Arguments in square brackets ([]) are optional; arguments in curly braces ({} ) are required. You must provide one argument from each group of arguments in curly braces ({} ) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used.

The following table describes the arguments that are specific to cwcli inventory cda command.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>[-m email]</td>
<td>Specify an e-mail address to send the results.</td>
<td>Optional. email is one or more e-mail addresses for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>notification. They can be separated by a space or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>comma.</td>
</tr>
<tr>
<td>[-l logfile]</td>
<td>Specify a file to which this command has to</td>
<td>Optional. Use the relative pathname to specify the</td>
</tr>
<tr>
<td></td>
<td>write log messages.</td>
<td>log_filename.</td>
</tr>
<tr>
<td></td>
<td>The default log filename is cli.log.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default log directory is:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>On Windows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NMSROOT\log</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Where NMSROOT is the LMS installed directory.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>On Solaris and Soft Appliance:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/var/adm/CSCOpx/log</td>
<td></td>
</tr>
<tr>
<td>-help</td>
<td>Displays command usage information</td>
<td>None.</td>
</tr>
</tbody>
</table>
### Argument: `[-invoke | -status]`
- **Invoke**—Invokes the Check Device Attribute operation.
- **Status**—Displays the check device attributes result.

**Usage Notes**
- Mandatory.
- These arguments are mutually exclusive. You cannot run `-invoke` and `-status` together.
- After using the `-invoke` argument to the check device attribute you must run the command again with `-status` argument to view the result.
- If you are checking the device credentials for same devices and for same set of credentials, then you can use `-invoke` argument only once.
- If you are checking the device credentials for different devices and different credentials then you must use `-invoke` argument first and then you must use `-status`.

### Argument: `[-credType credTypeList]`
- Enter the device credentials for which you want to view the status. You can use the following arguments to view the different credentials status:
  - 0 — Enter 0 to view all credentials status.
  - 1 — Enter 1 to view status for Read Community.
  - 2 — Enter 2 to view status for Write Community.
  - 3 — Enter 3 to view status for SNMP version 3 username and password.
  - 4 — Enter 4 to view status for Telnet username and password.
  - 5 — Enter 5 to view status for Telnet username and password in Enable mode.
  - 6 — Enter 6 to view status for SSH username and password.
  - 7 — Enter 7 to view status for SSH username and password in Enable mode.

**Usage Notes**
- Mandatory.
- If you do not specify the credentials type, all credentials status are displayed.

You can specify multiple arguments separated by comma to check multiple credentials.
## Argument Description Usage Notes

### Command Argument for Inventory CDA `createjob`

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[-device comma_separated_devicelist]</code></td>
<td>- Specify devices to be used for the job. The <code>comma_separated_devicelist</code> is list of devices.</td>
<td>Mandatory. These arguments are mutually exclusive. You cannot run <code>-device</code> and <code>-view</code> together.</td>
</tr>
<tr>
<td><code>[-view device_view_name]</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>[-schedule MM/dd/yyyy:HH:mm:ss]</code></td>
<td>You can specify the date and time as well as the frequency of the CDA job. You have to set both the <code>schedule</code> and <code>scheduletype</code> options for a scheduled job. You do not have to set the <code>schedule</code> and <code>scheduletype</code> for an Immediate job.</td>
<td>Optional. <code>scheduletype</code> can have any of the following values:</td>
</tr>
<tr>
<td>`[-scheduletype Once</td>
<td>Daily</td>
<td>Weekly</td>
</tr>
<tr>
<td><code>[-input argFile]</code></td>
<td>Input file containing the details of the subcommands to be used for a job creation.</td>
<td>Optional</td>
</tr>
<tr>
<td><code>[-description JobDescription]</code></td>
<td>Gives details of the job.</td>
<td><code>JobDescription</code> is a user-defined entry describing the job details.</td>
</tr>
<tr>
<td><code>[-notificationmail comma_separated_email_list]</code></td>
<td>Specify the e-mail addresses to which the configuration job will sends status notices.</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### Examples

```
cwcli inventory cda createjob -u Username -p Password -device Device 1, Device 2 -view device_view_name, -schedule Schedule -scheduletype Schedule Type
```

```
### CLI Utilities

#### Argument: `-credType credentialList`

Enter the device credentials for which you want to create a job. You can use the following arguments to view the different credentials status:

- 0 — Enter 0 to view all credentials status (ALL).
- 1 — Enter 1 to view status for Read Community.
- 2 — Enter 2 to view status for Write Community.
- 3 — Enter 3 to view status for SNMP version 3 username and password.
- 4 — Enter 4 to view status for Telnet username and password.
- 5 — Enter 5 to view status for Telnet username and password in Enable mode.
- 6 — Enter 6 to view status for SSH username and password.
- 7 — Enter 7 to view status for SSH username and password in Enable mode.

You can specify multiple arguments separated by comma to check multiple credentials.

**Usage Notes:** Mandatory

If you do not specify the credentials type, all credentials status are displayed.

#### Command Argument for Inventory CDA `stopjob`

`{-id Job ID}`

You can stop only one job at a time.

You can stop a CDA job that is in scheduled as well as running state.

**Usage Notes:** Mandatory

Use this command to stop an Inventory CDA job that is scheduled.

```
cwcli inventory cda stopjob -u userid -p password {-id jobID}
```

#### Command Argument for Inventory CDA `deletejob` and `jobdetails`

`{-id Job IDs}`

You can delete more than one job at a time.

Enter the Job IDs that you want to delete, separated by commas.

You can list the details of more than one job at a time. Enter the Job IDs separated by commas.

**Usage Notes:** Mandatory

Inventory CDA deletejob command:

```
cwcli inventory cda deletejob -u userid -p password {-id jobID1, jobID2..}
```

Inventory CDA jobdetails command:

```
cwcli inventory cda jobdetails -u userid -p password {-id jobID1, jobID2..}
```
The Table A-1 maps the device credentials that you have entered in the Device and Credentials (Inventory > Device Administration > Add / Import / Manage Devices) database and the credentials that appear in the cwcli inventory cda command:

### Table A-1 Credentials Mapping

<table>
<thead>
<tr>
<th>Credentials in Device and Credentials Database</th>
<th>Credentials displayed in cwcli inventory cda</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>deviceName</td>
</tr>
<tr>
<td>SNMP V2C RO Community String</td>
<td>ro</td>
</tr>
<tr>
<td>SNMP V2C RW Community String</td>
<td>rw</td>
</tr>
<tr>
<td>SNMP V3 Username and Password</td>
<td>snmpv3</td>
</tr>
<tr>
<td>Primary Credentials Username</td>
<td>telnet</td>
</tr>
<tr>
<td>Primary Credentials Username and Primary Enable Password</td>
<td>telnetEnable</td>
</tr>
<tr>
<td>Primary Credentials Username</td>
<td>ssh</td>
</tr>
<tr>
<td>Primary Credentials Username and Primary Enable Password</td>
<td>sshEnable</td>
</tr>
</tbody>
</table>
Table A-2 describes the Credential Verification Report Status messages:

### Table A-2 Understanding Credential Verification Report

<table>
<thead>
<tr>
<th>Status Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Check for device credentials completed. The device credentials data in the Device and Credential Repository matches the physical device credentials.</td>
</tr>
<tr>
<td>No authentication configured</td>
<td>Device was not configured with authentication mechanism (Telnet/LocalUsername/TACACS). LMS was able to use Telnet and log into the device successfully without using the values entered in the Device and Credential Repository.</td>
</tr>
<tr>
<td>Incorrect</td>
<td>Check for device credentials completed. The device credentials data in the Device and Credential Repository does not match with the physical device credentials for one of the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• The device credentials data in Device and Credential Repository is not correct.</td>
</tr>
<tr>
<td></td>
<td>• The device is unreachable or offline.</td>
</tr>
<tr>
<td></td>
<td>• One of the interfaces on the device is down.</td>
</tr>
<tr>
<td>No Data Yet</td>
<td>Check for device credentials is in progress.</td>
</tr>
<tr>
<td>Did Not Try</td>
<td>Check for device credentials is not performed for one of the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• A Telnet password does not exist, so could not login to the device.</td>
</tr>
<tr>
<td></td>
<td>• Device Telnet login mode failed, so enable mode login is not attempted.</td>
</tr>
<tr>
<td>No Value To Test</td>
<td>Check for device credentials is not performed because you have not entered the device credentials data.</td>
</tr>
<tr>
<td>Not Supported</td>
<td>Check for Telnet passwords is not performed because Telnet credential checking is not supported on this device.</td>
</tr>
<tr>
<td>Failed</td>
<td>Check failed because a Telnet session could not be established due to a not responding device.</td>
</tr>
<tr>
<td>Not Selected For Verification</td>
<td>Protocol was not selected for verification.</td>
</tr>
</tbody>
</table>

### Usage Examples for cwcli inventory cda Command

This section provides some examples of usage for the `cwcli inventory cda` command.

**Example 1: Invoking the Check Device Attributes**

```
cwcli inventory cda -u admin -p admin -invoke -device 3750-stack
```

The command output is:

```
CDA invoked for given device and credType list
SUMMARY
========

Successful: CDA: Success
```
Example 2: Checking the read and write device credentials for multiple devices

```
cwcli inventory cda -u admin -p admin -device 3750-stack, rtr% -credtype 1,2 -status
```

CDA Status:

```
deviceId | deviceName | ro | rw | snmpv3 | telnet | telnetEnable | ssh | sshEnable
---------|------------|----|----|--------|--------|-------------|-----|-------------
25       | rtr10005   | OK | OK |        |        |             |     |             
27       | 3750-stack | OK | OK |        |        |             |     |             
32       | rtr10K     | No Data Yet | No Data Yet |        |        |             |     |             
```

SUMMARY

```
Successful: CDA: Success
```

Example 3: Checking all device credentials for a group

```
cwcli inventory cda -u admin -p admin -view "/RME@ciscoworksservername/Pre-deployed" -status
```

CDA Status:

```
deviceId | deviceName | ro | rw | snmpv3 | telnet | telnetEnable | ssh | sshEnable
---------|------------|----|----|--------|--------|-------------|-----|-------------
29       | v2         | No Data Yet | No Data Yet | No Data Yet | No Data Yet | No Data Yet |     | No Data Yet 
```

SUMMARY

```
Successful: CDA: Success
```

Example 4: Checking device credentials for a device using the cwcli get request

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

Enter this in your browser:

```
http://ciscowork_servername:1741/rme/cwcli?command=cwcli inventory cda -u admin -p YWRtaW4= -device 10.10.10.12 -status
```

The output for this appears on your console:

```
<!-- Processing Starts -->
CDA Status:

```
deviceId | deviceName | ro | rw | snmpv3 | telnet | telnetEnable | ssh | sshEnable
---------|------------|----|----|--------|--------|-------------|-----|-------------
12       | 10.10.10.12 | OK | OK | No Value To Test | Incorrect | Did Not Try | Failed | Did Not Try 
```

SUMMARY

```
Successful: CDA: Success
```

```
<!-- Processing complete -->
```
Example 5: Checking device credentials for a device using the cwcli post request

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

The payload file, cda.xml contains:

```xml
<payload>
  <command>
    cwcli inventory cda -u admin -p YWRtaW4= -device 10.10.16.20 -status
  </command>
</payload>
```

At the command prompt enter:

```bash
perl samplepost.pl http://ciscowork_servername:1741/rme/cwcli cda.xml
```

To invoke the servlet using a script, see the Overview: cwcli invreport Command.

```bash
<!-- Processing Starts -->
CDA Status :
============
deviceId | deviceName | ro | rw | snmpv3 | telnet | telnetEnable | ssh | sshEnable
---------|------------|----|----|--------|--------|--------------|----|------
71 | 10.10.16.20 | No Data Yet | No Data Yet | No Data Yet | No Data Yet | No Data Yet | No Data Yet

SUMMARY
========
Successful: CDA: Success
<!-- Processing complete -->
```

Example 6: Creating a job using cwcli inventory cda createjob command

```bash
cwcli inventory cda createjob -u admin -p admin - Cat6230, Cat4500 | -view myview -schedule 03/23/2007:12:15:01 -scheduletype Once
```

This command creates a cda job for the devices Cat6230 and Cat4500 in the view myview and scheduled for 23rd march 2007 at 12:15 pm with schedule type specified as Once.

Example 7: Stopping a cwcli inventory cda job using stopjob command

There is a job 1098, which is currently running. You can use this command to stop the job 1098.

```bash
cwcli inventory cda stopjob -u admin -p admin -id 1098
```

Example 8: Deleting cwcli inventory cda jobs using deletejob command

There are two jobs 1057 and 1058 scheduled. You can use this command to stop the two jobs.

```bash
cwcli inventory cda deletejob -u admin -p admin -id 1057,1058
```

Example 9: Getting details of jobs using cwcli inventory cda jobdetails command

There are two jobs 1001 and 1002 that are scheduled. You can use this command to list the details of both the jobs:

```bash
cwcli inventory cda jobdetails -u admin -p admin -id 1001, 1002
```
Example 10: Listing the cda jobs based on the status using the listjobs command

cwcli inventory cda listjobs -u admin -p admin -jobstatus R, C
Use this command to list those jobs whose status is Running or Completed.

Example 11: Obtaining results of jobs using jobresults command

There are two jobs 1023 and 1024 that are completed. You can use this command to save the results of these jobs to the specified location.

cwcli inventory cda jobresult -u admin -p admin -jobid 1023, 1024 -csvoutput C:/jobs/results

Running the cwcli inventory crmexport Command

You can use this command to export device credentials in CSV or XML format.

The command syntax for cwcli inventory crmexport is:


Arguments in square brackets ([ ]) are optional; arguments in curly braces ( { }) are required. You must provide one argument from each group of arguments in curly braces ( { }) that is separated by vertical bars ( | ).

If you do not specify an optional argument, the default value configured for the system is used.

The following table describes the arguments that are specific to cwcli inventory crmexport command. The other common arguments used by cwcli export are explained in Using the cwcli inventory Command.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>{-filetype format }</td>
<td>-filetype format — Enter the file format to export, either XML or CSV.</td>
<td>Mandatory. The default CSV file format version is 3.0.</td>
</tr>
<tr>
<td>{ -filename outputfile }</td>
<td>-filename outputfile— Enter the filename.</td>
<td>Mandatory. Specifies the name of the file to which the device credentials information is to be exported on LMS server. If you are using cwcli remotely (get or post request), by default the output file is available at this location on LMS server: On Windows: NMSROOT\MDC\tomcat Where, NMSROOT is the LMS installed directory. On Solaris and Soft Appliance: NMSROOT/objects/dmgt</td>
</tr>
</tbody>
</table>

Usage Examples for cwcli inventory crmexport Command

This section provides some examples of usage for the cwcli inventory crmexport command.
Example 1: Exporting device credentials of all devices in XML format

cwcli inventory crmexport -device % -filetype xml -filename crmexport-xml -u admin -p admin

SUMMARY
====== Successful: Export: Success

The device credentials are exported into a file, crmexport-xml in XML format. The credentials that are exported depends on the data that you have provided when you added the devices to Device Credentials Repository.

Example 2: Exporting device credentials of all devices in Normal State in CSV format

cwcli inventory crmexport -view "/RME@ciscoworksservername/Normal Devices" -filetype csv
-filetype csv -filename crmexport-csv -u admin -p admin

SUMMARY
====== Successful: Export: Success

The device credentials for devices that are in Normal state are exported into a file, crmexport-csv in CSV version 3.0 format. The credentials that are exported depends on the data that you have provided when you added the devices to Device Credentials Repository.

Example 3: Exporting device credentials of all devices using cwcli get request method

The password that you enter here must be in base64 encoded.

In this example,
- YWRtaW4= is the base64 encoded password for admin.
- %25 is the URL encode for “%”

Enter this in your browser:
http://ciscowork_servername:1741/rme/cwcli?command=cwcli inventory crmexport -u admin -p YWRtaW4= -device %25 -filetype xml
-filetype xml -filename getxml

The output is written in the getxml file. The getxml file is located:

On Windows:
NMSROOT\MDC\tomcat
Where, NMSROOT is the LMS installed directory.
On Solaris and Soft Appliance:
NMSROOT/objects/dmgt

Example 4: Exporting device credentials of all devices using cwcli post request method

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

The payload file, crmexport.xml contains:

```
<payload>
  <command>
    cwcli inventory crmexport -u admin -p YWRtaW4= -device 10.66.162.208 -filetype xml
    -filename /opt/CSCOpx/crmexport-xml
  </command>
</payload>
```
At the command prompt enter:

```
perl samplepost.pl http://ciscowork_servername:1741/rme/cwcli crmexport.xml
```

To invoke the servlet using a script, see the Overview: cwcli invreport Command.

**SUMMARY**

```
Successful: Export: Success
```

The device credentials are exported into a file, `crmexport-xml` in XML format. This file is created in the `/opt/CSCOpx` directory. By default, the specified file is created in this location:

On Windows:

```
NMSROOT\MDC\tomcat
```

Where, `NMSROOT` is the LMS installed directory.

On Solaris and Soft Appliance:

```
NMSROOT/objects/dmgt
```

The credentials that are exported depends on the data that you have provided when you added the devices to Device Credentials Repository.

### Running the cwcli inventory deletedevice Command

You can use this command to delete devices.

The device information will be retained in the Device Credentials Repository. This information will not be removed till you delete the device from Device Credentials Repository.

The command syntax for `cwcli inventory deletedevice` is:

```
cwcli inventory deletedevice -u userid -p password [-d debuglevel] [-m email] [-l logfile] [-view name] { -device list | -input inputfile | ipaddress list }
```

Arguments in square brackets ([ ]) are optional; arguments in curly braces ({ }) are required. You must provide one argument from each group of arguments in curly braces ({ }) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used.

The following table describes the arguments that are specific to `cwcli inventory deletedevice` command. The other common arguments used by `cwcli export` are explained in Using the cwcli export Command.
This section provides some examples of usage for the `cwcli inventory deletedevice` command.

**Example 1: To delete a device**

```
cwcli inventory deletedevice -u admin -p admin -device 10.76.10.10
```

```
<cwcli> INFO - Total number of devices deleted successfully: 1
SUMMARY
=======
Successful: Delete Device: Success
```

**Example 2: To delete devices listed in a file**

The input file, `deletedevice` contains list of device Device Name separated by a comma:

```
-device 3750-stack,rtr1000,rtr10005
```

```
cwcli inventory deletedevice -u admin -p admin -input deletedevice.csv
```

**Example 3: To delete devices using cwcli get request**

The password that you enter here must be in base64 encoded. In this example, `YWRtaW4=` is the base64 encoded password for admin.

Enter the following in your browser:

```
http://ciscowork_servername:1741/rme/cwcli?command=cwcli inventory deletedevice -u admin -p YWRtaW4= -device 10.10.10.41,10.10.10.51
```

The output for this appears on your console:

```
<!-- Processing Starts  -->
<cwcli> INFO - Total number of devices deleted successfully: 2
SUMMARY
=======
Successful: Delete Device: Success
<!-- Processing complete -->
```
Example 4: To delete devices using cwcli post request

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

The payload file, deletedevicestate.xml contains:

```xml
<payload>
  <command>
    cwcli inventory deletedevice -u admin -p YWRtaW4= -device 10.77.9.10,10.77.9.18,10.76.8.6
  </command>
</payload>
```

At the command prompt enter:

```perl
perl samplepost.pl http://doclab2:1741/rme/cwcli deletedevice.xml
```

To invoke the servlet using a script, see the Overview: cwcli invreport Command.

<!-- Processing Starts  -->
```cwcli
INFO - Total number of devices deleted successfully: 3
SUMMARY
========
Successful: Delete Device: Success
<!-- Processing complete -->
```

Running the cwcli inventory getdevicestate Command

You can use this command to view the device state. The command syntax for cwcli inventory getdevicestate is:

```
cwcli inventory getdevicestate -u userid -p password [-a debuglevel] [-m email] [-l logfile] [-v view name] [-d device list | -i inputfile | -ip ipaddress list]
```

Arguments in square brackets ([]) are optional; arguments in curly braces ({}) are required. You must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used.

The following table describes the arguments that are specific to cwcli inventory getdevicestate command. The other common arguments used by cwcli export are explained in Using the cwcli inventory Command.
Usage Examples for cwcli inventory getdevicestate Command

This section provides some examples of usage for the cwcli inventory getdevicestate command.

Example 1: To view the device state of the devices

cwcli inventory getdevicestate -u admin -p admin -device 10.10.19.10,10.10.19.12

Example 2: To view the devices state specified in a file

The input file, deletedevice contains list of device name separated by a comma:

-device VG200,rtr1750,cat4000

cwcli inventory deletedevice -u admin -p admin -input devicestate.csv

Example 3: To view the devices state using get request

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

Enter the following in your browser:

http://ciscowork_servername:1741/rme/cwcli?command=cwcli inventory getdevicestate -u admin -p YWRtaW4= -device 10.16.10.15,10.16.10.35

The output for this appears on your console:

<!-- Processing Starts -->
<cwcli> INFO - Device State Information
DisplayName:Device State
10.16.10.15:PREDEPLOYED
10.16.10.35:NORMAL

--------
Successful: getdevicestate: Success

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>-input inputfile</td>
<td>-input inputfile—Enter the full path of the file containing comma-separated list of devices name as entered in Device Credentials Repository. The input file should be of this format: -device 1.1.1.1.1,2.2.2.2,3.3.3.3 or -device 1.1.1.1 -device 2.2.2.2 -device 3.3.3.3</td>
<td>Mandatory You must also enter the file format either CSV or txt.</td>
</tr>
</tbody>
</table>

Argument Description Usage Notes

-argument

-argument

-argument

-argument

-argument
SUMMARY
========
Successful: getdevicestate: Success
<!-- Processing complete -->

Example 4: To view the device state using post request

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

The payload file, getdevicestate.xml contains:

```
<payload>
<command>
  cwcli inventory getdevicestate -u admin -p YWRtaW4= -device
  12.20.12.26,10.6.12.21,12.18.10.129,10.7.9.13
</command>
</payload>
```

At the command prompt enter:

```
perl samplepost.pl http://ciscowork_servername:1741/rme/cwcli getdevicestate.xml
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

```
<!!- Processing Starts -->
<cwcli> INFO - Device State Information
DisplayName:Device State
12.18.13.129:ALIAS
10.7.9.13:PREDEPLOYED
10.6.12.21:NORMAL
12.20.12.26:NORMAL

SUMMARY
========
Successful: getdevicestate: Success
<!-- Processing complete -->
```

Overview: cwcli invreport Command

The cwcli invreport is a CiscoWorks command line tool which allows you to run previously created Inventory Custom Reports and also system reports. The supported output file format is Comma Separated Value (CSV).

The above command retrieves the inventory report in CSV format. The -file parameter stores the output in the file specified by filename. If you have not specified the filename, the output is stored at the following location:

- NMSROOT\files\rme\cri\archives\inventory\reportname_timestamp.csv (On Windows)
• `/var/adm/CSCOpx/files/rme/cri/archives/inventory/reportname_timestamp.csv` (On Solaris and Soft Appliance)

`NMSROOT` is the LMS install directory.

You can:
• Use the `-reportname` argument to generate the report.
  This can be the name of:
  – An already defined custom template
  or
  – A system report name such as Detailed Device Report.
• Use the `-input` argument to specify a file containing the parameters for the report generation.

Note: The `-view` argument is not allowed in the input file.

• Enable debug mode and set the debug level using the `-d` argument.
• E-mail the output to an e-mail recipient using the `-m` argument.
• Log the error messages to a file using the `-l` argument. The log and the output files are created in the current directory.
• List the existing reports with the `-listreports` argument.

Running the `cwcli invreport` Command

To use the `cwcli invreport` command, you must be able to run the cwcli command

You should be authorized to generate inventory reports.

The command syntax is:

```
cwcli invreport -u userid -p password [-d debuglevel] [-m email] [-l logfile] {-listreports | -reportname name { -view viewname | -device list | -ipaddress list} [-file filename] | -input inputfile}
```

Arguments in square brackets ([ ]) are optional; arguments in curly braces ( { }) are required. You must provide one argument from each group of arguments in curly braces ( { }) that is separated by vertical bars ( | ).

If you do not specify an optional argument, the default value configured for the system is used. Valid values for arguments are described in the following table:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-u user</code></td>
<td>Provide valid LMS username.</td>
<td>None.</td>
</tr>
<tr>
<td><code>-p password</code></td>
<td>Provide password for username.</td>
<td>None.</td>
</tr>
<tr>
<td></td>
<td>You can also specify the password in a file. See <code>Setting CWCLIFILE Environment Variable</code> for more details.</td>
<td></td>
</tr>
</tbody>
</table>
### Contribution Management with Cisco Prime LAN Management Solution 4.2

#### Appendix A

**CLI Utilities**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>[-a debug_level ]</td>
<td>Set debug level.</td>
<td>Optional.</td>
</tr>
<tr>
<td></td>
<td>debug_level is a number between 1 (the least</td>
<td></td>
</tr>
<tr>
<td></td>
<td>information is sent to the debug output) and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5 (the most information is sent to the debug</td>
<td></td>
</tr>
<tr>
<td></td>
<td>output). If you do not specify this argument,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4(INFO) is the default debug level.</td>
<td></td>
</tr>
<tr>
<td>[-m email]</td>
<td>Specify an e-mail address to send the results.</td>
<td>Optional.</td>
</tr>
<tr>
<td></td>
<td>email is one or more e-mail addresses for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>notification. They can be separated by a space</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or comma.</td>
<td></td>
</tr>
<tr>
<td>[-l log_filename ]</td>
<td>Logs the error messages and debug of messages of the invreport command, to the specified logfile name. If not specified, it will be written to default logs (invreports.log and cli.log).</td>
<td>Optional.</td>
</tr>
<tr>
<td></td>
<td>log_filename can be full pathname or filename in local directory.</td>
<td></td>
</tr>
<tr>
<td>[-l log_filename ]</td>
<td>Logs the error messages and debug of messages of the invreport command, to the specified logfile name. If not specified, it will be written to default logs (invreports.log and cli.log).</td>
<td>Optional.</td>
</tr>
<tr>
<td></td>
<td>log_filename can be full pathname or filename in local directory.</td>
<td></td>
</tr>
</tbody>
</table>
```
{-listreports | -reportname name | -view viewname | -device list | -ipaddress list | -file filename | -input inputfile}
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>
| {-listreports | -reportname name | -view viewname | -device list | -ipaddress list | -file filename | -input inputfile} | Specify any one of the required arguments: | -listreports argument lists out all Inventory system reports and custom reports templates. You can run this command if you have the required permissions to generate reports.  
- reportname name specifies the name of an already defined custom template or the name of a system report (such as Detailed Device Report) for which the CSV formatted report is to be generated.  
- input inputfile specifies the input file containing report parameters. The parameters in this file will be used to generate the CSV formatted report(s).  
For Solaris and Soft Appliance, you must specify the complete path of the input file.  
For Windows, this file should be located in the current directory or you can specify the complete path of the input file.  
The -view argument is not allowed in the input file. |
### Usage Examples

This section provides some examples of usage for the cwcli invreport command:

- **Example 1**
- **Example 2**
- **Example 3**
- **Example 4**
- **Example 5**
- **Example 6**

**Example 1**

```bash
    cwcli invreport -u admin -p admin -reportname "Detailed Device Report" -device %
```

This generates Detailed Device Report for all devices and CSV file will be located at:

- **NMSROOT\files\rme\cri\archives\inventory\Detailed Device Report_timestamp.csv** (On Windows)
- **/var/adm/CSCOpx/files/rme/cri/archives/inventory/Detailed Device Report_timestamp.csv** (On Solaris and Soft Appliance)

Optionally, you can also specify `-file filename`. Name of the file where CSV formatted report will be stored.

If you do not specify the location, the default location is:

- **NMSROOT\files\rme\cri\archives\inventory\reportname_timestamp.csv** (On Windows)
- **/var/adm/CSCOpx/files/rme/cri/archives/inventory/reportname_timestamp.csv** (On Solaris and Soft Appliance)

You cannot use this option with `-device`, `-view`, or `-input`. Also, you cannot specify wildcard characters.

### Usage Examples

- **Example 1**
- **Example 2**
- **Example 3**
- **Example 4**
- **Example 5**
- **Example 6**

**Example 1**

```bash
    cwcli invreport -u admin -p admin -reportname "Detailed Device Report" -device %
```

This generates Detailed Device Report for all devices and CSV file will be located at:

- **NMSROOT\files\rme\cri\archives\inventory\Detailed Device Report_timestamp.csv** (On Windows)
- **/var/adm/CSCOpx/files/rme/cri/archives/inventory/Detailed Device Report_timestamp.csv** (On Solaris and Soft Appliance)
Example 2

cwcli invreport -u admin -p admin -reportname "Detailed Device Report" -device % -file D:\cisco\CSCOpx\a.csv

This generates Detailed Device Report, a system report, for all devices, and the result will be written to D:\cisco\CSCOpx\a.csv

Example 3

cwcli invreport -u admin -p admin -reportname "Detailed Device Report" -device % -file a.csv

This generates the Detailed Device Report, a system report, for all devices, and the result will be written to the file a.csv in the current directory (from where you are running this command).

Example 4

cwcli invreport -u admin -p admin -input cliinputs.txt

Generate the reports using the parameters provided in the file cliinputs.txt. Using -input argument you can run multiple reports at a time by providing parameters in the file.

Example 5

cwcli invreport -u admin -p admin -listreports

Displays a list of all Inventory system report and custom templates.

You can run this command if you have the required permissions to generate reports.

Example 6

cwcli invcreport -u admin -p admin -d 3 -m xxx@yyy.com -reportname acmeinventory -view acme -file acmeinventory.txt

Generates the report named acmeinventory, using the acme device view and the CSV formatted output will be written to acmeinventory.txt

You can place this file in the current directory (from where you are running the command).

Example 7

cwcli invreport -u admin -p admin -reportname HardwareStatisticsReport -device devname -file hwstreport.txt

Generates the Hardware Statistics Report for the device devname and the CSV formatted output will be written to hwstreport.txt

Example 8

cwcli invreport -u admin -p admin -reportname DeviceStatisticsReport -device devname -file devstreport.txt

Generates the Device Statistics Report for the device devname and the CSV formatted output will be written to devstreport.txt

Example 9

cwcli invreport -u admin -p admin -reportname POEReport -device devname -file report.txt

Generates the POE Report for the device devname and the CSV formatted output will be written to report.txt
cwcli invreport Remote Access

You can also perform the `cwcli invreport` tasks using the servlet. You will have to upload a payload XML file, which contains the `cwcli invreport` command arguments and LMS user credentials.

You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the output either on the console or in the specified output file, if the credentials are correct and arguments are valid.

The name of the servlet is `/rme/cwcli`.

The following is the servlet to be invoked to execute any command:

**For post request,**

```
perl samplepost.pl http://lms-server:lms-port/rme/cwcli payload_XML_file
```

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

```
perl samplepost.pl https://lms-server:lms-port/rme/cwcli payload_XML_file
```

The default port for LMS server in HTTPS mode is 443.

The schema for creating the payload file in XML format is:

```
<payload>
  <command>
    cwcli inventory commandname -u user -p BAsed64 encoded pwd -arg1 arg1value...
  </command>
</payload>
```

To invoke the servlet using a script, see the Overview: `cwcli invreport Command`.

The script and the payload file should be residing in the client machine.
For get request,

\[http://lms-server:rmeport/rme/cwcli?command=cwcli\ invreport\ commandname\ -u\ user\ -p\ Base64\ encoded\ pwd\ -args1\ arg1value...\]

The default port for LMS server in HTTP mode is 1741. 

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

\[https://lms-server:lmsport/rme/cwcli?command=cwcli\ invreport\ commandname\ -u\ user\ -p\ Base64\ encoded\ pwd\ -args1\ arg1value...\]

The default port for LMS server in HTTPS mode is 443.

The Base64 encoded for “admin” is YWRtaW4=.

The URL encode for,

- Double quotes (“”) is %22
- Percentage sign (%) is %25

**Overview: cwcli netshow Command**

You can invoke NetShow features from Command Line Interface (CLI).

The `cwcli netshow` commands let you use NetShow features from the command line. You can use the `cwcli netshow` commands to view, browse, create, delete, and cancel NetShow jobs.

You can also view the Command Sets assigned to each user by entering the command `listcmdsets` from CLI.

You can set the following job attributes using the command line option:

- E-mail Notification
- Job Based Password
- Execution Policy
- Approver List

However, the Administrator must define and assign the command sets to you, in the browser interface.

If you do not have permission to run custom commands, you can run a command or command set from the CLI only if:

- The command set is assigned to you by the Administrator.
- The command set has at least one command that can be run on the specified device.

If you have permission to run custom commands, you can run any of the following adhoc commands:

- `show`
- `version`
- `where`
- `ping`
- `traceroute`
- `?`

Administrator level users have all command sets assigned to them. However, only system-defined command sets are assigned to all users, by default. Other commands have to be assigned to the user by the Administrator. If any users create a command, it is automatically assigned to them.
Running cwcli netshow Command

The command syntax for running `cwcli netshow` commands is:

```
cwcli netshow common_arguments subcommands command_arguments
```

In the CLI version, you can provide the arguments in the (operating system shell) command line or in an input file. The input file provides you with flexibility and control over commands and command sets. You can specify the devices on which you want to run the command sets.

In the input file, you can include subcommands and command arguments.

For example, you can create a new netshow job with command sets, set1 and set2, and the custom commands, custom command 1 and custom command 2, by entering:

```
cwcli netshow createjob -u Username -p Password -commandset “Command Set 1”, “Command Set 2” -device Device 1, Device 2 -customcmd “Custom command 1”, “Custom command 2” -schedule Schedule -scheduletype Schedule Type
```

Items in square brackets ([ ]) are optional; items in curly brackets ({ }) are required.

The arguments are described in the following sections.

Subcommands

Subcommands specify the actions that you perform. Valid values for subcommands are described in the following table.

<table>
<thead>
<tr>
<th>Sub Command</th>
<th>Description</th>
<th>Usage Notes</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>createjob</td>
<td>Creates a new job that can be scheduled to run immediately or to be run sometime in the future. You can also specify the job attributes you want to enable.</td>
<td>Either use an input file containing the details of the subcommands or enter the full command syntax.</td>
<td><code>cwcli netshow createjob -u Username -p Password -commandset “Command Set 1”, “Command Set 2” -device Device 1, Device 2 -customcmd “Custom command 1”, “Custom command 2” -schedule Schedule -scheduletype Schedule Type</code> Or <code>cwcli netshow createjob -u Username -p Password -input Input File</code></td>
</tr>
<tr>
<td>canceljob</td>
<td>Cancels an existing job.</td>
<td>Enter the job ID.</td>
<td><code>cwcli netshow canceljob -u Username -p Password -id “Job ID”</code></td>
</tr>
<tr>
<td>deletejob</td>
<td>Deletes existing jobs.</td>
<td>Enter the job IDs separated by commas.</td>
<td><code>cwcli netshow deletejob -u Username -p Password -id “Job ID 1”, “Job ID 2”</code></td>
</tr>
<tr>
<td>jobdetails</td>
<td>Displays details of specified job.</td>
<td>Enter the job IDs separated by commas.</td>
<td><code>cwcli netshow jobdetails -u Username -p Password -id “Job ID 1”, “Job ID 2”, “Job ID 3”</code></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Usage Notes</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>listjobs</td>
<td>Displays a list of jobs created by the user and the job status.</td>
<td>Specify the type of jobs to be listed. The command type is case sensitive.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The commands that you can use are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>A — All jobs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>R — Running jobs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C — Completed jobs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>P — Pending jobs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can use combinations of status options. Separate the options by commas.</td>
<td></td>
</tr>
<tr>
<td>listcmdsets</td>
<td>Displays a list of command sets assigned to the user.</td>
<td>None.</td>
<td></td>
</tr>
<tr>
<td>jobresults</td>
<td>Displays results of specified jobs</td>
<td>Specify the job IDs. Separate the job IDs by commas.</td>
<td></td>
</tr>
<tr>
<td>help</td>
<td>Displays command usage information.</td>
<td>None.</td>
<td></td>
</tr>
</tbody>
</table>

Common Arguments

Common arguments specify parameters that apply to all subcommands. Valid values for `common_arguments` are described in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u user</td>
<td>Enter a valid LMS username.</td>
<td>None</td>
</tr>
<tr>
<td>-p password</td>
<td>Enter the password for the username.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>You can also specify the password in a file. See Setting CWCLIFILE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Environment Variable for more details.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[-d debug_level] Set the debug level.</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>debug_level should be a number between 1-5.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 — The least information is sent to the debug output</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 — The most information is sent to the debug output.</td>
</tr>
<tr>
<td></td>
<td>[-1 log_filename] Identifies a file to which Network Show Commands will</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>write log messages.</td>
<td>log_filename can be a full path to the file or a filename in the local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>directory.</td>
</tr>
<tr>
<td></td>
<td>[-m Email ID] Enter your Email ID</td>
<td>You will get the output of the CLI operation in an Email.</td>
</tr>
</tbody>
</table>
Command Arguments

Command arguments specify parameters that apply only to specific subcommands. Valid values for command arguments are described in the following table.

Arguments in square brackets ([ ]) are optional. Arguments in curly brackets ( { }) are required. You must provide one argument from each group of arguments in curly brackets ( { }) that is separated by vertical bars ( | ).

<table>
<thead>
<tr>
<th>Command Arguments</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command Arguments for createjob</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>{-device devicelist</td>
<td>-view view_name}</td>
<td>Defines devices on which you want the command set to run.</td>
</tr>
<tr>
<td>{ -commandset commandset}</td>
<td>Defines available command sets that you want to run on the selected devices.</td>
<td>commandset is the name of the command set that was assigned to you. You can specify more than one command set separated by commas. The command set name is case sensitive. You must specify command set or custom command or both to create a job.</td>
</tr>
<tr>
<td>{-customcmd customcommand}</td>
<td>Defines the user-defined commands that you want to run on the selected devices.</td>
<td>customcommand is a user-defined show command. You must specify command set or custom command or both to create a job. The custom commands which can be run on NetShow are: • show • version • where • ping • traceroute • ? You can use the short forms of these commands. For example, sh for show.</td>
</tr>
<tr>
<td>{-description description}</td>
<td>Gives details of the job.</td>
<td>description is a user-defined entry describing the job details.</td>
</tr>
</tbody>
</table>
### CWCLI

#### CLI Utilities

**Command Arguments**

```
[-schedule MM/dd/yyyy:HH:mm:ss
-scheduletype Once | Daily | Weekly | Monthly | LastDayOfMonth | 6hourly | 12hourly]]
```

You can specify the date and time as well as the frequency of the NetShow job.
- To specify the date and time when you want to run the NetShow job, use the schedule option.
- To specify the frequency of the job use the scheduletype option.

You have to set both the schedule and schedule type options for a scheduled job.

You do not have to set the schedule and schedule type for an Immediate job.

**Usage Notes**

`scheduletype` can have any of the following values:
- Once
- 6hourly
- 12hourly
- Daily
- Weekly
- Monthly
- LastDayOfMonth

If the schedule option is not specified, the job will be created as an immediate job.

```
[-makercomments comments]  Job creator's comments to Job approver.
[-mkemail email]            Maker e-mail ID for sending approval notifications
[-notificationmail email]   Defines the e-mail addresses of persons who need to get mails when the job has started and completed.
[-execution Sequential|Parallel]  Execution policy. Specifies the order in which you want to run the job on the devices.
                                 Parallel—Allows the job to run on multiple devices at the same time.
                                 By default, the job runs on five devices at a time.
                                 Sequential—Allows the job to run on only one device at a time.
```

**Usage Notes**

If you do not specify these options in the CLI, the corresponding settings from the UI are used.

```
[-primary_user username
-primary_pass password]      Primary username and password to connect to devices.
[-enable_pass password]      Execution mode password to connect to device.
[-input input file]         Input file containing the details of the subcommands
```

**Usage Notes**

If you do not specifying the input file, you do not need to specify the subcommands.
## Executing Netshow CLI Remotely

You can run NetShow CLI from a remote console.

NetShow uses the Remote Access feature in the CLI framework to help you to invoke the NetShow commands from the client in the same way as you run them on the LMS server.

The name of the servlet, to be invoked, is /rme/cwcli.

You must invoke the following URLs to run any command.

- For POST request:
  
  `http://lms-server:lms-port/rme/cwcli payload XML file`

- For GET request:


### Command Arguments

<table>
<thead>
<tr>
<th>Command Arguments</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>
| **Command Argument for listjob** | ![Listjob Argument](image) | This can be:  
- All jobs  
- Running jobs  
- Completed jobs  
- Pending jobs. |
| **Command Argument for canceljob** | ![Canceljob Argument](image) | You can cancel only one job at a time. |
| **Command Argument for deletejob and jobdetails** | ![Deletejob Argument](image) | You can delete more than one job at a time. Enter the Job IDs that you want to delete, separated by commas. You can list the details of more than one job at a time. Enter the Job IDs separated by commas. |
| **Command Arguments for jobresults** | ![Jobresults Argument](image) | You can list the results of more than one job at a time. Enter the job IDs separated by commas. If you do not specify this argument, the job results appear in the console itself. If the specified path does not exist, the job results are stored in the default location. |

**Command Argument for listjob**

```bash
{-status status}
```

You can specify the status of the job. This can be:
- All jobs
- Running jobs
- Completed jobs
- Pending jobs.

**Command Argument for canceljob**

```bash
{-id Job ID}
```

You can cancel only one job at a time.

**Command Argument for deletejob and jobdetails**

```bash
{-id Job ID, Job ID}
```

You can delete more than one job at a time. Enter the Job IDs that you want to delete, separated by commas. You can list the details of more than one job at a time. Enter the Job IDs separated by commas.

**Command Arguments for jobresults**

```bash
{-id Job ID, Job ID}
```

You can list the results of more than one job at a time. Enter the job IDs separated by commas.

```bash
{-output file path}
```

You can specify the fully qualified pathname for saving the job results.
The contents of the payload.xml is:

```xml
<payload>
  <command>
    cwcli netshow command -u Username -p Password command_specific_args
  </command>
</payload>
```

For example to run the `listcmdsets` command payload.xml will be as follows:

```xml
<payload>
  <command>
    cwcli netshow listcmdsets -u Username -p Password
  </command>
</payload>
```

To invoke the servlet using a script, see the Overview: cwcli invreport Command.

The script and the payload file should be residing in the client machine.

---

**Performance Tuning Tool**

Performance Tuning Tool (PTT) is a Command Line Interface (CLI) utility that enables you to apply and list various profiles available in LMS server. Profiles consists of configuration files, which are in the form of XML files whose values are based on the recommendations for various applications. For more information on PTT features, refer to PTT Features.

There are two profiles shipped with LMS. You can use any of the profile that matches the system. For more information on PTT Profiles, see Profiles and PTT.

There maybe multiple configuration files that are involved while applying a profile. The parameters such as, snmp.threads.min, snmp.threads.max, ICSThreadCount, ICS DBConnectionCount, ThreadPoolCount, CDLNumOfThreads, max_db_connections, max_threads_for_config_fetch, EssentialsDMServicesHeapsize, ConfigJobManager.heapsize, and CDA_MIN_THREADS are tuned and available in each profile. You can apply the required profile to the system and improve performance. This is a major advantage of using PTT.

To know more about the command usage, see PTT Commands.

---

**PTT Features**

The PTT CLI utility allows you to:

- List the profile that is currently applied to the target machine.
- List the profiles that match the system configuration.
- List the profiles that match the operating system.
- Apply a selected profile onto the target machine.
- Reverse the changes done to a target machine by applying the default profile to restore the default settings.
- View details of a profile.
PTT Commands

Table A-3 lists the various PTT command options that you can use. These command options are common for Windows and Solaris and Soft Appliance.

Table A-3  PTT Command Options

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-apply &lt;profileName&gt;</td>
<td>Applies a particular profile.</td>
</tr>
<tr>
<td></td>
<td>To reset, specify the default profile name as parameter and apply that profile.</td>
</tr>
<tr>
<td>-apply</td>
<td>Finds the matching profile and applies it automatically in a single step.</td>
</tr>
<tr>
<td>-apply Default</td>
<td>Finds the default profile and applies it automatically in a single step.</td>
</tr>
<tr>
<td>-show</td>
<td>Displays the currently applied profile.</td>
</tr>
<tr>
<td>-list</td>
<td>Lists all the profiles that match the target operating system.</td>
</tr>
<tr>
<td>-list Match</td>
<td>Lists the profile that matches the system configuration.</td>
</tr>
<tr>
<td>-view &lt;profileName&gt;</td>
<td>Displays the profile details.</td>
</tr>
<tr>
<td></td>
<td>The details of the profile, which is specified in the command is displayed.</td>
</tr>
<tr>
<td>rmeptt -help</td>
<td>Displays help for all commands.</td>
</tr>
</tbody>
</table>

Command Usage

In Windows enter:

```
rmeptt.bat <option> <argument>
```

For example, to list all the profiles that matches the target operating system, the command is:

```
rmeptt.bat -list
```

In Solaris and Soft Appliance, enter:

```
rmeptt.sh <option> <argument>
```

For example to display the profile details, the command is:

```
rmeptt.sh -view x
```

Where x is the name of the profile.

Profiles and PTT

Profiles are XML files whose values are based on the recommendations of the various LMS applications. Each profile (XML file) consists of tuned parameters which when applied, improves performance.

There are two profiles that are shipped with LMS. They are:

- Default Profile
- Perftune - Windows and Perftune - Solaris and Soft Appliance

Note  All the configuration files are backed up before applying a profile.

PTT identifies the matching profile for a LMS server based on the following criteria:
• The operating system for which the profile is created.
• The System Configurations such as Dual CPU and 4 GB RAM.

A profile is considered matching only if it meets these criteria.

When you apply a profile, the tuned parameters, see Table A-4 corresponding to that profile is applied to the system.

These parameters belong to Sync Archive, Netconfig, Syslog, Device Management, Check Device Attributes (CDA) and Inventory Collection sub systems of the LMS application. The profile, with tuned parameters when applied, improves the performance.

Ensure that the Daemon manager is stopped, before running PTT.

Example 1
If the default profile is applied to a system which already has a Perftune - Windows profile applied to it, the parameters are rolled back to original values. See Table A-4 for Original values.

Example 2
If the Perftune - Windows profile is applied to a system which already has a default profile applied, the parameters are changed from the original values to new values. See Table A-5 for Original and New values.

Default Profile
A default profile is a profile with default values. It is used to rollback the changes done by PTT. You can roll back the changes made to a profile, by applying the default profile. This action rolls back the parameters to their original values. The parameters and the original values are:

<table>
<thead>
<tr>
<th>Sub system</th>
<th>Parameters</th>
<th>Original Values</th>
<th>Platform Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDA</td>
<td>CDA_MIN_THREADS</td>
<td>7</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>EssentialsDM</td>
<td>ConfigJobManager.heapsize</td>
<td>192m</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>EssentialsDM</td>
<td>EssentialsDMServiceHeapsize</td>
<td>256</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>Inventory Collection</td>
<td>snmp.threads.min</td>
<td>10</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>Inventory Collection</td>
<td>snmp.threads.max</td>
<td>15</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>Inventory Collection</td>
<td>ICS ThreadCount</td>
<td>10</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>Inventory Collection</td>
<td>ICS DBConnectionCount</td>
<td>5</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>NetConfig and SyncArchive</td>
<td>max_threads_for_config_fetch</td>
<td>5</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>NetConfig and SyncArchive</td>
<td>ThreadPoolCount</td>
<td>10</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
</tbody>
</table>
### Table A-4 Default Profile Original Values

<table>
<thead>
<tr>
<th>Sub system</th>
<th>Parameters</th>
<th>Original Values</th>
<th>Platform Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetConfig and SyncArchive</td>
<td>CDLNumOfThreads</td>
<td>5</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>NetConfig and SyncArchive</td>
<td>max_db_connections</td>
<td>20</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>Config Management (Config</td>
<td>Xmx</td>
<td>192</td>
<td>Solaris and Soft Appliance</td>
</tr>
<tr>
<td>Management Server Daemons -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dmgtd.conf Arguments for max</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>heap size.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Config Management (Config</td>
<td>Xms</td>
<td>64</td>
<td>Solaris and Soft Appliance</td>
</tr>
<tr>
<td>Management Server Daemons -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dmgtd.conf Arguments for minimum</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>heap size.)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Perftune - Windows and Perftune - Solaris and Soft Appliance**

This profile consists of parameters that are tuned to improve performance.

- Perftune - Windows profile is applied to a system that has a Windows operating system, provided the profile matches the required criteria.
- Perftune - Solaris and Soft Appliance profile is applied to a system that has a Solaris and Soft Appliance operating system, provided the profile matches the required criteria.

See Profiles and PTT for more information on criteria for a profile to match a system.

The parameters that can be tuned are:

### Table A-5 Perftune - Windows and Perftune - Solaris and Soft Appliance Parameters

<table>
<thead>
<tr>
<th>Sub system</th>
<th>Parameters</th>
<th>Original Values</th>
<th>New Value</th>
<th>Platform Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDA</td>
<td>CDA_MIN_THREADS</td>
<td>7</td>
<td>14</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>EssentialsDM</td>
<td>ConfigJobManager.heapsize</td>
<td>192m</td>
<td>256</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>EssentialsDM</td>
<td>EssentialsDMServiceHeapsize</td>
<td>256</td>
<td>512</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>Inventory Collection</td>
<td>snmp.threads.min</td>
<td>10</td>
<td>20</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>Inventory Collection</td>
<td>snmp.threads.max</td>
<td>15</td>
<td>25</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>Inventory Collection</td>
<td>ICS ThreadCount</td>
<td>10</td>
<td>20</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>Inventory Collection</td>
<td>ICS DBConnectionCount</td>
<td>5</td>
<td>10</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
<tr>
<td>NetConfig and SyncArchive</td>
<td>max_threads_for_config_fetch</td>
<td>5</td>
<td>10</td>
<td>Windows and Solaris and Soft Appliance</td>
</tr>
</tbody>
</table>
syslogConf.pl Utility

The syslogConf.pl is a perl script CLI utility. You can use this utility to:

- Change Syslog Analyzer Port.
- Change Syslog Collector Port.
- Configure Remote Syslog Collector (RSAC) Address and Port in LMS server.
- Change Syslog File Location.

You can run this script in the LMS server as well as the RSAC server. All the activities mentioned above can be performed in a LMS server by running the syslogConf.pl script from the command prompt.

In RSAC server, you can only change the Syslog Collector Port and Syslog File location. The Syslog Collector and Syslog Analyzer ports can be any number between 1025 and 5000.

This utility is available under:

- `NMSROOT/bin/` (On Solaris and Soft Appliance)
- `NMSROOT\bin` (On Windows)

`NMSROOT` is the LMS install directory. For Solaris and Soft Appliance, it will be `/opt/CSCOpx`.

A log file for the syslogconf.pl script is available at:

In Solaris and Soft Appliance

`/var/adm/CSCOpx/log/SyslogConf.log`

In Windows

`NMSROOT\log\SyslogConf.log`

Note: Before you run the syslogConf.pl script, ensure that the Daemon Manager is stopped.
Running the syslogConf.pl Script
To run the script:

Step 1
Go to the command prompt and enter:
NMSROOT/bin/perl NMSROOT/syslogConf.pl
When you run this syslogConf.pl script, a message appears with five options.
[1] Change Syslog Analyzer Port
[2] Change Syslog Collector Port
[4] Change Syslog File Location
[Q] Quit
Enter Your Choice:

Step 2
Enter your choice.

- If you enter 1 the following message is displayed with the old Syslog Analyzer Port number. You are also prompted to enter the new port number for the Syslog Analyzer.
  INFO: You have opted to change Local Syslog Analyzer port.
  Old Syslog Analyzer Port :xxxx
  Enter new Syslog Analyzer port:
  For example, you can change the Syslog Analyzer Port from 4444 to 2222.
  After providing the new port information, the following message is displayed.
  INFO: Local Syslog Analyzer port has been changed from 4444 to 2222 successfully

- If you enter 2 the following message is displayed with the old Syslog Collector Port number. You are also prompted to enter the new port number for the Syslog Collector.
  INFO: You have opted to change Local Syslog Collector port.
  Old Syslog Collector Port :xxxx
  Enter new Syslog Collector port:
  For example you can change the Syslog Collector Port from 1111 to 3333.
  After providing the new port information, the following message is displayed.
  INFO: Local Syslog Collector port has been changed from 1111 to 3333 successfully

- If you enter 3, the following message is displayed, with the old Syslog Collector Port number. You are also prompted to provide the new RSAC Address and the new port number for the Syslog Collector.
  INFO: You have opted to change RSAC port.
  Enter the RSAC Address:
  Old Syslog Collector Port :0
  Enter new Syslog Collector port:
  Ensure that the RSAC port that you configure in the LMS server corresponds with the Collector port configured in the RSAC server.
  You can specify srme-w2k as the RSAC Address, and change the Syslog Collector port from 0 to 3456.
  After providing the RSAC Address and port information, the following message is displayed.
  INFO: Remote Syslog Collector (RSAC) port has been changed from 0 to 3456.
• If you enter 4, the following message is displayed with the old Syslog Directory Path. You are also prompted to enter the new Syslog Directory path.

```
INFO: You have opted to change Syslog File Location
Old Syslog Directory : /var/log/
Enter Full Path of New Syslog Directory:
```

Ensure that you enter the full directory path, if you are running the syslogConf.pl script on Solaris and Soft Appliance. You can provide the relative directory path if you are running the syslogConf.pl script on Windows.

For example you can change the Syslog Directory location from /var/log/ to /var/log/newSyslogLoc.

After providing the required information, the following message is displayed.

```
Syslog file location changed from: /var/log/ to: /var/log/newSyslogLoc
```

• If you enter Q, you are allowed to quit from the script.

Software Management CLI Utility

You can invoke Software Management (SWIM) features from Command Line Interface (CLI).

The `cwcli swim` commands let you use SWIM features from the command line. You can use the `cwcli swim` commands to:

- List Images from Software Management (SWIM) Repository
- Export Images from Software Management (SWIM) Repository

These functions are only accessible to the Network Administrator, Network Operator and super users who have all of the roles.

If you do not have permission to run custom commands, you can run a command or command set from the CLI only if:

- The command set is assigned to you by the Administrator.
- The command set has at least one command that can be run on the specified device.

This section contains:

- Running `cwcli config`
- Running `cwcli swim Command`
- Running SWIM CLI Remotely

Running cwcli swim Command

The command syntax for running `cwcli swim` commands is:

```
cwcli swim subcommands common_arguments command_arguments
```

In the CLI version, you can provide the arguments in the (operating system shell) command line or in an input file.

The input file gives you flexibility and control over commands and command sets. You can specify the images on which you want to run the command sets.

In the input file, you can include subcommands and command arguments.

Items in square brackets ([]) are optional; items in curly brackets ({}) are required.
The arguments are described in the following sections.

### Subcommands

Subcommands specify the actions that you perform. Valid values for subcommands are described in the following table.

<table>
<thead>
<tr>
<th>Sub Command</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>listimages</td>
<td>Displays a list of images available in the Software Repository.</td>
<td>cwcli swim listimages -u Userid -p Password</td>
</tr>
<tr>
<td>exportimages</td>
<td>Exports specified images in a non-compressed format from the Software Repository to any directory. The default target directory is the current directory. For exportimages command either one of these arguments is mandatory: -imagenames</td>
<td>cwcli swim exportimages -u Username -p Password [-imagenames imagename1, imagename2...] [-all] [-dirname directoryname] [-input argumentFile] [-m email][-l logfile]</td>
</tr>
<tr>
<td>help</td>
<td>Displays command usage information.</td>
<td>cwcli swim -help</td>
</tr>
</tbody>
</table>

### Common Arguments

Common arguments specify parameters that apply to all subcommands. Valid values for `common_arguments` are described in the following table.

<table>
<thead>
<tr>
<th>Command Arguments</th>
<th>Description/Action</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-u user</code></td>
<td>Enter a valid LMS username.</td>
<td>None</td>
</tr>
<tr>
<td><code>-p password</code></td>
<td>Enter the password for the username. You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for more details.</td>
<td>None</td>
</tr>
</tbody>
</table>
| `-l log_filename` | Identifies a file to which Software Management Commands will write log messages. It you do not specify this, the log output will appear on screen. | This argument is optional. 
`log_filename` can be a full path to the file or a filename in the local directory. If you do not specify filename, the log file will be created in:
  - `/var/adm/CSCOpx/log` (On Solaris and Soft Appliance)
  - `NMSROOT\log` (On Windows)
`NMSROOT` is the LMS install directory. |
| `-m Email ID`     | Enter your Email ID                                                                                  | This argument is optional. You will get the output of the CLI operation in an e-mail.            |
Command Arguments

Command arguments specify parameters that apply only to specific subcommands. Valid values for command arguments are described in the following table.

Arguments in square brackets ([ ]) are optional. Arguments in curly brackets ( { }) are required. You must provide one argument from each group of arguments in curly brackets ( { }) that is separated by vertical bars (|).

<table>
<thead>
<tr>
<th>Command Arguments</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>-imagenames ImageName1, ImageName2</td>
<td>Specify the image names that you want to export using this command.</td>
<td>cwcli swim exportimages -u Username -p Password [-imagenames imagename1, imagename2...][-all] [-dirname directoryname] [-input argumentFile] [-m email][-l logfile] ImageName1, ImageName2 —List of images. Separate these names by commas.</td>
</tr>
<tr>
<td>-all</td>
<td>Specify this option if you want to export all images from Software Repository to the current directory or any specified directory.</td>
<td>--</td>
</tr>
</tbody>
</table>
| -input argumentFile | Input file containing the details of the subcommands | If you are specifying the input file, you need not specify the subcommands. For instance, if you are using sample.txt as the argumentFile for -input command, you have to provide the following command: cwcli swim exportimages -input sample.txt
Example of sample.txt:
- -imagenames imagename1, imagename2...
- -imagenames imagename4, imagename5...
Items in square brackets ([ ]) are optional; items in curly brackets ( { }) are required. |
| -dirname directoryname | Specify a directory name if you want to export images to a specified directory using this command. | If you do not specify this the images are exported to the NMSROOT/temp directory, where CLI is launched. |
Running SWIM CLI Remotely

You can run Software Management (SWIM) CLI from a remote console.

SWIM uses the Remote Access feature in the CLI framework to help you to invoke the SWIM commands from the client in the same way as you run them on the LMS server.

The name of the servlet to be invoked is /rme/cwcli.

You must invoke the following URLs to run any command.

- For POST request:
  
  http://lms-server:lms-port/rme/cwcli payload XML file

- For GET request:
  

The contents of the payload.xml is:

```xml
<payload>
  <command>
    cwcli swim command -u Username -p Password command_specific_args
  </command>
</payload>
```

For example to execute the listimages command payload.xml will be as follows:

```xml
<payload>
  <command>
    cwcli swim listimages -u Username -p Password
  </command>
</payload>
```

Note: The Base64 encoded password is used for accessing Software Management (SWIM) CLI remotely.

To invoke the servlet using a script, see the Overview: cwcli invreport Command.

The script and the payload file should be residing in the client machine.
Cisco Prime LMS allows you to create new configuration templates (.xml format) that can be deployed using the Template Center feature.

This appendix explains:

- Understanding the XML Schema
- Sample Template for Identity - Change of Authorization
- Sample Template for IF Statement

Understanding the XML Schema

This section explains the XML schema that you can use to create new templates (.xml format) and deploy them in LMS. See Detailed Description of Template XML Schema for more information.

The XML schema file is:

```xml
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:jaxb="http://java.sun.com/xml/ns/jaxb"
  xmlns:xjc="http://java.sun.com/xml/ns/jaxb/xjc"
  jaxb:extensionBindingPrefixes="xjc"
  jaxb:version="1.0">

  <xs:annotation>
    <xs:appinfo>
      <jaxb:globalBindings generateIsSetMethod="true">
        <xjc:serializable uid="1255591397484"/> <!-- 14-Oct-2009 -->
      </jaxb:globalBindings>
    </xs:appinfo>
  </xs:annotation>

  <!-- Defining root OOTB template -->
  <xs:element name="ootb-template">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="template-metadata" type="template-metadata" minOccurs="1" maxOccurs="1"/>
        <xs:element name="config" type="config" minOccurs="1" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```
Understanding the XML Schema

<!-- Defining the template meta data -->
<xs:complexType name="template-metadata">
  <xs:all>
    <xs:element name="template-details" type="template-details" minOccurs="1" maxOccurs="1" />
    <xs:element name="parameter-metadata" type="parameter-metadata" minOccurs="0" maxOccurs="1" />
  </xs:all>
  <xs:attribute name="name" type="xs:string" use="required" />
</xs:complexType>

<!-- Defining the template details -->
<xs:complexType name="template-details">
  <xs:all>
    <xs:element name="description" type="xs:string" maxOccurs="1" minOccurs="1" />
    <xs:element name="task" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="author" type="xs:string" minOccurs="0" maxOccurs="1" default="Cisco Systems" />
    <xs:element name="template-version" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="scope" type="xs:string" default="Device" minOccurs="0" maxOccurs="1" />
    <xs:element name="type" type="xs:string" default="Partial" minOccurs="0" maxOccurs="1" />
    <xs:element name="features" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="pin" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="hardware-platform" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="imagefeature" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="conflictingtag" type="conflictingtag" minOccurs="0" maxOccurs="1" />
  </xs:all>
</xs:complexType>

<!-- Defining the conflicting tag details -->
<xs:complexType name="conflictingtag">
  <xs:sequence>
    <xs:element name="platform" type="conflict-platform" minOccurs="1" maxOccurs="unbounded" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="conflict-platform">
  <xs:sequence>
    <xs:element name="feature" type="featureType" minOccurs="0" maxOccurs="1" />
  </xs:sequence>
  <xs:attribute name="name" type="xs:string" use="required" />
</xs:complexType>

<xs:complexType name="featureType">
  <xs:sequence>
    <xs:element name="cli-command" type="cli-command" minOccurs="0" maxOccurs="1" />
  </xs:sequence>
  <xs:attribute name="name" type="xs:string" use="required" />
  <xs:attribute name="message" type="xs:string" use="required" />
</xs:complexType>
<!-- Defining parameter meta data -->
<xs:complexType name="parameter-metadata">
  <xs:sequence>
    <xs:element name="param-group" type="param-group" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="param-group">
  <xs:sequence>
    <xs:element name="description" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="parameter" type="parameter" minOccurs="0" maxOccurs="unbounded" />
    <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
    <xs:attribute name="cliName" type="xs:string" use="required"></xs:attribute>
    <xs:attribute name="isMandatory" type="xs:boolean" use="required"></xs:attribute>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="parameter">
  <xs:sequence>
    <xs:element name="description" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="html-component" type="xs:string" minOccurs="0" maxOccurs="0" />
    <xs:element name="default-value" minOccurs="0" maxOccurs="unbounded">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="xs:string">
            <xs:attribute name="label" type="xs:string" use="optional"></xs:attribute>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>
    <xs:element name="data-type" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="mandatory" type="xs:boolean" minOccurs="0" maxOccurs="1" />
    <xs:element name="isGlobal" type="xs:boolean" minOccurs="0" maxOccurs="1" />
    <xs:element name="help-description" type="xs:string" minOccurs="0" maxOccurs="0" />
    <xs:element name="syntax" type="syntax" minOccurs="0" maxOccurs="1" />
  </xs:sequence>
  <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
</xs:complexType>

<xs:complexType name="syntax">
  <xs:all>
    <xs:element name="min" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="max" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="pattern" type="cli-command" minOccurs="0" maxOccurs="1" />
  </xs:all>
</xs:complexType>

</xs:complexType>

<!-- Configuration details -->
<xs:complexType name="config">
  <xs:sequence>
    <xs:element name="device-filtering-details" type="device-filtering-details" />
    <xs:element name="cli" type="cliType" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
  <xs:attribute name="platform" type="xs:string" use="required" />
</xs:complexType>

<xs:complexType name="cliType">
  <xs:all>
    <xs:element name="min" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="max" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="pattern" type="cli-command" minOccurs="0" maxOccurs="1" />
  </xs:all>
</xs:complexType>
Understanding the XML Schema

```xml
<xs:sequence>
  <xs:element name="clicommand" type="cli-command" minOccurs="1" maxOccurs="unbounded" />
</xs:sequence>

<xs:complexType>
  <xs:attribute name="name" type="xs:string" use="required" />
</xs:complexType>

<!-- Device filtering details -->
<xs:complexType name="device-filtering-details">
  <xs:sequence>
    <xs:element name="family" type="family" minOccurs="1" maxOccurs="unbounded" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="family">
  <xs:all>
    <xs:element name="min-supported-imageversion" type="min-supported-imageversion" minOccurs="1" maxOccurs="1" />
  </xs:all>
  <xs:attribute name="value" type="xs:string" use="required" />
</xs:complexType>

<xs:complexType name="min-supported-imageversion">
  <xs:sequence>
    <xs:element name="device-type" type="device-type" minOccurs="1" maxOccurs="unbounded" />
  </xs:sequence>
  <xs:attribute name="value" type="xs:string" use="required" />
</xs:complexType>

<xs:complexType name="device-type">
  <xs:all>
    <xs:element name="name" type="xs:string" minOccurs="0" maxOccurs="1" />
    <xs:element name="sysobjectid" type="xs:string" minOccurs="0" maxOccurs="1" />
  </xs:all>
</xs:complexType>

<!-- configuration cli -->
<xs:simpleType name="cli-command">
  <xs:restriction base="xs:string">
    <xs:annotation>
      <xs:appinfo>
        <jAXB type="CDATA" />
      </xs:appinfo>
    </xs:annotation>
  </xs:restriction>
</xs:simpleType>
</xs:schema>
```
## Detailed Description of Template XML Schema

The table below describes elements in the XML schema.

<table>
<thead>
<tr>
<th>Xml Tag Name</th>
<th>Tag Description</th>
<th>Occurrence</th>
<th>Sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ootb-template&gt;</td>
<td>Any Template should start with this</td>
<td>1</td>
<td>&lt;ootb-template&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>&lt;/ootb-template&gt;</td>
</tr>
<tr>
<td>&lt;template-metadata&gt;</td>
<td>Configuration specific metadata should be under this tag. It has the following attribute:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• name—Specifies the name of the Template. This name is used for identifying the template.</td>
<td>1</td>
<td>&lt;template-metadata name=&quot;3750 access config&quot;&gt;</td>
</tr>
<tr>
<td>&lt;template-details&gt;</td>
<td>This tag comes under template-metadata tag. This tag will take up the metadata such as description, task, author, revision to the template.</td>
<td>1</td>
<td>&lt;template-details&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>&lt;/template-details&gt;</td>
</tr>
<tr>
<td>&lt;description&gt;</td>
<td>This tag comes under template-details tag. Gives a small description about the template.</td>
<td>1</td>
<td>&lt;description&gt;c3750 stacked configuration&lt;/description&gt;</td>
</tr>
<tr>
<td>&lt;task&gt;</td>
<td>This tag comes under template-details tag. It gives the functionality of the tag.</td>
<td>0</td>
<td>&lt;task&gt;Snmp Community settings&lt;/task&gt;</td>
</tr>
<tr>
<td>&lt;author&gt;</td>
<td>This tag comes under template-details tag. It gives the name of the person who has created the template. Multiple names can be given separated by commas. By default, the author name is Cisco Systems.</td>
<td>0</td>
<td>&lt;author&gt;cisco systems&lt;/author&gt;</td>
</tr>
<tr>
<td>&lt;template-version&gt;</td>
<td>This tag comes under template-details tag. It gives the revision number to the template.</td>
<td>0</td>
<td>&lt;template-version&gt;1.0&lt;/template-version&gt;</td>
</tr>
</tbody>
</table>
### Elements in the XML Schema

<table>
<thead>
<tr>
<th>XML Tag Name</th>
<th>Tag Description</th>
<th>Occurrence</th>
<th>Sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;scope&gt;</code></td>
<td>This tag comes under template-details tag. It gives the scope of the template</td>
<td>0 1</td>
<td><code>&lt;scope&gt;port&lt;/scope&gt;</code></td>
</tr>
<tr>
<td></td>
<td>that accepts values of either Device, Port, Module</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>&lt;type&gt;</code></td>
<td>This tag comes under template-details tag. It refers to the type of the template</td>
<td>0 1</td>
<td><code>&lt;type&gt;partial&lt;/type&gt;</code></td>
</tr>
<tr>
<td></td>
<td>taking values of either partial or complete.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>&lt;features&gt;</code></td>
<td>This tag comes under template-details tag. It gives the list of features for</td>
<td>0 1</td>
<td><code>&lt;features&gt;dhcp snoop, auto</code></td>
</tr>
<tr>
<td></td>
<td>which this config can be applied. Features can be given in a comma separated</td>
<td></td>
<td><code>&lt;features&gt;qos&lt;/features&gt;</code></td>
</tr>
<tr>
<td></td>
<td>values.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>&lt;pin&gt;</code></td>
<td>This tag comes under template-details tag. It gives the devices in the network</td>
<td>0 1</td>
<td><code>&lt;pin&gt;edge&lt;/pin&gt;</code></td>
</tr>
<tr>
<td></td>
<td>to which the template is applicable. Comma separated values are allowed</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>&lt;hardware-platform&gt;</code></td>
<td>This tag comes under template-details tag. It gives the hardware type to which</td>
<td>0 1</td>
<td><code>&lt;hardware-platform&gt;stack&lt;/hardware-platform&gt;</code></td>
</tr>
<tr>
<td></td>
<td>the template is applicable. Comma separated values are allowed</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>&lt;imagefeature&gt;</code></td>
<td>This tag comes under template-details tag. It gives the image feature that is</td>
<td>0 1</td>
<td><code>&lt;imagefeature&gt;ipbase&lt;/imagefeature&gt;</code></td>
</tr>
<tr>
<td></td>
<td>required to apply this template.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>&lt;conflictingtag&gt;</code></td>
<td>This tag comes under template-details tag. The template cannot be applied when</td>
<td>0 1</td>
<td><code>&lt;conflictingtag&gt;&lt;/conflictingtag&gt;</code></td>
</tr>
<tr>
<td></td>
<td>any cli is given under this tag.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table B-1 Elements in the XML Schema

<table>
<thead>
<tr>
<th>XML Tag Name</th>
<th>Tag Description</th>
<th>Occurrence</th>
<th>Sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;platform&gt;</td>
<td>This tag comes under conflictingtag tag.</td>
<td>1</td>
<td>Unlimited</td>
</tr>
<tr>
<td></td>
<td>It has an attribute <code>name</code> that specifies to which platform the conflicting tag</td>
<td></td>
<td><code>&lt;platform name=&quot;ios&quot;&gt; &lt;/platform&gt;</code></td>
</tr>
<tr>
<td></td>
<td>belongs to. Following are the values taken by <code>name</code> attribute:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ios, catos, pixos, nam, Soft Appliance, ios_ssl, ios_wlsm, ios_mwam, ios_webvpn,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>webns, ACE, ACNS, CSM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;feature&gt;</td>
<td>This tag will come under conflictingtag.</td>
<td>1</td>
<td>Unlimited</td>
</tr>
<tr>
<td></td>
<td>It has the following attributes,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• name—Name of the feature that is conflicting to this template.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• message—Warning message that needs to be shown when this feature is available.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• platform—Software platform to which this feature is conflicting to this template.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;feature name=&quot;dot1x&quot; message=&quot;since dot1x conflict is there, do not configure</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>the following template in the device.&quot; platform=&quot;ios&quot;&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;/feature&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;cli-command&gt;</td>
<td>This tag comes under feature tag.</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Cli which needs to be searched in a running configuration. If this configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is found, the cli will not be deployed.</td>
<td></td>
<td><code>&lt;cli-command&gt;no aaa new-model clock summer-time utc recurring&lt;/cli-command&gt;</code></td>
</tr>
<tr>
<td>&lt;parameter-metadata&gt;</td>
<td>This tag comes under template-metadata tag.</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>This section describes the variables that are used in the template.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;/parameter-metadata&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table B-1: Elements in the XML Schema

<table>
<thead>
<tr>
<th>Xml Tag Name</th>
<th>Tag Description</th>
<th>Occurrence</th>
<th>Sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;param-group&gt;</td>
<td>This tag comes under parameter-metadata tag and is used to group the parameters. For example, if there are five parameters, two can be grouped in one and the remaining three in another group. Attributes of this tag: • name—Name of the group • cliName—A key that maps the parameter group to a Cli group. Both cliName and the name of the cli should be same. • isMandatory—To indicate if this group is mandatory for the template or not. Useful in case of partial template, where you will have the option in the UI as Skip this section.</td>
<td>1 Unlimited</td>
<td>&lt;param-group name=&quot;Identity Commands&quot; cliName=&quot;identity&quot; isMandatory=&quot;true&quot; &gt; &lt;description&gt;Readonly Community String&lt;/description&gt;</td>
</tr>
<tr>
<td>&lt;description&gt;</td>
<td>This tag comes under param-group tag. Provides a simple description about the parameter. It is mandatory as this will be taken as a Label for the html component.</td>
<td>1 1</td>
<td>&lt;description&gt;Readonly Community String&lt;/description&gt;</td>
</tr>
<tr>
<td>&lt;parameter&gt;</td>
<td>This tag comes under parameter-metadata tag. Describes about a single parameter to get input from the user. This parameter will be converted into a html component. Any variable defined in the cli should have a parameter tag defined. It takes the name as an attribute to this tag.</td>
<td>1 Unlimited</td>
<td>&lt;parameter name=&quot;readonly&quot;&gt;</td>
</tr>
<tr>
<td>&lt;html-component&gt;</td>
<td>This tag comes under parameter tag. Specifies what html component is rendered for the specified parameter.</td>
<td>0 Unlimited</td>
<td>&lt;html-component&gt;textbox&lt;/html-component&gt;</td>
</tr>
</tbody>
</table>
### Table B-1 Elements in the XML Schema

<table>
<thead>
<tr>
<th>XML Tag Name</th>
<th>Tag Description</th>
<th>Occurrence</th>
<th>Sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;default-value&gt;</td>
<td>This tag comes under parameter tag. Default value for the parameter. This tag can be used to give values for a select box. It has the following attribute: label—It is used to build the combo box content. The label value is displayed as a content to the combo box. The element value defined is considered as a selected value in the backend.</td>
<td>Unlimited</td>
<td>&lt;default-value label=&quot;0-shut&quot;&gt;0&lt;/default-value&gt;</td>
</tr>
<tr>
<td>&lt;data-type&gt;</td>
<td>This tag comes under parameter tag. It specifies datatype of the input that is given to the parameter.</td>
<td>1</td>
<td>&lt;datatype&gt;integer&lt;/datatype&gt; Boolean or Integer</td>
</tr>
<tr>
<td>&lt;mandatory&gt;</td>
<td>This tag comes under parameter tag. To specify if this parameter is mandatory parameter or not. Accepts value true or false.</td>
<td>1</td>
<td>&lt;mandatory&gt;&lt;/mandatory&gt;</td>
</tr>
<tr>
<td>&lt;isGlobal&gt;</td>
<td>This tag comes under parameter tag. To specify if this parameter is applicable for all devices or only one device. Accepts the following values: • true—applicable for all devices • false—applicable for per device level</td>
<td>1</td>
<td>&lt;isGlobal&gt;&lt;/isGlobal&gt;</td>
</tr>
<tr>
<td>&lt;help-description&gt;</td>
<td>This tag comes under parameter tag. Use for describing more about this parameter.</td>
<td>1</td>
<td>&lt;help-description&gt;&lt;/help-description&gt;</td>
</tr>
<tr>
<td>&lt;syntax&gt;</td>
<td>This tag come under parameter tag. To specify the validation part for numeric field and the string parameter.</td>
<td>1</td>
<td>&lt;syntax&gt;&lt;/syntax&gt;</td>
</tr>
</tbody>
</table>
### Understanding the XML Schema

<table>
<thead>
<tr>
<th>Xml Tag Name</th>
<th>Tag Description</th>
<th>Occurrence</th>
<th>Sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;min&gt;</td>
<td>This tag comes under syntax tag. To specify the minimum value for a numeric field. The datatype should be numeric.</td>
<td>0 1</td>
<td>&lt;Min&gt;0&lt;/min&gt;</td>
</tr>
<tr>
<td>&lt;max&gt;</td>
<td>This tag comes under syntax tag. To specify the maximum value for a numeric parameter. The datatype should be numeric.</td>
<td>0 1</td>
<td>&lt;max&gt;100&lt;/max&gt;</td>
</tr>
<tr>
<td>&lt;pattern&gt;</td>
<td>This tag comes under syntax tag. To specify the regular expression for the string parameter. The regular expression is used to validate the value that is specified by the user.</td>
<td>0 1</td>
<td>&lt;pattern&gt;[a-z]*&lt;/pattern&gt;</td>
</tr>
<tr>
<td>&lt;config&gt;</td>
<td>This tag comes under ootb-template tag. The respective config which needs to be deployed into the devices is defined here. For example, config tag should come under OOTB-Template. It has the following attribute: platform—Specifies to what software platform this config is applicable. Following are the values taken by this attribute: ios, catos, pixos, nam, Soft Appliance, ios_ssl, ios_wlsm, ios_mwam, ios_webvpn, webns, ACE, ACNS, CSM</td>
<td>1 1</td>
<td>&lt;config&gt;&lt;/config&gt;</td>
</tr>
<tr>
<td>&lt;device-filtering-details&gt;</td>
<td>This tag comes under config tag. To specify the filtering details for the device.</td>
<td>1 1</td>
<td>&lt;device-filtering-details&gt;&lt;/device-filtering-details&gt;</td>
</tr>
<tr>
<td>&lt;family&gt;</td>
<td>This tag comes under device-filtering-details tag. To specify what family this filtering belongs to. The Value should be as specified in mdfData.xml for the supported devices.</td>
<td>1 Unlimited</td>
<td>&lt;family value=&quot;cisco catalyst 3750-e series switches&quot;&gt; &lt;/family&gt;</td>
</tr>
</tbody>
</table>
### Understanding the XML Schema

**Table B-1: Elements in the XML Schema**

<table>
<thead>
<tr>
<th>Xml Tag Name</th>
<th>Tag Description</th>
<th>Occurrence</th>
<th>Sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;min-supported-image version&gt;</td>
<td>This tag come under family tag. To specify the minimum supported image version to which this template will be applicable.</td>
<td>1</td>
<td>&lt;min-support-imageversion&gt;12.2(40)se&lt;/min-support-imageversion&gt;</td>
</tr>
<tr>
<td>&lt;device-type&gt;</td>
<td>This tag comes under min-supported-imageversion. To specify which device type this template will be applicable.</td>
<td>1</td>
<td>Unlimited &lt;device-type&gt; &lt;/device-type&gt;</td>
</tr>
<tr>
<td>&lt;name&gt;</td>
<td>This tag comes under device-type tag. It gives the MDF name of the device type.</td>
<td>0</td>
<td>1                               &lt;name&gt; &lt;/name&gt;</td>
</tr>
<tr>
<td>&lt;sysobjectid&gt;</td>
<td>This tag comes under device-type tag. It gives the sysobjectid of the device.</td>
<td>0</td>
<td>1                               &lt;sysObjectld&gt;&lt;/sysObjectld&gt;</td>
</tr>
<tr>
<td>&lt;cli&gt;</td>
<td>This tag come under config tag. It specifies the cli for the mentioned software platform. It has the attribute called name. The value should be same as that of param-group name. This is used to map the param-group to that of cli.</td>
<td>0</td>
<td>Unlimited &lt;cli name=&quot;snmpSecurity&quot;&gt;</td>
</tr>
<tr>
<td>&lt;clicommand&gt;</td>
<td>This tag comes under cli tag. To specify the command that will be deployed.</td>
<td>1</td>
<td>Unlimited &lt;clicommand&gt;&lt;![CDATA[]]&gt; &lt;/clicommand&gt;</td>
</tr>
<tr>
<td>&lt;MLTCMD&gt;</td>
<td>To specify multi-line commands like, banner and crypto certificate commands. The commands within the MLTCMD tags are considered as a single command and will be downloaded as a single command onto the device. These tags are case-sensitive and you must enter them only in uppercase. You cannot start this tag with a space. You can have a blank line within a multi-line command.</td>
<td>0</td>
<td>Unlimited If you use this tag between cdata tags, then you must use &lt;MLTCMD&gt;. For example: &lt;MLTCMD&gt;banner login &quot;Welcome to Cisco Prime LMS - you are using Multi-line commands&quot; &lt;/MLTCMD&gt; If cdata is not present, then you must use &lt;MLTCMD&gt;. For example: &lt;MLTCMD&gt; banner login &quot;Welcome to Cisco Prime LMS - you are using Multi-line commands&quot; &lt;/MLTCMD&gt;</td>
</tr>
</tbody>
</table>
Sample Template for Identity - Change of Authorization

The section shows the template for Identity - Change of Authorization:

```xml
<?xml version="1.0" encoding="iso-8859-1"?>
<!--****************************************************-->  
<!--         Copyright (c) 2009, 2010 Cisco Systems, Inc.     -->
<!--         All rights reserved.                       -->
<!--****************************************************-->  
<ootb-template>
<template-metadata name="Identity - Change of Authorization">
  <template-details>
    <description>Identity - Change of Authorization</description>
    <task>Identity</task>
    <author>Cisco Systems</author>
    <template-version>1.0</template-version>
    <scope>Device</scope>
    <type>partial</type>
    <features></features>
    <pin>edge</pin>
    <hardware-platform>Device</hardware-platform>
    <imagefeature>ipbase</imagefeature>
  </template-details>
  <parameter-metadata>
    <param-group name="Identity Commands" cliName="identity" isMandatory="true">
      <description>A standard RADIUS interface is one where the request for authorization originates from the device attached to the network, and the response comes from the queried RADIUS servers. However, Catalyst Switches support the RADIUS Change of Authorization (CoA). CoA allows for the dynamic reconfiguration of sessions from external RADIUS servers.</description>
      <parameter name="ipaddress">
        <description>RADIUS client IP address or Host name</description>
        <html-component>textbox</html-component>
        <default-value></default-value>
        <data-type>string</data-type>
        <mandatory>true</mandatory>
        <isGlobal>true</isGlobal>
        <help-description></help-description>
        <syntax>
          <min></min>
          <max></max>
          <pattern></pattern>
        </syntax>
      </parameter>
      <parameter name="authtype">
        <description>Type of authorization the device uses for RADIUS clients</description>
        <html-component>select</html-component>
        <default-value label="any">any</default-value>
        <default-value label="all">all</default-value>
        <default-value label="session-key">session-key</default-value>
        <data-type>string</data-type>
        <mandatory>true</mandatory>
        <isGlobal>true</isGlobal>
        <help-description></help-description>
        <syntax>
          <min></min>
          <max></max>
          <pattern></pattern>
        </syntax>
      </parameter>
    </param-group>
  </parameter-metadata>
</template-metadata>
</ootb-template>
```
Sample Template for Identity - Change of Authorization

<parameter name="server-key">
  <description>RADIUS Key shared between the device and RADIUS clients</description>
  <html-component-password>
  <default-value></default-value>
  <data-type>string</data-type>
  <mandatory>true</mandatory>
  <isGlobal>true</isGlobal>
  <help-description></help-description>
  <syntax>
    <min></min>
    <max></max>
    <pattern></pattern>
  </syntax>
</parameter>

<parameter name="port">
  <description>Port on which the device listens for RADIUS requests [0 - 65535]</description>
  <html-component-textbox>
  <default-value>1700</default-value>
  <data-type>numeric</data-type>
  <mandatory>true</mandatory>
  <isGlobal>true</isGlobal>
  <help-description></help-description>
  <syntax>
    <min>0</min>
    <max>65535</max>
    <pattern></pattern>
  </syntax>
</parameter>

<parameter-metadata>
</parameter-metadata>
</template-metadata>
<config platform="ios">
<device-filtering-details>
<family value="Switches and Hubs">
<device-type>
  <name>Cisco Catalyst 2960-24TC Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.694</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-48TC Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.695</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960G-24TC Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.696</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960G-48TC Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.697</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-24TT Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.716</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-48TT Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.717</sysobjectid>
</device-type>
</family>
</device-type>
</device-filtering-details>
</config>
Appendix B  Config Template XML Schema

Sample Template for Identity - Change of Authorization

<device-type>
  <name>Cisco Catalyst 2960-8TC Compact Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.798</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960G-8TC Compact Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.799</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-24-S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.929</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-24TC-S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.928</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-48TC-S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.927</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-24PC-S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.950</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960PD-8TT-L Compact Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.952</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-8TC-S Compact Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1006</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-48TT-S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1005</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-48PST-L Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1016</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-24LC-S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1146</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-24PC-S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1147</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960-48PST-S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1148</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Enhanced Layer 2 EtherSwitch Service Module</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1048</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Enhanced Layer 2 EtherSwitch Service Module</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1051</sysobjectid>
</device-type>
Appendix B Config Template XML Schema

Sample Template for Identity - Change of Authorization

<device-type>
  <name>Cisco Enhanced Layer 2 EtherSwitch Service Module</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1052</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Enhanced Layer 2 EtherSwitch Service Module</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1055</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960S-48TS-S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1256</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960S-24TS-S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1257</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960S-48FPS-L Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1263</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960S-48LPS-L Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1264</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960S-24PS-L Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1265</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960S-48TS-L Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1266</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960S-24TS-L Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1267</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2960 stack</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1208</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 2926 Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.5.35</sysobjectid>
</device-type>
<device-type>
    <name>Cisco Catalyst 2980G-A Switch</name>
    <sysobjectid>1.3.6.1.4.1.9.5.51</sysobjectid>
</device-type>
<device-type>
    <name>Cisco Catalyst 2980G-A Switch</name>
    <sysobjectid>1.3.6.1.4.1.9.5.49</sysobjectid>
</device-type>
<device-type>
    <name>Cisco Catalyst 2948G-GE-TX Switch</name>
    <sysobjectid>1.3.6.1.4.1.9.5.62</sysobjectid>
</device-type>
<device-type>
    <name>Cisco Catalyst 2975 Switch</name>
    <sysobjectid>1.3.6.1.4.1.9.1.1068</sysobjectid>
</device-type>
</min-supported-imageversion>
</family>

<family value="Switches and Hubs">
    <min-supported-imageversion value="12.2(52)SE">
        <device-type>
            <name>Cisco Catalyst 3560G-24PS Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.614</sysobjectid>
        </device-type>
        <device-type>
            <name>Cisco Catalyst 3560G-24TS Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.615</sysobjectid>
        </device-type>
        <device-type>
            <name>Cisco Catalyst 3560G-48PS Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.616</sysobjectid>
        </device-type>
        <device-type>
            <name>Cisco Catalyst 3560G-48TS Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.617</sysobjectid>
        </device-type>
        <device-type>
            <name>Cisco Catalyst 3560 Series Switches</name>
            <sysobjectid>1.3.6.1.4.1.9.1.563</sysobjectid>
        </device-type>
        <device-type>
            <name>Cisco Catalyst 3560-48PS Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.564</sysobjectid>
        </device-type>
        <device-type>
            <name>Cisco Catalyst 3560-24TS Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.633</sysobjectid>
        </device-type>
        <device-type>
            <name>Cisco Catalyst 3560-48TS Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.634</sysobjectid>
        </device-type>
        <device-type>
            <name>Cisco Catalyst 3560B-24TD-E,S Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.793</sysobjectid>
        </device-type>
        <device-type>
            <name>Cisco Catalyst 3560B-48TD-E,S Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.794</sysobjectid>
        </device-type>
        <device-type>
            <name>Cisco Catalyst 3560B-24PD-E,S Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.795</sysobjectid>
        </device-type>
    </min-supported-imageversion>
</family>
</device-type>
<device-type>
  <name>Cisco Catalyst 3560E-48PD-E,S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.796</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3560-8PC Compact Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.797</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3560E-12D-S,E Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.930</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3560E-12SD-E,S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.956</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3560-12PC-S Compact Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1015</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3560V2-48PS Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1025</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3560V2-24DC Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1019</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3560V2-24TS Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1020</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3560V2-24PS Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1021</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3560V2-48TS Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1024</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Enhanced Layer2,Layer3 EtherSwitch Service Module</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1049</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Enhanced Layer2,Layer3 EtherSwitch Service Module</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1050</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Enhanced Layer2,Layer3 EtherSwitch Service Module</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1053</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Enhanced Layer2,Layer3 EtherSwitch Service Module</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1054</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Enhanced Layer2,Layer3 EtherSwitch Service Module</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1056</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Enhanced Layer2,Layer3 EtherSwitch Service Module</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1057</sysobjectid>
<!-- Cisco Catalyst 3750 Series Switches and Similar categories -->
<family value="Switches and Hubs">
  <min-supported-imageversion value="12.2(52)SE">
    <device-type>
      <name>Cisco 3750 Stack</name>
      <sysobjectid>1.3.6.1.4.1.9.1.516</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco Catalyst 3750G-12S Switch</name>
      <sysobjectid>1.3.6.1.4.1.9.1.530</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco Catalyst 3750-24PS Switch</name>
      <sysobjectid>1.3.6.1.4.1.9.1.536</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco 2600,2800,3700,3800 Series 16-Port EtherSwitch Service Module</name>
      <sysobjectid>1.3.6.1.4.1.9.1.663</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco 2800,3800 Series 23-Port EtherSwitch Service Module</name>
      <sysobjectid>1.3.6.1.4.1.9.1.664</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco 2851,3800 Series 48-Port EtherSwitch Service Module</name>
      <sysobjectid>1.3.6.1.4.1.9.1.666</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco 2851,3800 Series 24-Port EtherSwitch (with Stackwise Connectors) Service Module</name>
      <sysobjectid>1.3.6.1.4.1.9.1.665</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco 2600,2800,3700,3800 Series 16-Port EtherSwitch Service Module</name>
      <sysobjectid>1.3.6.1.4.1.9.1.702</sysobjectid>
    </device-type>
  </min-supported-imageversion>
</family>
<sysobjectid>1.3.6.1.4.1.9.1.688</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750E-24TD-E,S Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.789</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750E-48TD-E,S Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.790</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750E-48PD-E,S Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.791</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750E-24PD-E,S Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.792</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750G-24 Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.511</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750G-48 Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.512</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750-24TS Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.513</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750-48TS Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.535</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750G-24PS Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.602</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750G-48PS Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.603</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750G-48TS Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.604</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750G-24TS-1U Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.624</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750-24FS Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.656</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750V2-48PS Switch</name>
 <sysobjectid>1.3.6.1.4.1.9.1.1027</sysobjectid>
</device-type>
<device-type>
 <name>Cisco Catalyst 3750V2-24PS Switch</name>
Appendix B     Config Template XML Schema

Sample Template for Identity - Change of Authorization

<sysobjectid>1.3.6.1.4.1.9.1.1023</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3750V2-24TS Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1022</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3750V2-48TS Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1026</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3750X-24T-L,S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1222</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3750X-48T-L,S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1223</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3750X-24P-L,S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1224</sysobjectid>
</device-type>
<device-type>
  <name>Cisco Catalyst 3750X-48PF-L,S Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.1.1225</sysobjectid>
</device-type>
</min-supported-imageversion>
</family>

<fAMILY value="Switches and Hubs">
  <min-supported-imageversion value ="12.2(50)SG">
    <device-type>
      <name>Cisco Catalyst 4503 Switch</name>
      <sysobjectid>1.3.6.1.4.1.9.5.58</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco Catalyst 4506 Switch</name>
      <sysobjectid>1.3.6.1.4.1.9.5.59</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco Catalyst 4506-E Switch</name>
      <sysobjectid>1.3.6.1.4.1.9.1.875</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco Catalyst 4510R-E Switch</name>
      <sysobjectid>1.3.6.1.4.1.9.1.877</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco Catalyst 4503-E Switch</name>
      <sysobjectid>1.3.6.1.4.1.9.1.874</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco Catalyst 4507R-E Switch</name>
      <sysobjectid>1.3.6.1.4.1.9.1.876</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco Catalyst 4507R Switch</name>
      <sysobjectid>1.3.6.1.4.1.9.1.501</sysobjectid>
    </device-type>
    <device-type>
      <name>Cisco Catalyst 4506 Switch</name>
      <sysobjectid>1.3.6.1.4.1.9.1.502</sysobjectid>
    </device-type>
    </min-supported-imageversion>
  </family>
<name>Cisco Catalyst 4503 Switch</name>
<sysobjectid>1.3.6.1.4.1.9.1.503</sysobjectid>
</device-type>
<device-type>
<name>Cisco Catalyst 4510R Switch</name>
<sysobjectid>1.3.6.1.4.1.9.1.537</sysobjectid>
</device-type>
</min-supported-imageversion>
</family>

<!-- Cisco Catalyst 6500 Series Switches and Similar categories -->
<family value="Switches and Hubs">
<min-supported-imageversion value ="12.2(33)SXI">
<device-type>
<name>Cisco Catalyst 6513 Switch</name>
<sysobjectid>1.3.6.1.4.1.9.1.400</sysobjectid>
</device-type>
<device-type>
<name>Cisco Catalyst 6509-NEB-A Switch</name>
<sysobjectid>1.3.6.1.4.1.9.1.534</sysobjectid>
</device-type>
<device-type>
<name>Cisco Catalyst 6506 Switch</name>
<sysobjectid>1.3.6.1.4.1.9.1.282</sysobjectid>
</device-type>
<device-type>
<name>Cisco Catalyst 6509-NEB Switch</name>
<sysobjectid>1.3.6.1.4.1.9.1.310</sysobjectid>
</device-type>
<device-type>
<name>Cisco Catalyst 6509 Switch</name>
<sysobjectid>1.3.6.1.4.1.9.1.283</sysobjectid>
</device-type>
<device-type>
<name>Cisco Catalyst 6504-E Switch</name>
<sysobjectid>1.3.6.1.4.1.9.1.657</sysobjectid>
</device-type>
<device-type>
<name>Cisco Catalyst 6509-V-E Switch</name>
<sysobjectid>1.3.6.1.4.1.9.1.832</sysobjectid>
</device-type>
<device-type>
<name>Cisco Catalyst 6500 Series SSL Services Module</name>
<sysobjectid>1.3.6.1.4.1.9.1.554</sysobjectid>
</device-type>
<device-type>
<name>Cisco Catalyst 6503 Switch</name>
<sysobjectid>1.3.6.1.4.1.9.1.449</sysobjectid>
</device-type>
</min-supported-imageversion>
</family>
<device-filtering-details>
<cli name="identity">
<clicommand>
<![CDATA[
    aaa server radius dynamic-author
    client ${ipaddress}
    server-key ${server-key}
    port ${port}
    auth-type ${authtype}
]]>
</clicommand>
</cli>
</config>
Sample Template for IF Statement

The section shows the template for IF statement:

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<ootb-template>

- <!-- ****************************************************
- <!--          Copyright (c)2011 Cisco Systems, Inc.
- <!--          All rights reserved.
- <!-- ****************************************************
- <ootb-template>
- <template-metadata name="SGACL-NEXUS">
- <template-details>
  <description>This template is used to define Secure Group Access Lists (SGACL). In SGACLs, you can control the operations that users can perform based on assigned security groups. You can use Secure Group tags to modify security groups and introduce new privileges or restrict current permissions.</description>
  <task>TrustSec</task>
  <author>System</author>
  <template-version>1.0</template-version>
  <scope>Device</scope>
  <type>partial</type>
  <features>Secure Group Access</features>
  <tags>SGACL</tags>
  <pin>Access</pin>
  <hardware-platform>Nexus 7000</hardware-platform>
- </template-details>
- <parameter-metadata>
  - <param-group cliName="intcommands" isMandatory="true" name="SGACL-NEXUS">
    <div style="word-wrap: break-word">
      Notes:
      <ul>
        <li>SGT Value and DGT Value fields are mandatory if you have selected RBACL SGT Mapping as SGT Value and RBACL DGT Mapping as DGT Value respectively</li>
        <li>In the Secure Group Tag value field, you can enter only hexadecimal values ranging from 0x2 to 0xffef</li>
      </ul>
    </div>
  </param-group>
  - <parameter name="Vlanid">
    <description>Vlan ID [1-3967]</description>
    <html-component>textbox</html-component>
    <data-type>numeric</data-type>
    <mandatory>true</mandatory>
    <isGlobal>true</isGlobal>
    <help-description />
    <syntax>
      <min>1</min>
      <max>3967</max>
      <pattern />
    </syntax>
  </parameter>
  - <parameter name="vrfname">
    <description>VRF Name</description>
    <html-component>textbox</html-component>
    <data-type>string</data-type>
    <mandatory>true</mandatory>
    <isGlobal>true</isGlobal>
    <help-description />
    <syntax>
  </syntax>
</parameter-metadata>
</template-metadata>
</ootb-template>
```
- `<min />`  
- `<max />`  
- `<pattern />`  

```xml
</syntax>
</parameter>
- `<parameter name="Ipaddress"`  
  `<description>IP Address</description>`  
  `<html-component>textbox</html-component>`  
  `<data-type>string</data-type>`  
  `<mandatory>true</mandatory>`  
  `<isGlobal>true</isGlobal>`  
  `<help-description />
- `<syntax>`  
  `<min />`  
  `<max />`  
  `<pattern>(25[0-5]|2[0-4]\.[0-9]\.\.[0-9])\.(25[0-5]|2[0-4]\.[0-9]\.\.[0-9])\.(25[0-5]|2[0-4]\.[0-9]\.\.[0-9])\.(25[0-5]|2[0-4]\.[0-9]\.\.[0-9])</pattern>`  
  `</syntax>`
</parameter>
- `<parameter name="sgttag">`  
  `<description>Secure Group Tag Value[0x2-0xfffe]</description>`  
  `<html-component>textbox</html-component>`  
  `<data-type>String</data-type>`  
  `<mandatory>true</mandatory>`  
  `<isGlobal>true</isGlobal>`  
  `<help-description />
- `<syntax>`  
  `<min />`  
  `<max />`  
  `<pattern />`  
  `</syntax>`
</parameter>
- `<parameter name="sgtip">`  
  `<description>Secure Group Tag of IP Address[1-65519]</description>`  
  `<html-component>textbox</html-component>`  
  `<data-type>numeric</data-type>`  
  `<mandatory>true</mandatory>`  
  `<isGlobal>true</isGlobal>`  
  `<help-description />
- `<syntax>`  
  `<min>1</min>`  
  `<max>65519</max>`  
  `<pattern />`  
  `</syntax>`
</parameter>
- `<parameter name="RGACLname">`  
  `<description>RGACL Name</description>`  
  `<html-component>textbox</html-component>`  
  `<data-type>string</data-type>`  
  `<mandatory>true</mandatory>`  
  `<isGlobal>true</isGlobal>`  
  `<help-description />
- `<syntax>`  
  `<min />`  
  `<max />`  
  `<pattern />`  
  `</syntax>`
</parameter>
- `<parameter name="RGACLmode">`  
  `<description>Mode</description>`  
  `<html-component>select</html-component>`  
  `<default-value label="Deny packet forwarding">deny</default-value>`  
  `<default-value label="Permit packet forwarding">permit</default-value>`
Appendix B  Config Template XML Schema

Sample Template for IF Statement

<data-type>string</data-type>
<mandatory>true</mandatory>
<isGlobal>true</isGlobal>
<help-description/>
- <syntax>
  <min/>
  <max/>
  <pattern/>
</syntax>
</parameter>
- <parameter name="UDPportparameters">
  <description>UDP Port Parameters</description>
  <html-component>select</html-component>
  <default-value label="Destination port parameters">dst</default-value>
  <default-value label="Source port parameters">src</default-value>
  <data-type>string</data-type>
  <mandatory>true</mandatory>
  <isGlobal>true</isGlobal>
  <help-description/>
  - <syntax>
    <min/>
    <max/>
    <pattern/>
  </syntax>
</parameter>
- <parameter name="UDPparametermatching">
  <description>UDP Parameter Matching</description>
  <html-component>select</html-component>
  <default-value label="Match packets on the given port number">eq</default-value>
  <default-value label="Match packets on port number greater than the given port number">gt</default-value>
  <default-value label="Match packets on port number less than the given port number">lt</default-value>
  <default-value label="Match packets not on the given port number">neg</default-value>
  <data-type>string</data-type>
  <mandatory>true</mandatory>
  <isGlobal>true</isGlobal>
  <help-description/>
  - <syntax>
    <min/>
    <max/>
    <pattern/>
  </syntax>
</parameter>
- <parameter name="portnumber">
  <description>Port Number[0-65535]</description>
  <html-component>textbox</html-component>
  <data-type>numeric</data-type>
  <mandatory>true</mandatory>
  <isGlobal>true</isGlobal>
  <help-description/>
  - <syntax>
    <min>0</min>
    <max>65535</max>
    <pattern/>
  </syntax>
</parameter>
- <parameter name="RBACLSGT">
  <description>RBACL Secure Group Tag Mapping</description>
  <html-component>select</html-component>
  <default-value label="SGT Value">sgtvalue</default-value>
  <default-value label="Any">any</default-value>
  <data-type>string</data-type>
  <mandatory>true</mandatory>
  <isGlobal>true</isGlobal>
  <help-description/>
  - <syntax>
    <min/>
    <max/>
    <pattern/>
  </syntax>
</parameter>
<default-value label="Unknown">unknown</default-value>
<data-type>string</data-type>
<mandatory>true</mandatory>
<isGlobal>true</isGlobal>
<help-description />
</parameter>
  - <parameter name="sgtvalues">
    <description>Secure Group Tag Value[0-65519]</description>
    <html-component>textbox</html-component>
    <data-type>numeric</data-type>
    <mandatory>false</mandatory>
    <isGlobal>true</isGlobal>
    <help-description />
    - <syntax>
      <min>0</min>
      <max>65519</max>
    </syntax>
  </parameter>
  - <parameter name="RBACLDGT">
    <description>RBACL Destination Group Tag Mapping</description>
    <html-component>select</html-component>
    <default-value label="DGT Value">dgtvalue</default-value>
    <default-value label="Unknown">unknown</default-value>
    <data-type>string</data-type>
    <mandatory>true</mandatory>
    <isGlobal>true</isGlobal>
    <help-description />
    - <syntax>
      <min /> 
      <max /> 
      <pattern /> 
    </syntax>
  </parameter>
  - <parameter name="dgtvalues">
    <description>Destination Group Tag Value[0-65519]</description>
    <html-component>textbox</html-component>
    <data-type>numeric</data-type>
    <mandatory>false</mandatory>
    <isGlobal>true</isGlobal>
    <help-description />
    - <syntax>
      <min>0</min>
      <max>65519</max>
    </syntax>
  </parameter>
</param-group>
</parameter-metadata>
</template-metadata>
- <config platform="Nexus">
  - <device-filtering-details>
    - <family value="Data Center Switches">
      <min-supported-imageversion value="NX-OS 5.0.2">
        - <device-type>
          <name>Cisco Nexus 7000 10-Slot Switch</name>
          <sysobjectid>1.3.6.1.4.1.9.1.2.3.1.3.612</sysobjectid>
        </device-type>
      </device-type>
    </family>
  </device-filtering-details>
</config>
<name>Cisco Nexus 7000 18-Slot Switch</name>
<sysobjectid>1.3.6.1.4.1.9.12.3.1.3.777</sysobjectid>
</device-type>

- <device-type>
  <name>Cisco Nexus 7000 9-Slot Switch</name>
  <sysobjectid>1.3.6.1.4.1.9.12.3.1.3.932</sysobjectid>
</device-type>
</min-supported-imageversion>
</family>

<device-filtering-details>
  <cliname="intcommands">
  <clicommand>
  vlan ${Vlanid} cts role-based enforcement exit vrf context ${vrfname} cts role-based sgt-map
  exit cts role-based access-list ${RGACLname} ${RGACLmode} udp
  sgt-map
  exit cts role-based access-list ${RGACLname} ${RGACLmode} udp
  sgt-map
  access-list ${RGACLname} #elseif(${RBACLDGT} eq "dgtvalue")
  sgt-map
  access-list ${RGACLname} #elseif(${RBACLDGT} eq "dgtvalue")
  sgt-map
  access-list ${RGACLname} #else
  sgt-map
  access-list ${RGACLname} #endif</clicommand>
</cliname>
</config>
</ootb-template>
Troubleshooting Tips and FAQs

This appendix covers the Troubleshooting tips and FAQs for:

- Configuration Archive
- NetConfig
- Config Editor
- Software Management
- Job Approval
- cwcli config
- cwcli export
- VRF Lite

For Installation related FAQs and Troubleshooting tips, see the *Installing and Migrating to Cisco Prime LAN Management Solution 4.2*.

Configuration Archive

This section provides the troubleshooting information and FAQs for Configuration Archive:

- Configuration Archive FAQs
- Troubleshooting Configuration Archive

This section contains:

- Login Authentication in Telnet Mode
- Login Authentication in SSH Mode
- Enable Login Authentication in Telnet Mode
- Enable Login Authentication in SSH Mode
Configuration Archive FAQs

- Q. Can I define the protocol order for configuration fetch and deploy?
- Why does the Telnet session appear in the data capture trace although I have selected TFTP as the configuration transport protocol?
- Q. How Configuration Management interprets device credentials?
- Q. What are the supported device prompts?

Q. Can I define the protocol order for configuration fetch and deploy?
A. Yes, you can define the order of protocol that has to be used for Configuration Management applications (Configuration Archive, Config Editor, and NetConfig). You can define this in the Transport Settings window (Admin > Collection Settings > Config > Config Transport Settings).

Q. When I select:
   a. TFTP alone as the configuration transport protocol
   b. Run Sync Archive Job for a device
   c. Run a data capture trace
The data capture trace shows Telnet traffic along with SNMP/TFTP sessions.

Q. Why does the Telnet session appear in the data capture trace although I have selected TFTP as the configuration transport protocol?
A. The Telnet session that appears in the data capture trace is a socket connection to the Telnet port. It identifies the IP address of the Cisco Prime LMS server. This is important in multi-homed servers where the IP address that Cisco Prime server uses to contact the device, has to be identified.

Q. How Configuration Management interprets device credentials?
A. You can enter the device credentials when you,
   • Add/import devices using the LMS Device Management option (Inventory > Device Administration > Add / Import / Manage Devices). In this flow, you can enter:
     – Primary Username—User name for the device.
     – Primary Password—Password for the device.
     – Primary Enable Password—Console-enabled password for the device.
   • If you have enabled Enable Job Password option (Admin > Network > Configuration Job Settings > Config Job Policies) then while scheduling for a job, you can enter these credentials:
     – Login User name—User name for the device.
     – Login Password—Password for the device.
     – Enable Password—Console-enabled password for the device.

These credentials are used while running the job. The credentials that you have entered in the Device and Credential Repository are ignored while running the job.

TACACS (Terminal Access Controller Access Control System) uses a separate centralized server to track usernames and passwords. This simplifies authentication and authorization, because information is maintained in only one database rather than being spread out over many devices.

If your devices are configured to use TACACS, you must provide TACACS device credentials when you add or import the devices.
Login Authentication in Telnet Mode

When LMS logs into non-privileged mode (User mode), depending on your device authentication configuration, the device will prompt for either username and password, or password only.

If the device prompts for username and password, LMS responds with the following:

- If Primary Username and Primary Password credentials are entered in the Device and Credential Repository, LMS sends Primary Username and Primary Password to the device.

  If you have enabled Enable Job Password option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (Inventory > Device Administration > Add / Import / Manage Devices) is ignored.

- If:
  - Authentication fails with the Primary credentials or Login User name and Login Password
  - Or
  - The Primary credentials or Login User name and Login Password are not present in the database.

  LMS reports the login as failure.

If the device prompts for password only, LMS responds with the following:

- If Primary Password is entered in the database, LMS sends Primary Password to the device.

  If you have enabled Enable Job Password option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (Inventory > Device Administration > Add / Import / Manage Devices) is ignored.

  If you have configured only the Telnet password (without configuring username) on your device. You have to enter a string in the Login Username field. That is, you cannot leave the Login Username field blank.

  The Login Username string will be ignored while connecting to the device as the device is configured only for the Telnet password.

- If:
  - Authentication fails with the Primary Password or Login Password
  - Or
  - The Primary Password or Login Password is not present in the database.

  LMS reports the login as failure.

Login Authentication in SSH Mode

This section describes how the device credentials are interpreted by LMS in SSH mode.

Open an SSH session to the device.

The device prompts for username and password, LMS responds with the following:

- If Primary Username and Primary Password are entered in the database, LMS sends Primary Username and Primary Password to the device.
If you have enabled Enable Job Password option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (Inventory > Device Administration > Add / Import / Manage Devices) is ignored.

- If:
  - Authentication fails with the Primary credentials or Login User name and Login Password
  Or
  - The Primary credentials or Login User name and Login Password are not present in the database
  LMS reports the login as failure.

**Enable Login Authentication in Telnet Mode**

This section describes how the TACACS and other credentials are interpreted by LMS in Telnet mode.

Logging into the Privileged mode (Enable mode) involves two steps:

1. LMS logs into non-privileged mode (See Login Authentication in Telnet Mode).
2. If logging into non-privileged mode is successful, LMS issues “enable” command for the device to enter into privileged mode.

If the device prompts for password, LMS responds with the following:

- If Primary Enable password is entered in the database, LMS sends Enable Primary password to the device.

  If you have enabled Enable Job Password option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (Inventory > Device Administration > Add / Import / Manage Devices) is ignored.

- If authentication fails or Enable Password or Primary Enable Password is not present in database
  or
- If logging into non-privileged mode fails or authentication fails in all above cases.
  LMS reports the login as failure.

**Enable Login Authentication in SSH Mode**

This section describes how the TACACS and other credentials are interpreted by LMS in SSH mode.

Logging into the Privileged mode (Enable mode) involves two steps:

1. LMS logs into non-privileged mode (See Login Authentication in SSH Mode).
2. If logging into non-privileged mode is successful, LMS issues the `enable` command for the device to enter into privileged mode.

If the device prompts for password, LMS responds with the following:

- If Primary Enable Password is entered in the database, LMS sends Primary Enable password to the device.
Configuration Archive

If you have enabled Enable Job Password option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (Inventory > Device Administration > Add / Import / Manage Devices) is ignored.

- If authentication fails or Enable Password or Primary Enable Password is not present in database
  
or
  
- If logging into non-privileged mode fails or authentication fails in all above cases. LMS reports the login as failure.

Q. What are the supported device prompts?

A. The supported device prompts are:

The supported Device authentication prompts are:

- Routers
  
  “Username:”, “Username:
  
  “Password:”, “Password:

- Switches
  
  “username:”, “Username:
  
  “password:”, “Password:

- Cisco Interfaces and Modules — Network Analysis Modules
  
  “login:”
  
  “Password:” “password:”

- Security and VPN — PIX
  
  “username:”, “Username:
  
  “passwd:”, “password:”, “Password:

- Content Networking—Content Service Switch
  
  
  “Password:”, “password:”, “passwd:”, “Password:”, “password:”, “passwd:”

- Content Networking — Content Engine
  
  “Username:”, “login:”
  
  “Password:”

- Storage Networking — MDS Devices
  
  “Username:”, “Username:
  
  “Password:”, “Password:”
## Troubleshooting Configuration Archive

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM0003</td>
<td>Version $1 does not exist in archive $2</td>
<td>Version may have been deleted</td>
<td>None</td>
</tr>
<tr>
<td>CM0005</td>
<td>Archive does not exist for $1</td>
<td>Error during archive creation.</td>
<td>Check the file system/user privileges.</td>
</tr>
<tr>
<td>CM0006</td>
<td>Archives do not exist</td>
<td>Error during archive creation.</td>
<td>Check the file system/user privileges.</td>
</tr>
<tr>
<td>CM0008</td>
<td>Checkout not permitted on archive $1</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0010</td>
<td>Checkin not permitted on archive $1</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0011</td>
<td>Delete not permitted</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0012</td>
<td>Could not create new version on archive $1</td>
<td>Insufficient disk space or config file may be incomplete.</td>
<td>Check whether disk space is available and that the directory has required permissions</td>
</tr>
<tr>
<td>CM0013</td>
<td>Cannot delete version on archive $1</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0015</td>
<td>Could not check out config for archive $1</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0016</td>
<td>Could not undo check out config for archive $1</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0017</td>
<td>Could not check in config for archive $1</td>
<td>$2</td>
<td>Check whether the file system is full and if you have required permissions.</td>
</tr>
<tr>
<td>CM0021</td>
<td>Version does not exist in archive $1</td>
<td>Version may have been deleted</td>
<td>None</td>
</tr>
<tr>
<td>CM0022</td>
<td>Archive already exists</td>
<td>Archive names should be unique</td>
<td>Enter a different name</td>
</tr>
<tr>
<td>CM0023</td>
<td>Archive creation not permitted</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0024</td>
<td>Error while deleting archive</td>
<td>You may not have the required permission</td>
<td>Check with the administrator for your privilege.</td>
</tr>
<tr>
<td>CM0025</td>
<td>Cannot delete device archive</td>
<td>Only the system purge can delete the device archive</td>
<td>Schedule for a purge job.</td>
</tr>
</tbody>
</table>
| CM0026     | Archive Relocation failed                          | The destination folder may not have the required disk space or required permission. | • Check if the destination folder has the required permission  
  • Check if the disk space is available  
  • Check if the user has the write permission. |
<p>| CM0034     | Cannot list versions for $1                        | You may not have the required permission or version do not exist. | Check with the administrator for your privilege.    |
| CM0037     | Database Connection Error                          | Database Engine may be down                       | Restart the RMEDbMonitor and CmfDbMonitor services. |</p>
<table>
<thead>
<tr>
<th>Message ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM0038</td>
<td>Error in Database</td>
<td>Database Engine may be down</td>
<td>Restart the RMEDbMonitor and CmfDbMonitor services</td>
</tr>
</tbody>
</table>
| CM0040     | Error while reading the file from the system | Either:  
  - The file may not exist  
  Or  
  - You may not have required permissions. | Verify whether you have the correct privileges and that the file system is not corrupted. |
| CM0041     | Error while writing the file to the system | Either:  
  - The file may not exist  
  Or  
  - You may not have required permissions. | Verify whether you have the correct privileges and that the file system is not full |
| CM0043     | Error while copying the file | Either:  
  - The source or destination file may not exist  
  Or  
  - You may not have required permissions. | Verify whether:  
  - The files exist  
  - The file system is not full.  
  - You have permission |
| CM0050     | Cannot compare the configurations since they are not of the same type. | Configuration types are different | Select device of the same type. |
| CM0051     | Cannot connect to ConfigMgmtSever process | Process may be down or maximum connection have been reached. | Restart the ConfigMgmtSever process. |
| CM0054     | Error while initializing Transport for $1 | Device packages may not exist. | Check whether:  
  - The user exists in LMS and has required permissions,  
  - Device is reachable  
  - Required device packages are available in LMS. |
<p>| CM0076     | Job creation failed | $1 | Check whether Jrm and CTMJrmServer processes are running |
| CM0077     | Job modification failed | $1 | Check whether Jrm and CTMJrmServer processes are running |
| CM0080     | Could not send e-mail. | The e-mail configuration in your profile may be either missing or incorrect | Check e-mail configuration. |
| CM0082     | Job execution failed. | The job policy may not be enabled | Enable the policy and try again |
| CM0085     | Cannot list jobs of type | Jobs of this type may not exist in LMS. | Enable the policy and try again. |</p>
<table>
<thead>
<tr>
<th>Message ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM0086</td>
<td>Cannot load job with id.</td>
<td>Job may not exist in LMS</td>
<td>Verify that the Job ID exists and try again</td>
</tr>
<tr>
<td>CM0087</td>
<td>Cannot obtain lock on device</td>
<td>Another application/job may have locked the device.</td>
<td>Verify that there are no other jobs is running on the device. Retry the job after some time.</td>
</tr>
<tr>
<td>CM0088</td>
<td>Configuration archival failed for $1</td>
<td>Not enough disk space.</td>
<td>Check whether the device is reachable and that the credentials are correct.</td>
</tr>
<tr>
<td>CM0090</td>
<td>Reload task failed on device</td>
<td>Device may not be reachable.</td>
<td>Check whether the device is reachable and that the credentials are correct.</td>
</tr>
<tr>
<td>CM0096</td>
<td>Job ID is not valid</td>
<td>The job may not exist in LMS</td>
<td>Verify that the job exists and try again.</td>
</tr>
<tr>
<td>CM0097</td>
<td>No failed devices in the job</td>
<td>There may not be any failed devices in the job.</td>
<td>Check for failed devices and try again.</td>
</tr>
<tr>
<td>CM0098</td>
<td>Invalid Job-based password specified</td>
<td>The Job-based password data may be null or cannot be used.</td>
<td>Enter the correct Job-based password and try again.</td>
</tr>
<tr>
<td>CM0109</td>
<td>Cannot read admin preferences.</td>
<td>Application may not have been initialized correctly</td>
<td>Retry the task</td>
</tr>
<tr>
<td>CM0122</td>
<td>No commands to write.</td>
<td>Command may not be available</td>
<td>Verify whether there are any commands to deploy</td>
</tr>
<tr>
<td>CM0123</td>
<td>Exception while getting all baseline templates.</td>
<td>Templates may have been deleted</td>
<td>Check if the template exist.</td>
</tr>
<tr>
<td>CM0125</td>
<td>Cannot persist template.</td>
<td>Template may be empty or invalid.</td>
<td>Check whether the commands are valid</td>
</tr>
<tr>
<td>CM0126</td>
<td>Cannot find baseline archive $1</td>
<td>Archive may have been deleted</td>
<td>Check if the archive exist.</td>
</tr>
<tr>
<td>CM0128</td>
<td>Cannot get baseline branch.</td>
<td>Branch may not exist.</td>
<td>Check if the branch exist.</td>
</tr>
<tr>
<td>CM0131</td>
<td>Cannot find template</td>
<td>Template may have been deleted</td>
<td>Check if the template exist.</td>
</tr>
<tr>
<td>CM0132</td>
<td>Cannot find result for job</td>
<td>Job may not exist.</td>
<td>Check if the job has been deleted.</td>
</tr>
<tr>
<td>CM0133</td>
<td>Invalid check-type for command</td>
<td>Check type may be invalid</td>
<td>Verify if the check-type is valid.</td>
</tr>
<tr>
<td>CM0136</td>
<td>Regular expression match failed.</td>
<td>Not a valid Regular expression.</td>
<td>Check if the expression is valid.</td>
</tr>
<tr>
<td>CM0137</td>
<td>No commandlets.</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>CM0138</td>
<td>Cannot find result for device</td>
<td>Device has been deleted.</td>
<td>Check if the device exist.</td>
</tr>
<tr>
<td>CM0139</td>
<td>Could not archive configuration</td>
<td>File system may be full or user may not have the required permission.</td>
<td>Check whether device is reachable and device credentials are correct. Increase timeout value, if required.</td>
</tr>
<tr>
<td>CM0148</td>
<td>User or device authorization failed.</td>
<td>User may not exist or does not have privileges to operate on any or all of the devices in the job.</td>
<td>Check whether the user exists and has required privileges to execute jobs.</td>
</tr>
<tr>
<td>CM0201</td>
<td>Could not start the SdiEngine.</td>
<td>The package path may be incorrect</td>
<td>Check whether the specified package path is correct</td>
</tr>
</tbody>
</table>
## NetConfig FAQs

Q. What are the supported protocols for NetConfig Reload task?

Q. What are the supported protocols for NetConfig Reload task?

A. The supported protocols for NetConfig Reload task are Telnet, SSH and TFTP. SSH and TFTP protocols are supported by NetConfig Reload task only if these protocols are also supported by the devices.
# Troubleshooting NetConfig

This section provides the troubleshooting information for the NetConfig application:

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG0025</td>
<td>Cannot retry.</td>
<td>Retry is not supported on periodic jobs.</td>
<td>None.</td>
</tr>
<tr>
<td>CFG0026</td>
<td>You can retry only failed jobs.</td>
<td>A Successful job has been selected instead of a Failed job.</td>
<td>Select a Failed job and try again.</td>
</tr>
<tr>
<td>CFG0029</td>
<td>Job approval is enabled.</td>
<td>You have scheduled a job that requires Job approval with the Immediate schedule type. The job will run only when it has been approved by the Approver.</td>
<td>Do not select Immediate job type while scheduling the job.</td>
</tr>
<tr>
<td>CFG0009</td>
<td>Error occured while processing.</td>
<td>Check netconfigclient.log for more details.</td>
<td>Retry the operation. If the problem persists, send the logs to Cisco Technical Assistance Center (TAC). The netconfig logs are available at this location: On Windows: NMSROOT\log\netconfigclient.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/netconfigclient.log</td>
</tr>
<tr>
<td>CFG0029</td>
<td>Job approval is enabled.</td>
<td>This job requires job approval. So it can run only when the job is approved. So you cannot schedule a job with immediate schedule type.</td>
<td>Do not select Immediate schedule type.</td>
</tr>
<tr>
<td>CFG0041</td>
<td>You have selected an instance that does not have a task associated with it.</td>
<td>None.</td>
<td>Select an instance that has an associated task.</td>
</tr>
</tbody>
</table>
# Config Editor

This section provides the troubleshooting information for the Config Editor application:

<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEDT0001</td>
<td>No device selected</td>
<td>You have not selected a device.</td>
<td>Select a device and try again.</td>
</tr>
<tr>
<td>CEDT0002</td>
<td>There is no configuration file for the device.</td>
<td>There is no configuration file for the selected device in the archive.</td>
<td>Perform Synch Archive to get the configuration file for the device.</td>
</tr>
<tr>
<td>CEDT0003</td>
<td>Modified Config not selected.</td>
<td>You have not selected a modified configuration from the Modified Configs list.</td>
<td>Select a configuration file from Modified Configs list.</td>
</tr>
<tr>
<td>CEDT0004</td>
<td>No Config Selected for Download.</td>
<td>You have not selected a configuration file for downloading either from the archive or from Modified Configs list.</td>
<td>Select a configuration file for downloading either from the archive or the Modified Configs list.</td>
</tr>
<tr>
<td>CEDT0005</td>
<td>Enter job description.</td>
<td>You have not entered a job description while creating a job.</td>
<td>Enter the job description. This is mandatory.</td>
</tr>
<tr>
<td>CEDT0007</td>
<td>No job selected.</td>
<td>You have not selected a job.</td>
<td>Select a job</td>
</tr>
<tr>
<td>CEDT0009</td>
<td>Job {JobId} cannot be {Action}</td>
<td>You have tried to do any of the following:</td>
<td>User should select the appropriate job and appropriate action.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Edit a completed job</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Copy an incomplete job</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Stop a completed job</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Stop an already stopped job.</td>
<td></td>
</tr>
<tr>
<td>CEDT0010</td>
<td>Cannot get details for Job {JobID}.</td>
<td>The Job was recorded incorrectly.</td>
<td>None.</td>
</tr>
<tr>
<td>CEDT0011</td>
<td>Could not get the summary of the job.</td>
<td>None</td>
<td>Check Cfgedit.log for more details.</td>
</tr>
<tr>
<td>CEDT0012</td>
<td>Job not found.</td>
<td>None</td>
<td>Check Cfgedit.log for more details.</td>
</tr>
<tr>
<td>CEDT0013</td>
<td>Some change in Jsp leading to incompatible with Action class.</td>
<td>None.</td>
<td>Check cfgedit.log for more details.</td>
</tr>
<tr>
<td>CEDT0014</td>
<td>Label not selected for search</td>
<td>You have tried to search labeled configurations without selecting a label.</td>
<td>Select a label from the drop down.</td>
</tr>
<tr>
<td>CEDT0015</td>
<td>Cannot open configuration file.</td>
<td>None.</td>
<td>Check Cfgedit.log for more details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contact Cisco TAC with log details for further assistance.</td>
<td></td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CEDT0016</td>
<td>Cannot open Baseline Template.</td>
<td>Template may be deleted</td>
<td>Check whether the template exists.</td>
</tr>
<tr>
<td>CEDT0017</td>
<td>Baseline Templates not present for the selected device.</td>
<td>There are no templates for the selected device type.</td>
<td>Create a Baseline Template for the selected device type from the archive.</td>
</tr>
<tr>
<td>CEDT0018</td>
<td>No Config found for the specified search pattern</td>
<td>The pattern you have entered cannot be found in any of the configs</td>
<td>Change the search pattern.</td>
</tr>
<tr>
<td>CEDT0019</td>
<td>External Config to be opened not selected</td>
<td>You have not selected an External Config.</td>
<td>Select the External Config File from the browser.</td>
</tr>
<tr>
<td>CEDT0021</td>
<td>Version to be opened not selected.</td>
<td>None.</td>
<td>Select a valid version</td>
</tr>
<tr>
<td>CEDT0022</td>
<td>Cannot load query. Check whether the query exists</td>
<td>The query you selected may have been deleted.</td>
<td>Use Configuration &gt; Configuration Archive &gt; Views &gt; Custom Queries to check whether the query exists. Create a query if it does not exist.</td>
</tr>
<tr>
<td>CEDT0023</td>
<td>Cannot find query. Check whether the query exists</td>
<td>The query you selected may have been deleted.</td>
<td>Use Configuration &gt; Configuration Archive &gt; Views &gt; Search Archive&gt; to check whether the query exists. Create a query if it does not exist.</td>
</tr>
<tr>
<td>CEDT0024</td>
<td>No External Syntax Checker is registered with CMIC.</td>
<td>Either:</td>
<td>Register the syntax checker tool correctly with CMIC before Launching External Syntax checker.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You may have launched the External Syntax checker without registering the syntax checker tool with CMIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The syntax checker is not registered correctly with CMIC.</td>
<td></td>
</tr>
<tr>
<td>CEDT0025</td>
<td>Syntax Checking functionality is not supported by this device image.</td>
<td>The device image you have selected does not support Syntax Checking functionality.</td>
<td>Select another device image that supports Syntax Checking functionality.</td>
</tr>
<tr>
<td>CEDT0029</td>
<td>One or more of the devices selected are already added to this job.</td>
<td>A config for the device has already been added</td>
<td>Only one config can be downloaded to a device in a Job.</td>
</tr>
<tr>
<td>CEDT0030</td>
<td>No configuration file exists for the device</td>
<td>There is no configuration file for the selected device in the archive.</td>
<td>Perform Synch Archive to get the configuration file for the device</td>
</tr>
<tr>
<td>CEDT0031</td>
<td>There are no commands to download.</td>
<td>None.</td>
<td>Remove the device from job and try again.</td>
</tr>
</tbody>
</table>
Appendix C  Troubleshooting Tips and FAQs

Software Management

This section provides the troubleshooting information and FAQs for the Software Management applications:

- Software Management FAQs
- Troubleshooting Software Management

### Software Management FAQs

- Q. What are the high-level features of Software Management?
- Q. What privilege level is required to run Software Management functions?
- Q. How do I know which functions I can access in Software Management?
- Q. Are there DNS dependencies for Remote Copy Protocol (RCP) to work properly for a device?
- Q. Can I use Remote Copy Protocol (RCP) to transfer images to devices?
- Q. What connection mechanism does Software Management use to upgrade software?
- Q. What is the default Simple Network Management Protocol (SNMP) timeout used by Software Management? Can I configure it?
- Q. Can I configure TACACS or Radius authentication for devices that Software Management has upgraded?
- Q. Can I configure default privileges on terminal lines for Cisco IOS devices that Software Management has upgraded?
- Q. What is Job Approval?
- Q. What is the approver list?
- Q. Is the Job Approval policy enforced system-wide?
- Q. How do I configure Job Approval for Software Management?

#### Message-ID | Error Message | Probable Cause | Possible Action
---|---|---|---
CEDT0032 | Approval is enabled. Cannot schedule immediate jobs. | You cannot schedule Immediate jobs if Approval is enabled. | Select Schedule type, Once instead of Immediate
CEDT0033 | Selected Job Execution date is invalid. | You have selected a past date for running a job. | Select a valid future date.
CEDIT0034 | Job user name or password not entered. | You have enabled the Job based password option but not entered password. | Either:
  - Deselect the Job-based password option
  - Enter the user name and password fields.
CEDT0039 | Enter at least one pattern. | You have not entered any search patterns. | Either:
  - Select one of the queries listed
  - Enter a search pattern.
Appendix C  Troubleshooting Tips and FAQs

Software Management

• Q. Which Cisco IOS devices support bootldr images?
• Q. How do you identify bootldr image files?
• Q. How does the Software Management bootldr recommendation process work?
• Q. Where is the storage location of the bootldr image on the Cisco IOS device?
• Q. Does Software Management erase Bootflash if there is not enough free space on Bootflash?
• Q. Does Software Management change the configuration file for bootldr upgrades?
• Q. Can Software Management back up the current bootldr image while Software Management runs the Distribute Images job?
• Q. Does Software Management recommend bootldr images from Cisco.com in the Distribute Images function?
• Q. Can I upgrade modules on the device using advanced Distribution mode?
• Q. What image extension type are not supported in Software Management?
• Q. How can secured image upgrades be performed using Software Management?
• Q. How to use Reboot order configuration feature?
• Q. Is Image import from URL is treated as separate Job?
• Q. What is the best effort verification performed while distributing the image using Advance mode?
• Q. When does Software Management Application use SSH?
• Q. How can a protocol be Enabled/Disabled for a job?
• Q. How are devices upgraded using Secured Copy Protocol?
• Q. How much Disk space should be available while performing parallel image upgrade to large number of devices (more than 100)?
• Q. What is the swap file size required for Software Management application?
• Q. What Version of SCP is supported in Software Management application?
• Q. What are the pre requisites for using SCP for image upgrade?
• Q. Why is the job still running after I cancel it?
• Q. Why do I get an error message such as, Navigation to other areas of this application is not available until the opened wizard is finished or canceled?
• Q. The Cisco.com profile window is sometimes filled with user and password and sometimes not. Why?
• Q. I am not able to select both sequential execution and sequential reboot at 'Schedule Job' step during distribution?
• Q. During Distribution by Advance flow, I get “Software Management application could not verify the flash inputs since there was no flash information available. Edit the expert input file and verify once again. If you do not edit the expert input file, you can continue with the task by clicking Next. However, the results may be inaccurate.”?
• Q. Why am I not able to see “Immediate” during software management jobs?
• A. Check if approval is enabled. If approval is enabled for Software Mgmt Jobs, you will not be able to schedule Immediate job.
• Q. I am not able to select the device (greyed box) at Software Management device selector page, but I'm able to select at inventory.
- Q. I am not able to select a user script which is in xxx path.
- Q. In ACS login mode, I'm not able to see links that I usually get to see.
- Q. In the Job Details Window (clicking on job ID in the Software Management Job Browser) I don't see the job status being updated.
- Q. What Validations are performed by Software Management before actual image distribution onto the device?
- Q. What is the minimum software version required to be running on the device for Software Management to upgrade the software?
- Q. Can I have a different script for each device in a job?
- Q. What device types can be used as remote stage device?
- Q. What device types cannot be upgraded using remote stage flow?
- Q. What are the pre-requisites for using the device as remote stage?
- Q. What Configuration changes are performed by Software Management on the remote stage device?
- Q. If I use the device as remote stage device does it impact the device's other functionalities? or what are the performance implications of using the device as remote stage device?
- Q. Are there any Bad version of IOS for Remote stage device?
- Q. Can I perform module upgrade (like Bootloader/mica/microcom etc.) using remote stage flow?
- Q. How many devices in a job can be upgraded using remote stage?
- Q. Can I perform Parallel upgrade using remote stage flow?
- Q. Can I perform Slam dunk upgrade using the remote stage?
- Q. What is the difference between Run-from-RAM and Run-from-Flash devices?
- Q. When does Software Management use the remote copy protocol (rcp) to transfer images?
- Q. How does Software Management ensure that file corruption does not occur during transfer?
- Q. After an upgrade, why does Software Management sometimes leave behind image files in the tftpboot directory?
- Q. How much temporary space do you need during image distribution?
- Q. Is Cisco.com connection mandatory for Software Management?
  A. Cisco.com connection is not mandatory for using basic Software Management functionality. Image distribution, library management, tracking software upgrade changes, and other functions can run without Cisco.com connectivity.
- Q. How does Software Management handle proxy environments?
- Q. Does Software Management support proxy with user authentication environments?
- Q. Why is the Cisco.com filter option on the Software Management Edit Preferences screen not provided for Catalyst or Cisco 700 Series images?
- Q. How come the Cisco.com filter option does not work in LS1010 devices?
- Q. Can I configure Software Management to retrieve images from a Cisco.com mirror site rather than the main Cisco.com site?
- Q. Why I cannot download crypto images?
- Q. How does Software Management verify the integrity of the images after importing them from Cisco.com?
Appendix C  Troubleshooting Tips and FAQs

Software Management

- Q. Why does the Flash size displayed in the Add Image to Repository (Source:Cisco.com) function not match the actual size for some Cisco IOS devices?
- Q. What is a Dual Flash Bank device?
- Q. Does Software Management support software upgrades on dual RSP-based systems?
- Q. Why does Software Management require static IP routes or dynamic IP routing protocol for configuration for the upgrade of a run-from-Flash (RFF) partition on a Single Flash Bank (SFB) device?
- Q. Although the configuration of the Single Flash Bank (SFB) device includes an IP default gateway, why does Software Management not upgrade the device?
- Q. How do you change the IP default gateway configuration to allow Software Management to upgrade a device?
- Q. Why does Software Management require Cisco IOS Software Release 11.1 or later to run on a Single Flash Bank (SFB) device for an upgrade when you have configured the device with Frame Relay subinterfaces?
- Q. How is the job directory organized?
- Q. Which modem cards does Software Management support?
- Q. Which devices and software versions get support for the modem upgrades?
- Q. Which formats of Microcom firmware images does Software Management support?
- Q. Which format of Modem ISDN channel aggregation (MICA) portware do Cisco 3600 devices support?
- Q. Why does the Undo option not receive support for modem upgrades?
- Q. What connection mechanism does Software Management use for modem upgrades?
- Q. Does Software Management erase Flash for modem upgrades if there is not enough free space on Flash?
- Q. What is CIP?
- Q. Which devices support the Channel Interface Processor (CIP) microcode upgrade? What is the minimum software version necessary?
- Q. What is the minimum Channel Interface Processor (CIP) version that Software Management supports?
- Q. How can you import Channel Interface Processor (CIP) images to the Software Management library?
- Q. Is there support for the Undo option for Channel Interface Processor (CIP) upgrades?
- Q. What connection mechanism does Software Management use to upgrade Channel Interface Processor (CIP)?
- Q. Does Software Management change the configuration file for the Channel Interface Processor (CIP) upgrade?
- Q. Does Software Management support CIP2?
- Q. In which order does Software Management upgrade modules on a Cisco Catalyst 5500/5000 device?
- Q. Does the Supervisor Engine card reboot after the upgrade of all modules?
- Q. Does Software Management determine if the newly deployed Supervisor Engine software or module software is compatible with the module types (or module hardware versions)?
• Does Software Management support the upgrade of software on redundant Supervisor Engine card-based systems?
• Does Software Management update the configuration file on Cisco Catalyst 5500/5000 devices during the software upgrade?
• Does Software Management determine if the Supervisor Engine has the minimum required RAM to run a new image?
• Are there restrictions on the downgrade of the software on the Supervisor Engine card and other modules?
• Do you need to reconfigure the device when you downgrade the Supervisor Engine software?
• In the 4.1(1) software release and later, Supervisor Engine III cards allow the storage of configuration files on Flash cards. Does Software Management preserve the backed up configuration files on Flash during a software upgrade?
• Does Software Management allow you to upgrade epsboot images on Token Ring cards on Cisco Catalyst 5500/5000 devices?
• Why does the Add Image to Repository (Source: Cisco.com) task not display Token Ring LAN Emulation (LANE) or Permanent Virtual Circuit (PVC)-only ATM software images?
• How can I make the Image Recommendation faster?
• Why do the software version numbers that the show module command output displays from the Supervisor Engine command-line interface (CLI) and the version numbers that Software Management uses fail to match in some cases?
• Does Software Management recommend the right ATM image for your ATM module type?
• Should you use special images with Software Management for Cisco Catalyst 2900XL/3500XL devices?
• How does Software Management handle image import functionality of TAR and bin types of images for Catalyst 2900XL/3500XL devices?
• Why do software upgrades take longer on Cisco Catalyst 2900XL/3500XL devices?
• How do you upgrade Route Switch Module (RSM) and LightStream 1010 (LS1010) module software on Cisco Catalyst 5500/5000 and 6500/6000 series switches?
• Why does the Distribute Images task show all the images from Cisco.com for LightStream 1010 (LS1010) and Cisco Catalyst 8500 devices, even though you have configured Cisco.com filtering?
• What is the minimum version that Cisco 700 series ISDN routers support?
• What connection mechanism does Software Management use for Cisco 700 series upgrades?
• Both Cisco 760 and 770 series devices run the same image. Why do you see only some images with versions later than 4.0(1) for 770 series devices but see all images for 760 series devices?
• Why do you not see the option to reboot the device later on the Job Control page for Cisco 700 series routers?
• Why do you not see the option to modify the boot commands on the Job Control page for Cisco 700 series routers?
• Why does Software Management report download failures for some images even though the device runs the new image after the job completes?
• In which order does Software Management upgrade modules on a Catalyst 5000 device?
Software Management

- Q. Does Software Management check to see that the newly deployed Supervisor software or module software is compatible with the module types (or module hardware versions)?
- Q. Does Software Management support upgrading software on redundant Supervisor card-based systems?
- Q. What is the purpose of user scripts?
- Q. What if the user script crashes? Will it crash the Software Management job also?
- Q. When a Software Management job is scheduled, how is the baseline determined? When I distribute a job, is an automatic backup performed?
- Q. Can I set up a periodic download of Software Management images from Cisco.com?
- Q. Is browser timeout something I should consider when downloading?
- Q. What are crypto images?
- Q. How much temporary space is required during image distribution?
- Q. At what time will the images directory get created during the process of obtaining images from a device? Does this happen during the initial step?
- Q. How can I speed up Image Recommendation?
- Q. When a job is rejected, can it be edited or should I resubmit?
- Q. Can different group members edit jobs? What are the restrictions?
- Q. What is the role of the registry files?
- Q. How do I upgrade Network Analysis Module (NAM) using Software Management?
- Q. Can I change the job scheduled time?
- Q. How does Software Management handle the job status for an abnormally terminated job?
- Q. How does Software Management handle the job status of a pending job whose scheduled time has passed?
- Q. Why are some files left in the Software Management folder after Software Management has been uninstalled?
- Q. How can I enable or disable the SSH to Telnet fallback for Software Management jobs?
- Q. How can I export the images from SWIM repository to a local drive or a file system mounted to the LMS server?
- Q. Does Flash get erased if there is no sufficient space for Patch Distribution?
- Q. When I try to copy images, the Image Copy option fails indicating that the External TFTP server is inaccessible.
- Q. Can I specify the name of my input file as imagenames.txt when I try to export images using the Software Management (SWIM) CLI exportimages command?
- Q. I am getting timeout exception in cmdsvc (command service library) during a device connection/socket establishment. How do I change the default timeout and delays in cmdsvc?
Q. What are the high-level features of Software Management?

A. Software Management offers the following management functions:

• Software Distribution—Schedules download of software images to a single device or groups of devices. Hardware and firmware validation verifies whether the new image can run on the device. Image Upgrade can be performed in Sequential or in parallel. Also the In Parallel mode of upgrade device reboot can be controlled for the job.

  Provides several workflow to achieve this functionality
  – Distribute By Device [Basic]
  – Distribute [Advance]
  – Distribute by Image
  – Distribute by Remote Stage/External TFTP server
  – Patch Distribution

• Software Repository—Builds and maintains a library archive of software images. Software images can be added to repository from,
  – Device—Allows to archive the current software images on the device
  – Cisco.com—Integrates with Cisco Connection Online (Cisco.com) to download software images.
  – File System—Allows to import an image from a directory accessible from the LMS server
  – Network—Allows the library to synchronize with the software images running on the devices. A periodic job can generate a list of images that are not in the library. You then have the option to import new images into the library and check them for discrepancies between software images running on the network and images in the library.
  – URL—Allows to download images from URL you specify.

• Upgrade Analysis—Determines the hardware upgrades required on network devices to enable them to run new software. Software Management allows analysis based on the location of image to be analyzed. Following locations are supported.
  – Cisco.com
  – Local Repository

• Job Management
  – Job Approval — Allows organizations to require approvals before allowing software upgrades.
  – Software Management jobs can be operated upon to,
    Retry
    Undo
    Cancel
    Stop

• Reports
  – Work order—Displays changes that will be made to network devices as part of the software upgrade.
  – Synchronization report—Displays which Software Management-supported devices are running software images that are not in the software image repository.
  – Audit trail—Tracks software changes made on the LMS server
Q. What privilege level is required to run Software Management functions?
A. Different options in Software Management require different levels of user privileges. Privilege levels are known as “roles” in LMS. For a list of LMS functions and required user roles, use the Permissions Report function (Reports > System > Users > Permission).

Q. How do I know which functions I can access in Software Management?
A. To find which functions you can access in Software Management:
   • Select Reports > System > Users > Who Is Logged On to find your assigned roles.
   • Select Reports > System > Users > Permission to verify which LMS and Software Management tasks you can run.

Q. Are there DNS dependencies for Remote Copy Protocol (RCP) to work properly for a device?
A. Yes. If there are multiple IP addresses configured on the device, all IP addresses on the device must be configured in the Domain Name System (DNS). Examples of devices with multiple IP addresses are those having many interfaces, with each interface configured with its own IP address, or a device that interfaces configured with primary and secondary IP addresses.

Configure the DNS so that all IP addresses are resolved to the same host name. The host name in the DNS should match the host name entered in the Device and Credential Repository.

Q. Can I use Remote Copy Protocol (RCP) to transfer images to devices?
A. Use the RCP transport protocol for image transfers only on Cisco IOS devices that support the CISCO-FLASH-MIB. Catalyst switches that run Supervisor software older than 5.2, and 700 Series devices do not support the RCP protocol.

The Cisco IOS devices can not use RCP if they only support OLD-CISCO-FLASH-MIB, (for example, MC3810) or if they do not support any Flash Management Information Base (MIB) (for example, RSP 7000 devices running Cisco IOS Software Releases 10.3-11.0).

Q. What connection mechanism does Software Management use to upgrade software?
A. Simple Network Management Protocol (SNMP) is the preferred mechanism used by Software Management to upgrade software. Some devices, however, cannot be upgraded using SNMP alone. For such devices, Software Management uses a Telnet interface to do the upgrades. SNMP upgrades all Run-from-RAM Cisco IOS devices, Dual Flash Bank Run-from-Flash (DFB RFF) devices, and all Catalyst switches. If SSH is preferred for device connection then SSH is Used for connecting to the device.

Software Management uses Telnet to perform the following upgrades:
   • Single Flash Bank Run-from-Flash Cisco IOS devices (SFB 2500s, 1600s, AS5200)
   • RSP 7000 devices running Cisco IOS Software Releases 10.3 - 11.0
   • Cisco 700 Series
   • CIP, MICA, Microcom upgrades
   • 3500/2900 series of devices
   • 1900/2820 Series
   • VPN 3000 Series of devices.

For complete list of supported protocols see Supported Device Table for Software Management.
Q. What is the default Simple Network Management Protocol (SNMP) timeout used by Software Management? Can I configure it?
A. Default retry is 2 and default SNMP time out value is 2. This value is configurable using Admin > Collection Settings > Inventory > Inventory, Config Timeout and Retry Settings.

Q. Can I configure TACACS or Radius authentication for devices that Software Management has upgraded?
A. Software Management supports upgrading devices that are configured for TACACS or Radius authentication. An exception is software upgrades on the Run-from-Flash partition if the device is configured with Radius protocol authentication. The Device and Credential Repository must be configured with the appropriate information to access the device.

Q. Can I configure default privileges on terminal lines for Cisco IOS devices that Software Management has upgraded?
A. Software Management upgrades software by using the Telnet interface or Command-Line Interface (CLI) on devices that do not support enough Management Information Base (MIB) instrumentation for software management.

Software Management uses Telnet to connect into the devices and executes privileged commands such as copy tftp flash, copy flash tftp, erase flash, show version, copy flash modem to perform upgrades.

Software Management modifies the configuration file using the Telnet interface to upgrade the software. For Software Management to work on a device, there are some restrictions on how default privileges and enable mode authentication are configured.

The restrictions apply to only those Cisco IOS devices that are managed by Software Management through the Telnet interface. Cisco 700 Series and Catalyst 5000/6000/4000 devices are not affected. Restrictions include the following:

• Software Management tries to run the above CLI commands from privilege level 15. The user must always configure an enable password/secret for privilege level 15, and the same password/secret must be entered in the Device and Credential Repository.

If the device is configured with TACACS authentication for enable mode access, then the Enable TACACS user name and password must be entered in the Device and Credential Repository. The Enable User name and password authenticated by TACACS+ server always should receive a privilege level of 15.

• The default privilege level configured on a vty line must allow Software Management to run the CLI commands mentioned earlier as well change the configuration file on the device. The privilege level does not need to be 15, but setting the privilege level to 15 guarantees Software Management can always work on the device.

Q. What is Job Approval?
A. Job Approval allows an organization to require approvals before an administrator distributes software images. When an image distribution job is created, the administrator (or whoever creates the job) selects from a list of users who can approve the job.

For the job to run, one of the users on the approver list must approve it before its scheduled time. If the job is not approved, it will be rejected at the scheduled time.
Q. What is the approver list?
A. An approver list consists of user names in LMS who have the authority to approve software upgrades.

The following steps are required:


b. Create the list by using the Create Approver List (Admin > Network > Configuration Job Settings > Create/Edit Approver Lists). Only users who have an Approver role can be added to the Approver List.

Q. Is the Job Approval policy enforced system-wide?
A. Yes. To create a job that does not require approval, disable the Software Management option.

Q. How do I configure Job Approval for Software Management?
A. To configure Job Approval, do the following:

a. Add the approver user.

b. Create an Approver List

c. Enable the Job Approval option

Q. Which Cisco IOS devices support bootldr images?
A. The following Cisco IOS device families support bootldr images:

- Cisco 4500 and 4700
- Cisco 7500, Route Switch Processor (RSP)-based 7000
- Cisco 7200
- Cisco AS5200, AS5300, and AS5800 Access Servers
- Route Switch Module (RSM) on Cisco Catalyst 5500/5000
- ESR 10K, 10K2 devices

See the Supported Device Table for Software Management application on Cisco.com for further information.

Q. How do you identify bootldr image files?
A. Bootldr image files follow this name convention, platform-boot-mz.version

An example is rsp-boot-mz.11.0(17)BT. If the second part (feature part) of the image file name contains “boot”, then the image is a bootldr image. The software library recognizes the file name and imports the image as a bootldr image. Bootldr images earlier than Cisco IOS Software Release 10.3 contain xboot in the feature part of the image. Software Management does not support such images.
Q. How does the Software Management bootldr recommendation process work?
A. Different hardware platforms in Cisco IOS Software have different bootldr images. For example, the bootldr image for the Cisco 4500 device is c4500-boot-mz; the bootldr image for the Cisco 7200 is c7200-boot-mz.

From the library, Software Management determines which bootldr images belong to the same family as the target device. Software Management then recommends the most current of all available images.

Unlike system software images, bootldr images do not have RAM requirements. Therefore, Software Management does not perform prerequisite matches between the device and the image.

Q. Where is the storage location of the bootldr image on the Cisco IOS device?
A. Software Management always uses the Bootflash card as the target Flash for the bootldr image. Software Management stores bootldr images on the Bootflash card only, even though Cisco IOS Software allows the store of bootldr images on a Flash card.

If you use other Flash cards for the store of bootldr images, problems can occur when you have stored other types of images, such as system software, Microcom, or Modem ISDN channel aggregation (MICA), in the same location.

Q. Does Software Management erase Bootflash if there is not enough free space on Bootflash?
A. If the Bootflash card does not have enough free space to store the new bootldr image, Software Management erases the Bootflash to make room for the new boot image. A verification warning alerts you of the Bootflash erase.

To see this warning, click the Failure/Warning link in the Status column of the Verify Image Upgrade window.

Software Management backs up and restores files on Bootflash with sizes of less than 1 MB.

Q. Does Software Management change the configuration file for bootldr upgrades?
A. Upon bootldr upgrade, Software Management changes the device configuration file such that the configuration file that downloads to the device contains:

Assume that the file name of the newly downloaded bootldr image is c4500-boot-mz.112-13.bin.

– no boot boottldr
– boot boottldr c4500-boot-mz.112-13.bin

Q. Can Software Management back up the current bootldr image while Software Management runs the Distribute Images job?
A. Software Management backs up the system software image only during the Cisco IOS Distribute Images job execution. The backup of bootldr images cannot take place. Use the add images function to import the bootldr image from device to library. (Select Configuration > Tools > Software Image Management > Software Repository > Add).

Q. Does Software Management recommend bootldr images from Cisco.com in the Distribute Images function?
A. Yes, Software Management does recommend the download of bootldr images directly from http://www.cisco.com during the Distribute Images job creation.
Q. Can I upgrade modules on the device using advanced Distribution mode?
A. No. Expert flow is not officially tested with all the possible module upgrade scenarios. Current implementation claims only system software upgrades using the expert flow.

Q. What image extension type are not supported in Software Management?
A. The following file/image types are not supported:

doc, txt, pdf, xls, ppt, jpg, jpeg, bmp, csv, mpg, au, xml, html, htm, java, class, tex, ps, pps.

Q. How can secured image upgrades be performed using Software Management?
A. Current Version (4.1) supports new protocols such as, SCP and SSH. You can choose the appropriate protocols based on the device support.

For the devices that are upgraded using Telnet/SSH, new feature called Job based password can be enabled for scheduled job. You can specify a temporary password for the upgrade job and it will take precedence over all the credentials in the Device and Credential Repository.

Q. How to use Reboot order configuration feature?
A. This feature is applicable only in case of “parallel” mode of image upgrade. This feature can be used to perform sequential rebooting of devices. You can make this decision based on the network topology or any other deployment policy. The devices will be rebooted in the order specified by you.

Q. Is Image import from URL is treated as separate Job?
A. Yes, the workflow results in a job.

Q. What is the best effort verification performed while distributing the image using Advance mode?
A. Verification in Advance distribution mode is referred as the best effort verification because you can proceed to schedule the image upgrade even without the inventory data. This is designed to support devices that are not yet managed in Cisco Prime (pre-deployed devices).

Q. When does Software Management Application use SSH?
A. If the device type selected is to be upgraded using the CLI then Software Management application uses SSH (if opted in the preference). Even for fetching information required during the job creation stage, SSH is used.

Q. How can a protocol be Enabled/Disabled for a job?
A. Using the User Interface, Admin > Network > Software Image Management > View/Edit Preferences. Available protocols list the Software Management supported protocols. You have to add or remove the protocols to selected protocol order in order to enable or disable the protocol used for image transfer.

Q. How are devices upgraded using Secured Copy Protocol?
A. Image staging and other checks performed before the image distribution remains same for upgrade using SCP. The options such as Flash erasure, Delete, etc. are performed using Cisco Flash mib or old Cisco flash mib only.

The difference lies in the model used for image upgrade. LMS positions itself as a client for the Secured Copy options. Devices with SCP server are (like 2650XM) requested to initiate a file transfer job. The image is transferred from LMS to the devices.
Q. How much Disk space should be available while performing parallel image upgrade to large number of devices (more than 100)?
A. The amount of disk depends upon the number of images staged in the upgrade job. If the image selected is common for all the devices then disk space required is equal to size of the image. If different images are selected for each job then disk space required is the sum of all the images.

Q. What is the swap file size required for Software Management application?
A. LMS recommend a swap size of 2MB for managing 300 devices.

Q. What Version of SCP is supported in Software Management application?
A. Current implementation of SCP is based on the fcpsvc library that uses the SSHv1 stack. Current version of SCP supported is 1.0

Q. What are the pre requisites for using SCP for image upgrade?
A. The device should have SCP server Any image having 3DES feature has SCP server in it. SSH should be enabled on the device.

Q. Why is the job still running after I cancel it?
A. In Sequential mode, the job stops only after the image upgrade for the current device or module is finished. Canceling a running job does not cancel the software upgrade being performed at that time. The job stops only after the current upgrade is complete.

During this time, the Browse Job Status screen shows that the job is still running. In case of parallel upgrades, when a job is cancelled, the current set of devices being processed will be continued and not stopped. However, new devices will be processed only after the current devices have completed running.

Q. Why do I get an error message such as, Navigation to other areas of this application is not available until the opened wizard is finished or canceled.?
A. Yes, you get this when you are in a wizard (you will see Back, Next, Finish, and Cancel when you are in a wizard at the bottom) and you click any of the other navigational links.

Q. The Cisco.com profile window is sometimes filled with user and password and sometimes not. Why?
A. If the Cisco.com user name and password is configured for you the same will be pre-populated. You can configure the Cisco.com credentials in the Cisco.com User Account Setup dialog box (Admin > System > Cisco.com Settings > User Account Setup).

Q. I am not able to select both sequential execution and sequential reboot at 'Schedule Job' step during distribution?
A. If you had selected execution to be sequential the same order applies to reboot. However, if the execution is parallel you will be allowed to select reboot sequential.

Q. During Distribution by Advance flow, I get “Software Management application could not verify the flash inputs since there was no flash information available. Edit the expert input file and verify once again. If you do not edit the expert input file, you can continue with the task by clicking Next. However, the results may be inaccurate.”?
A. You get this when there are no inventory information available for the device. You can expect this error for 2900, 3500, 3550 xl devices.
Q. Why am I not able to see “Immediate” during software management jobs?
A. Check if approval is enabled. If approval is enabled for Software Mgmt Jobs, you will not be able to schedule Immediate job.

Q. I am not able to select the device (greyed box) at Software Management device selector page, but I’m able to select at inventory.
A. Software Management support might not be there. See the Supported Device Table for LMS on Cisco.com

Q. I am not able to select a user script which is in xxx path.
A. The scripts are expected to be available in the specific path. The Software Management scripts are located at:
   \textit{NMSROOT}/files/scripts/swim (On Solaris and Soft Appliance)
   \textit{NMSROOT}\files\scripts\swim (On Windows)
   
   Where \textit{NMSROOT} is the Cisco Prime installed directory.

Q. In ACS login mode. I'm not able to see links that I usually get to see.
A. On the ACS server, check if some role to task mapping (tree) has got changed. The required Software Management task option should be selected on the ACS server for a particular role.

Q. In the Job Details Window (clicking on job ID in the Software Management Job Browser) I don't see the job status being updated.
A. The job status will not be updated, as only the job running status is getting refreshed.

Q. What Validations are performed by Software Management before actual image distribution onto the device?
A. Software performs the following checks before the job execution:
   • Checks whether job file is Available at the job id and has required data in the format and prepares a list of devices to be upgraded in the job.
   • Checks whether LMS License is valid
     – Whether license file is valid
     – Number of devices managed
   • Removes all devices from the list which are not authorized for the user to perform image distribution.
     Removes all devices from the list which are in Suspended state or Conflicting state. Pre-deployed state devices are not removed.
   • Checks for the proper pre/post job script (if any) ownership and permission
     – On Solaris and Soft Appliance, check is performed for \texttt{rwxr-x---} permissions for script file (0750)
     – On Windows, check is performed if the given script has write permissions for any non-admin and non-casuser
   • Verifies that critical data required for image upgrade are present in the job file.
Q. What is the minimum software version required to be running on the device for Software Management to upgrade the software?
A. For Cisco IOS device minimum supported version is 11.0 whereas for Catalyst Images Minimum supported version is 3.8.
   For more details on minimum supported version for each device type refer to Supported Devices Table.

Q. Can I have a different script for each device in a job?
A. No, you cannot have separate script for each device. In Software Management 4.1, script is defined in admin preference option and is common for all Software Management jobs.

Q. What device types can be used as remote stage device?
A. All IOS devices with running image version >=12.0 version and complete CISCO-FLASH-MIB support can be used as Remote-Stage device.

Q. What device types cannot be upgraded using remote stage flow?
A. Content Engines (CE), Network Analysis Modules (NAM), Content Service Switches (CSS), and PIX.

Q. What are the pre-requisites for using the device as remote stage?
A. It must be an IOS device and it must be running >= 12.0 version and it must support CISCO-FLASH-MIB completely.

Q. What Configuration changes are performed by Software Management on the remote stage device?
A. tftp-server `flash-partition-name:image-name` alias `image-name` is the only command that will be added to the Remote stage device to make the image copied to Remote Stage device as accessible through TFTP from other devices.

Q. If I use the device as remote stage device does it impact the device's other functionalities? or what are the performance implications of using the device as remote stage device?
A. There will not be any impact on device's other functionalities and also they will not be any performance implications on the device that is used as Remote-Stage.

Q. Are there any Bad version of IOS for Remote stage device?
A. 12.3(5x) series.

Q. Can I perform module upgrade (like Bootloader/mica/microcom etc.) using remote stage flow?
A. No.

Q. How many devices in a job can be upgraded using remote stage?
A. There is no limit specific to remote stage flow. the number of devices in a remote stage job is same as that of other distribution flow.

Q. Can I perform Parallel upgrade using remote stage flow?
A. Yes

Q. Can I perform Slam dunk upgrade using the remote stage?
A. No. The image that you want to use must be in the Software Repository.
Q. What is the difference between Run-from-RAM and Run-from-Flash devices?
A. Most Cisco IOS devices load the software image from Flash to RAM when rebooting, then run the software from RAM. Such devices are called Run-from-RAM (RFR) devices. For these devices, the software image on Flash can be upgraded without rebooting the device.

Certain Cisco IOS devices (namely 2500s, 1600s, and AS5200s) run the system software image directly from Flash. These are Run-from-Flash (RFF) devices. The Flash partition in which the current image is stored is the RFF partition, which is read-only.

Software Management supports upgrading software images on RFF partitions by using a procedure called Rxboot upgrade. Before upgrading, reboot the device and put it into Rxboot mode, which makes the RFF partition available to write a new software image.

Q. When does Software Management use the remote copy protocol (rcp) to transfer images?
A. Generally the order defined in selected protocol list will be used for transferring (to upload and download) Cisco IOS® Software. If RCP is in the top of the selected protocol list then RCP is used as the first protocol for image transferring onto the devices that support CISCO-FLASH-MIB.

Check the supported protocol list for the device to find out whether device supports RCP or not. Cisco Catalyst 5500/5000 switches and Cisco 700 series devices do not support rcp. Cisco IOS devices that do not support rcp include the Cisco 7000 series (route processor [RP]-based 7000 only) and MC3810.

All other Cisco IOS devices support the rcp protocol.

Q. How does Software Management ensure that file corruption does not occur during transfer?
A. Software Management computes the checksum of the image file. Then, Software Management compares this checksum to the checksum from the device after the copy of the image file to the device Flash.

Software Management also verifies the size of the file on the Flash. If either the size or checksum do not match, Software Management aborts the distribution and marks the job status as an error.

Q. After an upgrade, why does Software Management sometimes leave behind image files in the tftpboot directory?
A. Software Management removes the image files from the tftpboot directory after the upgrade unless the TFTP fallback job option is set. If the TFTP fallback option is set, Software Management uploads the image from the device and leaves the image in the tftpboot directory for fallback.

Software Management also modifies the boot system commands on the device to add a fallback command to boot from the original image on the LMS TFTP server if the upgraded image does not boot.

Q. How much temporary space do you need during image distribution?
A. The amount of free space necessary depends on the image file size and the number of devices for simultaneous upgrade. If the TFTP fallback option is set, you need additional free disk space to keep the current image in the tftpboot directory. Both the tftpboot and temp directories use disk space.

Q. Is Cisco.com connection mandatory for Software Management?
A. Cisco.com connection is not mandatory for using basic Software Management functionality. Image distribution, library management, tracking software upgrade changes, and other functions can run without Cisco.com connectivity.
Cisco.com connectivity provides the additional benefits of obtaining images and their attributes from Cisco.com and viewing the status of outstanding bugs against the software images running on the devices in the network.

The following features of Software Management require Cisco.com connectivity:

- Adding image to Repository from Cisco.com. Software Management can import images for all supported devices.
- Distributing images directly from Cisco.com to devices, also called Recommend Images from Cisco.com. Without a Cisco.com connection, the Recommend Images screen Image list box will not show any images from Cisco.com when it creates the Distribute Images job.
- Cisco.com upgrade analysis.
- Cisco IOS image deferral processing.

Q. How does Software Management handle proxy environments?

A. Software Management uses HTTP protocol to communicate to Cisco.com about downloading images and their attributes. If you use an HTTP proxy for Internet connectivity, configure Proxy URL information in Admin > System > Cisco.com Settings > Proxy Server Setup.

Q. Does Software Management support proxy with user authentication environments?

A. Yes, Software Management support proxy that requires user authentication.

Q. Why is the Cisco.com filter option on the Software Management Edit Preferences screen not provided for Catalyst or Cisco 700 Series images?

A. During the Distribute Images task, Software Management communicates with Cisco.com to obtain a list of applicable images and their attributes. Based on this information, Software Management recommends an image.

There are many Cisco IOS images available on Cisco.com, which can cause a substantial delay in retrieving image attributes from Cisco.com. Some of these images will not be relevant to the user. Software Management filters the amount of images being considered to make a more meaningful and manageable subset.

For Catalyst and 700 devices, fewer images are available on Cisco.com than for Cisco IOS; therefore, it is not necessary to filter the images.

Q. How come the Cisco.com filter option does not work in LS1010 devices?

A. Although LS1010 devices run Cisco IOS images, there are some differences in how the LS1010 images are released. LS1010 images do not follow the Cisco IOS-type image releases like general deployment (GD), limited deployment (LD), and early deployment (ED).

Therefore, Software Management cannot effectively filter LS1010 type images. Nor does Software Management filter Catalyst 8500 Series images.

Q. Can I configure Software Management to retrieve images from a Cisco.com mirror site rather than the main Cisco.com site?

A. No. Although the mirror Cisco.com sites contain the images, they do not store image attributes, such as minimum RAM and FLASH requirement. This information is available only from the main Cisco.com site at http://www.cisco.com.
Q. Why I cannot download crypto images?
A. Crypto images are available only to authorized Cisco.com users. All users can view the images during the Recommendation stage but only users with the right privileges can download the image. Make sure that the Cisco.com Login user configured in Cisco Prime has permission to download crypto images.

Q. How does Software Management verify the integrity of the images after importing them from Cisco.com?
A. Software Management checks the validity of the downloaded images by comparing the MD5 checksum of the image with the MD5 checksum value retrieved from the Cisco.com database.

Q. Why does the Flash size displayed in the Add Image to Repository (Source:Cisco.com) function not match the actual size for some Cisco IOS devices?
A. Software Management does not erase files whose sizes are less than 1 MB on Cisco IOS devices because those files may be config files that are backed up to Flash partitions or .html files or Java applets used for management.

Software Management subtracts sizes of all files whose sizes are less than 1 MB from the size of the Flash partition. The result of the subtraction is displayed as the size of the Flash partition in the Software Management user interface.

The Software Repository Management window (Configuration > Tools > Software Image Management > Software Repository) displays the size of the largest Flash partition on the device. The size is displayed as an integer-truncated value in megabytes.

The Distribute Images screen displays information for all Flash partitions on the device. The values are displayed with two-decimal-digit precision.

The example below illustrates Software Management’s behavior on a Cisco IOS device, which has two files whose sizes are 10 KB and 50 KB respectively.

The Flash card’s total size is 8 MB. Because it has two files whose sizes are less than 1 MB, the Add Image to Repository screen displays the size as 7 MB. The Distribute Images screen displays the size as 7.94 MB.

```
enm-2502> show flash
System flash directory:
File Length Name/status
1 8089628 c2500-js-1.112-14.bin
2 10470 test_file1
3 52995 test_file2
8153288 bytes used, 235320 available, 8388608 total
8192K bytes of processor board System flash (Read ONLY)
```

Q. What is a Dual Flash Bank device?
A. The Flash card can be partitioned into two equal banks. Each bank is called a Flash partition. A Flash card that is not partitioned is Single Flash Bank (SFB) and the device is called an SFB device. A device that has its Flash card divided into two partitions is a Dual Flash Bank (DFB) device.

When Flash is partitioned into two separate banks, they are named flash1 and flash2. Software image files have to be completely stored in a single partition, so the maximum size of a software image is limited by the total size of any Flash partition.

On a Dual Flash Bank Run-from-Flash (DFB RFF) device, Software Management supports upgrading the flash partition that does not contain the running image. In other words, Software Management cannot upgrade the RFF partition on DFB devices.
This is because the other partition, which can be upgraded directly, is the recommended partition for storing the new software image.

The AS5200 device has two Flash cards, Bootflash and Flash. The Flash is an RFF system and Bootflash is an RFR system. The Bootflash is intended for storing bootldr images on the AS5200 and flash is for storing Cisco IOS System Software.

Q. Does Software Management support software upgrades on dual RSP-based systems?
A. Software Management updates the software on the master RSP processor by copying the software image file to the master RSP Flash card (bootflash: slot0: slot1:) and updating the config file on the master RSP. Software Management cannot do a complete job of upgrading the software on the slave RSP processor.

Software Management can only copy the software image file to the slave RSP processor, but it cannot update the config file on that processor. Users will have to run a separate Distribute Images job to copy the software image file to the slave RSP processor.

Since Software Management cannot update the config file on the slave RSP processor, users must select Don't touch config file and select the No Reboot option in the job created for upgrading software on the slave RSP processor.

Q. Why does Software Management require static IP routes or dynamic IP routing protocol for configuration for the upgrade of a run-from-Flash (RFF) partition on a Single Flash Bank (SFB) device?
A. Software Management upgrades SFB devices that are in Rxboot mode. Rxboot mode does not support IP routing, IP bridging, or Simple Network Management Protocol (SNMP). The Rxboot image can support only one IP interface. Before the reboot of the device while in the Rxboot mode, Software Management determines the:

• Interface that connects the device to LMS servers. Software Management shuts down all interfaces except the one that connects to the LMS server.
• Default gateway IP address for the forward of all IP traffic when the device is in the Rxboot mode.
• Software Management queries the ipRouteEntry MIB variables ipRouteDest and ipRouteIfIndex to determine the default gateway IP address and the interface that connects.

If the device configuration does not include static IP routes or dynamic IP routing protocol, the ipRouteEntry table is not set on the device. Consequently, Software Management cannot determine the default gateway and the interface that connects to LMS.

Q. Although the configuration of the Single Flash Bank (SFB) device includes an IP default gateway, why does Software Management not upgrade the device?
A. Software Management requires an IP default gateway address and an interface that connects. If you configure only the IP default gateway with the configuration command (ip default-gateway ip-address), you do not generate the ipRouteEntry MIB table on the device.

You can parse the IP default gateway from the configuration file; however, there is no reliable way to get the connecting interface from the device without the ipRouteEntry MIB. Without the ipRouteEntry MIB, Software Management does not allow upgrades, even if you have manually configured the IP gateway on the device.
Q. How do you change the IP default gateway configuration to allow Software Management to upgrade a device?
A. Use the IP default gateway configuration command to convert to a static IP route. Replace `ip default-gateway gateway_ip_address with ip route 0.0.0.0 0.0.0.0 gateway_ip_address`, which removes the `ip default-gateway` command from the configuration file. Check the output of the show ip route command to verify the correct configuration of a static IP route on the device.

Q. Why does Software Management require Cisco IOS Software Release 11.1 or later to run on a Single Flash Bank (SFB) device for an upgrade when you have configured the device with Frame Relay subinterfaces?
A. Releases earlier than Cisco IOS Software Release 11.1 do not include Frame Relay subinterfaces in ifTable and ipRouteTable in RFC 1213. Software Management requires information from these tables to perform Rxboot mode upgrades.

Therefore, Software Management requires Cisco IOS Software Release 11.1 or later to run on an SFB device when the device has Frame Relay subinterfaces.

Q. How is the job directory organized?
A. When Software Management schedules a job, it creates a new directory:

- On Solaris and Soft Appliance: `/var/adm/CSCOpx/files/rme/swim`
- On Windows, `NMSROOT\files\rme\swim`  
  Where `NMSROOT` is the Cisco Prime installed directory.

The directory name is the integer ID of the job. (Example: `/var/adm/CSCOpx/files/rme/swim/23`, where 23 is the Job ID.)

The Job directory contains the following files depending upon the type of Software Management task:

<table>
<thead>
<tr>
<th>Distribution Job</th>
<th>Image Import Job</th>
<th>Synchronization Job</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <code>swim_debug.log</code></td>
<td>• <code>swim_debug.log</code></td>
<td>• <code>swim_debug.log</code></td>
</tr>
<tr>
<td>• <code>workorder.html</code></td>
<td>• <code>workorder.html</code></td>
<td>• <code>workorder.html</code></td>
</tr>
<tr>
<td>• <code>distribution.xml</code></td>
<td>• <code>import.xml</code></td>
<td>• <code>import.xml</code></td>
</tr>
<tr>
<td>• <code>PostOperation.txt</code></td>
<td>• <code>PostOperation.txt</code></td>
<td>• <code>synchreport.xml</code></td>
</tr>
<tr>
<td>• <code>SwOperation.txt</code></td>
<td>• <code>SummaryTable.tab</code></td>
<td>• <code>jobinfo.xml</code></td>
</tr>
<tr>
<td>• <code>SummaryTable.tab</code></td>
<td>• <code>Hostname.upgStatus</code></td>
<td>• <code>synchReport.txt</code></td>
</tr>
<tr>
<td>• <code>Hostname._Config.Snap</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Where,
- `swim_debug.log` contains the debug information during the job execution.
- `workorder.html` contains the changes that user has chosen to perform with the job
- `deviceName.upgStatus` - a serialized file created on job completion for Retry and Undo options.
- `PostOperation.txt` used for all jobs scheduled through UI.
• SwOperation.txt indicates Job has been triggered. Absence indicate job has crashed for whatever reasons.
• SummarTable.tab for UI purposes always exists for executed job.
• _Config_snap contains the Changes that are performed by Software Management on the original configuration.
• HostName_telnet.log for some device types only.

Q. Which modem cards does Software Management support?
A. Software Management upgrades Modem ISDN channel aggregation (MICA) and Microcom 56K modems.

Q. Which devices and software versions get support for the modem upgrades?
A. Support is available for Modem ISDN channel aggregation (MICA) portware upgrades on:
• Cisco AS5200 that runs Cisco IOS Software Release 11.3(2)T or later and Bootldr version 11.2(11)P or later.
• Cisco AS5300 that runs Cisco IOS Software Release 11.2(9)XA, 11.3(2)T, or later.
• Cisco 3640 that runs Cisco IOS Software Release 11.2(12)P, 11.3(2)T, or later.
  Support is available for Microcom firmware upgrades on:
• AS5200 that runs Cisco IOS Software Release 11.2(10a)P or later.
• AS5300 that runs Cisco IOS Software Release 11.1(14)AA, 11.2(7a)P, or later.

Note Cisco AS5800 devices also have modems. However, the modem microcode for these devices is bundled with the system software only and receives upgrades as part of the system software upgrade.

Q. Which formats of Microcom firmware images does Software Management support?
A. The Microcom firmware for 56K modems is available in two formats:
  – Controller firmware and the Digital Signal Processor (DSP) code as two files, for example,
    mcom-modem-fw-xx.bin and mcom-modem-dsp-xx.bin.
  – A combination of firmware and the DSP code in a single format, for example,
    mcom-modem-code-xx.bin.

The Cisco AS5300 supports only the image combination. If the Cisco AS5200 runs a Cisco IOS Software release later than Cisco IOS Software Release 11.2(10)P, the AS5200 supports only the combination file format.

Software Management supports only the combination format files (for example, mcom-modem-code-xx.bin). Software Management does not support separate firmware and DSP code files. You cannot import the files to the software library.
Q. Which format of Modem ISDN channel aggregation (MICA) portware do Cisco 3600 devices support?

A. The 3640 digital modem network modules can run two types of modem microcode.
   - 3600-Specific Modem Microcode File—This file has a 3600-specific header and should have the characters c3600-mica in the file name. Software Management does not support such files.
   - Cisco AS5300 Modem Microcode File—In Cisco IOS Software Release 11.2(12)P, 11.3(2)T, and later, the 3640 supports the AS5300 microcode files directly and the 3600-specific microcode files.

The AS5300 microcode files have Executable and Linking Format headers that contain the version and other information about the image file. Even though the microcode file formats differ between the 3600 and the AS5300, the actual microcode that downloads to the MICA modems is the same.

Software Management supports only AS5300 format files. Therefore, the earliest Cisco IOS Software release that the 3640 supports is Cisco IOS Software Release 11.2(12)P.

Q. Why does the Undo option not receive support for modem upgrades?

A. To support the Undo option, Software Management must determine the version of software that runs and identify the image file on the device that corresponds. The image file must be present in the library or available on Cisco.com.

In the case of modem upgrades, Software Management cannot precisely determine the current software version on the modems in all cases. Moreover, different modems can run different software versions, which makes the undo process difficult to support.

Q. What connection mechanism does Software Management use for modem upgrades?

A. Software Management uses Simple Network Management Protocol (SNMP) to initiate the modem image file transfer to the device Flash. After Software Management copies the image to Flash, Software Management uses the Telnet interface to the device to run a command line interface (CLI) command that downloads the code to the modems. (The command is `copy flash modem`.)

Q. Does Software Management erase Flash for modem upgrades if there is not enough free space on Flash?

A. Yes, if the target Flash card does not have enough free space for the store of the new modem image, Software Management erases the target Flash. Software Management does not erase the Flash card if:
   - The upgrade of the system software does not occur within the same job as the modem upgrade.
   - The target Flash partition for the modem upgrade contains the current system software image.

Instead, Software Management prevents the modem upgrade on that Flash partition. On the Cisco AS5200, the Bootflash card stores modem images, which can contain the bootloader image that currently runs.

If there is not enough free space to contain the new modem image, Software Management erases the Bootflash card. Back up and restore bootloader images in the case that an erase of the Bootflash is necessary for the upgrade of the modem image. Software Management issues a verification warning if Software Management needs to erase the Bootflash.

Q. What is CIP?

A. CIP stands for Channel Interface Processor card. This interface card allows you to connect the Cisco 7000 router to IBM or IBM-compatible mainframes.
Q. Which devices support the Channel Interface Processor (CIP) microcode upgrade? What is the minimum software version necessary?
A. Software Management supports CIP upgrades on Cisco 7000 and 7500 routers that run Cisco IOS Software Release 11.1(1) or later.

Q. What is the minimum Channel Interface Processor (CIP) version that Software Management supports?
A. Software Management supports CIP version 22.0 at minimum.

Q. How can you import Channel Interface Processor (CIP) images to the Software Management library?
A. The Add Images function (Configuration > Tools > Software Image Management > Software Repository > Add) does not support the import of CIP microcode images from Cisco.com.
   a. You first must download the images to the file system on the LMS server.
   b. Then, choose Add option with source as File System to import them to the software repository.
      Software Management does not recommend the download of CIP microcode directly from Cisco.com for an upgrade.
   c. Populate the software Repository with modem images before you run the Distribute Images function.

Q. Is there support for the Undo option for Channel Interface Processor (CIP) upgrades?
A. No, there is no support for the Undo option for CIP upgrades.

Q. What connection mechanism does Software Management use to upgrade Channel Interface Processor (CIP)?
A. Software Management uses the Telnet interface to the device to copy the CIP image to the Flash. Software Management uses TFTP (via Simple Network Management Protocol [SNMP]) for the configuration upgrade to add the boot command to load CIP microcode.

Q. Does Software Management change the configuration file for the Channel Interface Processor (CIP) upgrade?
A. To load the new CIP microcode, the CIP upgrade process adds these configuration commands:
   ```
   microcode cip flash new_cip_image_name
   microcode reload
   ```

Q. Does Software Management supports CIP2?
A. Yes, Software Management supports CIP2 images for CIP supported device types.

Q. In which order does Software Management upgrade modules on a Cisco Catalyst 5500/5000 device?
A. Software Management upgrades the Supervisor Engine module on the device before other modules. Software Management upgrades the remainder of the modules in slot-number order. For example, Software Management upgrades the module on Slot 3 before Slot 5.
Q. Does the Supervisor Engine card reboot after the upgrade of all modules?

A. If you elect to reboot devices immediately after the upgrade of software, Software Management reloads the Supervisor Engine card. The reload of the card results in the reload of all modules, before the upgrade of software on other intelligent modules. This process supports instances in which the new module requires a newer version of Supervisor Engine software.

If you choose not to reboot the device after the download of software, you then must reload the Supervisor Engine module manually. You also should consider that software that you have newly loaded on a module may require new Supervisor Engine software.

If a new Supervisor Engine software is necessary, you should reload the Supervisor Engine module before you load the new software to the other intelligent modules (such as ATM, FDDI, and Token Ring).

For example, you may download 3.1(1) FDDI software and 4.1(1) Supervisor Engine software in a single job. The 3.1(1) FDDI software may require 4.1(1) Supervisor Engine software. Then, you must reset the Supervisor Engine module before you can upgrade the FDDI software. In such cases, you must have already chosen the Reboot Immediately option.

Q. Does Software Management determine if the newly deployed Supervisor Engine software or module software is compatible with the module types (or module hardware versions)?

A. Software Management does not verify whether the newly deployed Supervisor Engine software supports all modules that are available on the chassis.

Usually, with the upgrade of Supervisor Engine software to a newer release, the software provides backward compatibility for all the modules that exist on the chassis. However, you should check the release notes of the Supervisor Engine software or module software to be sure that the software versions are compatible.

Q. Does Software Management support the upgrade of software on redundant Supervisor Engine card-based systems?

A. The redundant architecture of Cisco Catalyst devices ensures that when the device reboots after a software upgrade, the redundant Supervisor Engine automatically synchronizes all the data from the primary Supervisor Engine. No special processes are necessary.

Q. Does Software Management update the configuration file on Cisco Catalyst 5500/5000 devices during the software upgrade?

A. Software Management updates the configuration file on Catalyst 5500/5000 devices only when the device has a Supervisor Engine III card. Software Management updates the boot system commands and the config register value if necessary.

For Supervisor Engine I and II and other module upgrades, Software Management does not update the configuration file on the device. Instead, Software Management uses CISCO-STACK-MIB and TFTP to download the configuration file. Before Software Management changes the configuration file on the device, Software Management backs up the file to the Job Schedule directory.

The example below illustrates the Software Management update of the configuration file. Assume that a Supervisor Engine III card runs 3.1(1) software. Also, assume that the software image file is on slot0 with the name cat5000-sup3.3-1-1.bin.

The configuration file boot system commands before the upgrade are:

```
set boot system flash slot0:cat5000-sup3.3-1-1.bin
```
Software Management has upgraded the software to 4.1(2). The new software image is on the same Flash card as cat5000-sup3-4-1-2.bin. Software Management then performs these configuration updates:

```
clear all boot system all
```
This removes all boot system commands on the device.

```
set boot system flash slot0:cat5000-sup3.4-1-2.bin
set boot system flash slot0:cat5000-sup3.3-1-1.bin
```
The update modifies the BOOT environment variable on the Supervisor Engine III card. You can display the environment values on the device is you issue the show boot command from the Supervisor Engine command-line interface (CLI).

The config register update occurs only if the least significant four bits of the config register are not all set to “1”.

For example, if the current config register value is 0x10F (with the least significant four bits all 1s), Software Management requires no change to the config register. If the current config register value is, for example, 0x111 or 0x11A, Software Management modifies the config register to 0x11F. The action generates this command:

```
set boot config-register 0x11F
```

Q. Does Software Management determine if the Supervisor Engine has the minimum required RAM to run a new image?

A. Software Management uses the Minimum Required RAM field for the Supervisor Engine software image. You can set this field when you import the image into the library. If you do not input a value in this field, Software Management uses this matrix to determine the RAM requirement:

<table>
<thead>
<tr>
<th>Image Type</th>
<th>Software Version</th>
<th>RAM Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>I, II sup</td>
<td>&lt; 2.1(1)</td>
<td>4 MB</td>
</tr>
<tr>
<td>I, II sup</td>
<td>≥ 2.1(1) &amp; &lt; 3.1(1)</td>
<td>8 MB</td>
</tr>
<tr>
<td>I, II sup8</td>
<td>≥ 3.1(1) &amp; &lt; 4.1(1)</td>
<td>8 MB (8 MB RAM image)</td>
</tr>
<tr>
<td>I, II sup</td>
<td>≥ 3.1(1) &amp; &lt; 4.1(1)</td>
<td>16 MB</td>
</tr>
<tr>
<td>I, II sup</td>
<td>≥ 4.1(1)</td>
<td>16 MB</td>
</tr>
<tr>
<td>III sup3</td>
<td>≥ 3.1(1)</td>
<td>32 MB</td>
</tr>
</tbody>
</table>

Images that are 8 MB RAM are available in 3.1 and 3.2 software releases only for Supervisor Engine I and II cards.

Software Management tries to use CISCO-MEMORY-POOL MIB to determine the available memory on a device. The MIB is implemented from 4.1(1) Supervisor Engine software (on all different Supervisor Engine card types—I, II, and III).

- If a device runs the software that implements this MIB, Software Management performs a memory check between the image requirement and the size of DRAM that is on the device.
- If the device does not have enough RAM to run the image, Software Management generates a verification warning.
- If the current software on the device is earlier than 4.1, Software Management generates a generic verification warning about memory requirements.
Q. Are there restrictions on the downgrade of the software on the Supervisor Engine card and other modules?
A. You can downgrade Supervisor Engine card software to version 4.1(1) or later.
For example, if a Supervisor Engine card runs 4.2(1) software, you can downgrade the software to 4.1(2) or 4.1(1). However, you cannot downgrade the same Supervisor Engine card to 3.2(1b). If a Supervisor Engine card runs 3.2(2), you cannot downgrade the software to 3.1(1) or 2.4(1).
There are no restrictions for the downgrade of software on other modules, such as ATM, FDDI, and Token Ring. However, you should check the release notes of new software before you attempt downgrades on modules.

Q. Do you need to reconfigure the device when you downgrade the Supervisor Engine software?
A. When you downgrade Supervisor Engine software, parts of the configuration may be lost. You must check the configuration file and reconfigure as necessary. Use the backed up Software Management configuration file from the Job Schedule directory as a reference, or use the backed up configuration file from the Config Archive.

Q. In the 4.1(1) software release and later, Supervisor Engine III cards allow the storage of configuration files on Flash cards. Does Software Management preserve the backed up configuration files on Flash during a software upgrade?
A. Software Management erases a Flash card on Supervisor Engine III if the free space on the Flash card cannot store the target software image. Software Management does not erase files of sizes that are less than 1 MB during software upgrades. Since configuration files generally do not exceed 1 MB, Software Management does not erase these files.

Q. Does Software Management allow you to upgrade epsboot images on Token Ring cards on Cisco Catalyst 5500/5000 devices?
A. Software Management does not allow upgrades of epsboot images on Catalyst 5500/5000 devices. An epsboot string in the file names can identify epsboot images. Epsboot upgrades are not often necessary. You can perform the upgrades with the Supervisor Engine card command-line interface (CLI).

Q. Why does the Add Image to Repository (Source: Cisco.com) task not display Token Ring LAN Emulation (LANE) or Permanent Virtual Circuit (PVC)-only ATM software images?
A. The Add Image to Repository (Source: Cisco.com) function in Software Management displays software images for only a subset of these ATM modules:
- WS-X5153
- WS-X5154
- WS-X5155
- WS-X5156
- WS-X5157
- WS-X5158
Software images for these modules have version numbers that range from 2.2 to 3.2(8).
The WS-X5153 to WS-X5158 modules can run:
- ATM LANE
- PVC Traffic Shaping
- Token Ring LANE software images

Software Management also supports the upgrade of software on these modules:
- WS-X5161
- WS-X5162
- WS-X5165
- WS-X5167
- WS-X5168

However, no mechanism exists to import the images from Cisco.com directly into the Software Management software library for these modules. The software images that run on the modules support LANE on Ethernet, Token Ring, and PVC traffic shaping.

You must download the software images for these modules directly from Cisco.com. Then, import the images into the library with the Add Image to Repository function.

Software Management does not support software management on WS-X5166 modules.

Q. How do you identify software image files for each of the ATM modules that Software Management does support? What are the file-name conventions on Cisco.com?

A. ATM software image file names and version numbers determine on which modules the software image can run and identify the features that receive support. This table provides details on version numbers and file-name conventions.

Q. How can I make the Image Recommendation faster?

A. If you select Cisco.com image recommendation, try to limit the images by filtering.

<table>
<thead>
<tr>
<th>Module IDs</th>
<th>Image Feature/Version</th>
<th>Image File Name Format (Example)</th>
<th>Version to Input in Software Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-X5153 to WS-X5158</td>
<td>Ethernet LAN Emulation (LANE) 2.2 to 3.2(7)</td>
<td>cat5000-atm.ver_number 3.2(7) cat5000-atm.3-2-7.bin</td>
<td>2.2-3.2(7)</td>
</tr>
<tr>
<td>WS-X5153 to WS-X5158</td>
<td>Ethernet LANE 3.2(8)</td>
<td>c5atm-wblane.Cisco_IOS_Software_rel_number c5atm-wblane.113-2.5.WA4.4m.bin</td>
<td>3.2(8)</td>
</tr>
<tr>
<td>WS-X5153 to WS-X5158</td>
<td>Token Ring LANE 70.x</td>
<td>c5k-trlane.ver_number c5k-trlane.70-1-1.bin</td>
<td>70.x</td>
</tr>
<tr>
<td>WS-X5153 to WS-X5158</td>
<td>Permanent Virtual Circuit (PVC) Traffic Shaping 50.x</td>
<td>cat5000-atm-pvcshape.ver_number cat5000-atm-pvcshape.50-1-1.bin</td>
<td>50.x</td>
</tr>
</tbody>
</table>
ATM version-number conventions differ for different classes of ATM images. PVC, Token Ring LANE, and Truckee types of ATM images have unique version-number conventions. Software Management recognizes the version numbers that appear in the last column of the table. The input of an incompatible version number results in upgrade job failures.

ATM software release notes give the original version number of the image as well as a version number that is close to the Software Management version-number scheme. Check the release notes for version-number schemes.

**Q.** Why do the software version numbers that the `show module` command output displays from the Supervisor Engine command-line interface (CLI) and the version numbers that Software Management uses fail to match in some cases?

**A.** ATM module software for Cisco Catalyst devices uses Cisco IOS Software code as a basis. The software release for Truckee ATM modules as well as ATM software releases 3.2(7) and later use the Cisco IOS Software version-number scheme.

Software Management does not recognize the Cisco IOS Software version-number scheme for Catalyst ATM software images. Use the simple version-number scheme that appears in the table in this document. (See the Version to Input in Software Management column.)

Output of the `show module` command of the Supervisor Engine CLI and the `show` command on the ATM module can display different versions. If the software that runs on the Supervisor Engine is earlier than 4.1, the Supervisor Engine software does not recognize the Cisco IOS Software version-number scheme of ATM images.

Therefore, the Supervisor Engine displays a different version number than the output of the `show version` command on the ATM module.

**Q.** Does Software Management recommend the right ATM image for your ATM module type?

**A.** Yes, Software Management distinguishes different flavours of ATM images and recommends images based on current class of ATM card on the device.
Q. Should you use special images with Software Management for Cisco Catalyst 2900XL/3500XL devices?
A. The 2900XL/3500XL devices have three images:
   – Regular Cisco IOS Software image.
   – A TAR format HTML image that contains files for Visual Switch Manager.
   – A TAR format image that contains both of these images.

Software Management uses the TAR format image that contains the Cisco IOS Software and HTML image. This image posts on Cisco.com, as do other images for 2900XL/3500XL.

When you use LMS for software upgrades, you should use images with the description Enterprise-IOS and HTML-Use. When you use Add Image to Repository from Cisco.com/Slam Dunk, you are able to see only these images.

Q. How does Software Management handle image import functionality of TAR and bin types of images for Catalyst 2900XL/3500XL devices?
A. For 2900/3500 device types Both .tar format and .bin format images are supported as system software. Network Synchronization option (Add image from network as source) will not be able to import tar images because when the image downloads to the switch, the image distributes as small individual files on the Flash in different directories.

The switch command-line interface (CLI) does not provide commands to combine all the files and make a new TAR file that Software Management can then upload. Whereas the .bin image can be imported from the device as well as from the Network Synchronization option.

Q. Why do software upgrades take longer on Cisco Catalyst 2900XL/3500XL devices?
A. Software Management uses command-line interface (CLI) to download software to 2900XL/3500XL devices. Because the software on these devices has many HTML/gif files on the Flash, the software must first delete all the files and then proceed with the new software download. Deletion of the images takes time, which is why software downloads to devices can take up to 20 minutes.

Q. How do you upgrade Route Switch Module (RSM) and LightStream 1010 (LS1010) module software on Cisco Catalyst 5500/5000 and 6500/6000 series switches?
A. The RSM (also called the VLAN router) on a Catalyst 5500/5000 or 6500/6000 switch and the LS1010 module on a Catalyst 5500/5000 switch run Cisco IOS Software. RSMs and LS1010 modules have individual IP addresses and Simple Network Management Protocol (SNMP) agents. The LMS Inventory manages these modules as separate devices.

You can find the IP address of the RSM if you look at the Detailed Inventory report of the Catalyst 5500/5000 and 6500/6000 device that has the RSM on the chassis. The Module IP Address column in the Stack Modules section shows the IP addresses of all modules on the chassis.

If you do not find the addition of RSM or LS1010 to Inventory, you must first add the module as a device to Inventory before you attempt Software Management functions. Software Management functions that run on Cisco IOS devices also can run on an RSM or an LS1010.
Q. Why does the Distribute Images task show all the images from Cisco.com for LightStream 1010 (LS1010) and Cisco Catalyst 8500 devices, even though you have configured Cisco.com filtering?
A. Although LS1010 and the 8500 devices run Cisco IOS Software images, differences exist in the means of image release. The images do not follow the Cisco IOS Software image releases, such as general deployment (GD), limited deployment (LD), and early deployment (ED). Therefore, Software Management cannot effectively filter LS1010-type and 8500-type images.

Q. What is the minimum version that Cisco 700 series ISDN routers support?
A. For Cisco 760 Series ISDN routers, Software Management requires a minimum software version of 3.2(4) on the device. For Cisco 770 Series ISDN routers, the minimum version necessary is 4.0(1).

Q. What connection mechanism does Software Management use for Cisco 700 series upgrades?
A. Software Management uses the Telnet interface to the device to copy the 700 series image to the Flash. Software Management uses TFTP protocol. The LMS workstation is the TFTP client, and the device is the TFTP server.

Q. Both Cisco 760 and 770 series devices run the same image. Why do you see only some images with versions later than 4.0(1) for 770 series devices but see all images for 760 series devices?
A. When you load an image with a version earlier than 4.0(1) onto a 770 series device, the sysObjectID box changes to something other than Cisco-assigned. Also, LMS identifies the device as a non-Cisco device. Therefore, Software Management does not list images with versions earlier than 4.0(1) for Cisco 770 series upgrades.

Q. Why do you not see the option to reboot the device later on the Job Control page for Cisco 700 series routers?
A. There is no option to reboot the device later because 700 series routers reboot at the time of the new image download.

Q. Why do you not see the option to modify the boot commands on the Job Control page for Cisco 700 series routers?
A. Only one image at a time can appear on the 700 series devices, which means the boot command does not apply to these devices.

Q. Why does Software Management report download failures for some images even though the device runs the new image after the job completes?
A. Some new Cisco 700 series images use nonstandard name convention or nonstandard versions. Software Management incorrectly parses the version number from file names of those images. After the download of the new image, the device reboots. Software Management retrieves the new image version from the device and compares that with the version that Software Management parsed. The two versions do not match. As a result, the software download appears to have failed, which generates as an error. This problem occurs with c760-in.b-US.42-3.5.bin and c760-in.b-US.43.1.bin images for all countries. You can resolve this issue by entering the correct version number when you import the image from the file system. For example, for c760-in.b-US.42-3.5.bin, enter 4.2(3.5). For c760-in.b-US.43.1.bin, enter 4.3(1) as the version number.
Q. In which order does Software Management upgrade modules on a Catalyst 5000 device?
A. Software Management upgrades the Supervisor module on the device before other modules. The remainders of the modules are upgraded in the order of their slot number. For example, the module on Slot #3 is upgraded before Slot #5.

Q. Does Software Management check to see that the newly deployed Supervisor software or module software is compatible with the module types (or module hardware versions)?
A. Software Management does not verify whether the newly deployed Supervisor software supports all modules that are available on the chassis.

Usually, when Supervisor software is upgraded to a newer release, the software provides backward compatibility for all the modules that exist on the chassis. Users are encouraged to check the release notes of the Supervisor software or module software to make sure that the software versions are compatible.

Q. Does Software Management support upgrading software on redundant Supervisor card-based systems?
A. The redundant architecture of Catalyst devices ensures that when the device reboots after a software upgrade, the redundant Supervisor automatically synchronizes all the data from the primary Supervisor. No special processing is required.

Q. What is the purpose of user scripts?
A. User-supplied scripts are run before and after each device upgrade. They can be used for pre- and post validation checks. For example,
   – The pre-upgrade script can check whether the device is accessible.
   – The pre-upgrade script can check whether any users are connected to the access server. If the script finds that some users are connected, it can decide whether to disable the connections before proceeding with the upgrade.
   – The post-upgrade script can check whether the device has upgraded successfully or not. Depending on the return value, Software Management either halts or continues with the rest of the upgrade job.

Q. What if the user script crashes? Will it crash the Software Management job also?
A. No, crashing of the script will not stop the Software Management job. Software Management executes the script in a different process space so the script crashing will not crash the Software Management job. However, Software Management will assume the script has failed.

Q. When a Software Management job is scheduled, how is the baseline determined? When I distribute a job, is an automatic backup performed?
A. There are two options that import images from the network to the Software Repository:
   • Baseline tasks
   • Synchronization

   The baseline task (Configuration > Tools > Software Image Management > Software Repository > Add > Network) should be done only once as a part of the initial setup. This imports the images running on the network to your Repository.

   To keep the Repository synchronized with any new images and changes caused by upgrades from sources other than Software Management, schedule a synchronization job to run periodically at appropriate intervals.
When this synchronization job runs, it looks for differences between the Repository and the network and allows any new images to be imported. During job distribution, Software Management backs up the current running image only if the option, Use current running image as tftp fallback image was selected when the job was created.

Q. Can I set up a periodic download of Software Management images from Cisco.com?
A. No. However, you can schedule a one-time import from Cisco.com to occur at a later time. Software Management does not allow you to automatically import images from Cisco.com to the Repository based upon your preferences.

Q. Is browser timeout something I should consider when downloading?
A. The Image Import option from Cisco.com and other devices can be done on a scheduled basis. Since this process runs as a background task on the server, the browser is not involved. However, when an Immediate Import job runs, it is performed as a foreground task, and the browser can still timeout.

Q. What are crypto images?
A. Crypto images are software images that use 56-bit Data Encryption Standard (DES) (or higher) encryption, and are subjected to export regulations. You must be a registered Cisco.com user, and be eligible and authorized to download such images.

Q. How much temporary space is required during image distribution?
A. The amount of free space that is required depends upon the image file size and the number of devices that are being upgraded simultaneously. If the `tftpfallback` option is set, additional free disk space is required to keep the current image in the tftpboot directory. Disk space is used both in the tftpboot and temp directories.

Q. At what time will the images directory get created during the process of obtaining images from a device? Does this happen during the initial step?
A. The software images directory gets created at the time of importing an image to the Repository; however, this should be transparent to you.

Q. How can I speed up Image Recommendation?
A. If you include Cisco.com for Image Recommendation, try to limit the images by filtering (Admin > Network > Software Image Management > View/Edit Preferences).

Q. When a job is rejected, can it be edited or should I resubmit?
A. No. You cannot edit or retry the rejected job. You should schedule a new job.

Q. Can different group members edit jobs? What are the restrictions?
A. The only job attribute that can be edited is the schedule time for non-Job Approval jobs. Any user who has the Network Administrator role defined can edit jobs or create new jobs; however, in the Job Approval model, the jobs can only be approved by users who are in the approver list specified during the creation of the job.
Q. What is the role of the registry files?

A. Software Management manipulates the Windows registry to automatically manage remote authentication during the rcp transfers on Windows. The following registry parameters are important for rcp service on Windows:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\DEBUG`
  Dictates the amount of debug information written in the Windows event log. (Default = 0, Maximum = 0xff)

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\rhosts`
  Contains the list of authenticated hosts that can run remote commands on this machine. This list is automatically managed by Software Management.

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\rusers`
  Contains the list of authenticated remote users that can run remote commands on this machine. This list is automatically managed by Software Management.

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\NoRuserCheck`
  If set to 1, the remote user authentication is skipped or, in other words, any remote user from authenticated hosts can run commands on this machine. (Default = 0)

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\NoRhostCheck`
  If set to 1, the remote host authentication is skipped or, in other words, commands can be run on this machine from any remote machine. (Default = 0)

Q. How do I upgrade Network Analysis Module (NAM) using Software Management?

A. To upgrade NAM using Software Management:

- Ensure that the passwords for NAM’s application and maintenance modes are the same. This is because Software Management takes the password information from Inventory. However, Inventory requires the application mode password to manage the device, and Software Management requires the maintenance mode password to upgrade the device. Therefore, the passwords for NAM’s application and maintenance modes should be the same.

- For a NAM card present in a Catalyst 6000 device running CatOS, ensure that you set auto logout to a value that is high enough to allow the copying of the new image. This is because a NAM image is usually very large (nearly 65 MB), and it may take between 1 to 2 hours to copy this image during Software Management upgrade. We recommend that you set the auto logout to 0 to ensure that there is no auto logout while the image is being copied. To set the auto logout value, use the CLI command, `set logout 0`.

  For a NAM card present in a Catalyst 6000 device running IOS, ensure that you set exec timeout to a value that is high enough to allow the copying of the new image. We recommend that you set the exec timeout value to 0 (exec-timeout 0 0) on all the vty lines.

- Ensure that the htdocs directory under CSCOpx has enough space to stage the NAM image. During the NAM upgrade, Software Management first copies the NAM image from the `NMSROOT/files/sw_images` directory (On Solaris and Soft Appliance) or `NMSROOT\files\sw_images` (On Windows), to the `NMSROOT\CSCOpx\htdocs\swimtemp` (On Solaris and Soft Appliance) or `NMSROOT\CSCOpx\htdocs\swimtempdirectory` (On Windows), and then copies the NAM image to the NAM card, using HTTP.
• Ensure that NAM is added with the correct Local User (root) and its password.
• Ensure that NAM is added with the correct SNMP read/write community strings.
• Ensure that the switch, which contains NAM, is added with the correct attributes.

Q. Can I change the job scheduled time?
A. The job scheduled time can be modified only for pending jobs that do not require approval.
   For a job that requires approval, you must cancel the job and retry or recreate the job.

Q. How does Software Management handle the job status for an abnormally terminated job?
A. Software Management checks the last modification time of the job results file for each running job
   when the Browse Job Status screen is displayed. If the results file has not been modified for the last
   six hours, Software Management assumes that the job was terminated abnormally (server reboot is
   a probable cause for the termination), and the job status is changed to Error.

Q. How does Software Management handle the job status of a pending job whose scheduled time has
   passed?
A. Software Management checks the scheduled time for each pending job when the Browse Job Status
   screen is displayed. If the current time is an hour past the scheduled time for starting the job, (lack
   of operating system resources is a probable cause for the job not running at the scheduled time), the
   job status is changed to Error.

Q. Why are some files left in the Software Management folder after Software Management has been
   uninstalled?
A. When uninstalled, Software Management does not remove the software images directory from the
   LMS server. The software images directory contains subdirectories for storing software images for
   various device families.

Q. How can I enable or disable the SSH to Telnet fallback for Software Management jobs?
A. To enable or disable SSH to Telnet fallback for Software Management jobs:

   Step 1  Go to Admin > Network > Software Image Management > View/Edit Preferences.
   Under the Distribution pane, there is a checkbox option, Use SSH for software image upgrade and
   software image import through CLI (with fallback to TELNET).

   Step 2  Do either of the following:
   • Check this option, to enable the use of SSH for software image upgrade and software image import
     through CLI along with fallback to Telnet.
   • Uncheck this option, to disable the use of SSH for software image upgrade and software image
     import through CLI along with fallback to Telnet.

   Step 3  Click Apply to save your changes.
Q. How can I export the images from SWIM repository to a local drive or a file system mounted to the LMS server?
A. To export the image from Software Repository to a local drive or a file system:

Step 1 Select Configuration > Tools > Software Image Management > Software Repository. The Software Repository Management dialog box appears.

Step 2 Select images that you want to export, then click Export. A confirmation message appears, The selected images will be exported.

Step 3 Click OK. The Select directory to export window appears.

Step 4 Click on Browse to select a directory to which you want to export the selected images. The Server Side File Browser dialog box appears.

Step 5 Choose the required directory and click OK. The Image Directory field in the Select directory to export window displays the directory location which you had selected.

Step 6 Click Next. A progress bar appears indicating the progress of the export of images. The Export Images Summary Report appears after completion of the export of the images with these details:
- Number of Selected Images
- Target Directory
- Summary

Step 7 Click Finish. You have successfully exported the images to the selected directory.

Q. Does Flash get erased if there is no sufficient space for Patch Distribution?
A. No. Patch Distribution requires sufficient amount of free space in Flash and so it cannot be erased.

Q. When I try to copy images, the Image Copy option fails indicating that the External TFTP server is inaccessible.
A. If you come across this error, try any of these:
- Check whether TFTP service is running or stopped in the External TFTP server. If stopped, start it.
- Check if any security agent is preventing the application. If so register the application with security agent or disable the security agent.

Q. Can I specify the name of my input file as imagenames.txt when I try to export images using the Software Management (SWIM) CLI exportimages command?
A. Do not name your input files similar to arguments.

For example, if you specify

cwcli swim exportimages -input imagenames.txt -u admin -p admin
the following error message will be displayed

Invalid argument: imagenames

For example, you can specify the input filename as sample.txt

You can enter the following argument in your sample.txt

-imagenames image1,image2,image3,image4...........

So the exportimages command with input file will be:

cwcli swim exportimages -input sample.txt -u admin -p admin

Q. I am getting timeout exception in cmdsvc (command service library) during a device connection/socket establishment. How do I change the default timeout and delays in cmdsvc?

A. You can change the default timeout and delays in cmdsvc using the cmdsvc.properties file available in the following directory: \$NMSROOT\objects\cmf\data

To change the default timeout and delay values:

Step 1 Go to the directory \$NMSROOT\objects\cmf\data

Step 2 Open the cmdsvc.properties file.

Various timeout and delay values are listed in the file.

Step 3 Remove the Hash symbol (#) to uncomment a particular timeout or delay value.

Step 4 Remove the existing timeout or delay value.

Step 5 Enter new timeout or delay value.

Step 6 Save the cmdsvc.properties file.

Troubleshooting Software Management

<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM0013</td>
<td>Image Import option not supported for the selected devices</td>
<td>Image Import option is not supported because of device limitations. Check Software Management feature support matrix against the selected device platform.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM0014</td>
<td>No images to import into library from the selected devices</td>
<td>Either: - There are no images on the Flash Or - Cannot get Flash information from inventory.</td>
<td>Check the Inventory Detailed Device Report to ensure that Flash file information exists for the device. If report generation fails, schedule an inventory collection job and redo the Software Management image import job.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| SWIM0019    | Could not perform Image recommendation for the selected devices because of insufficient data. | Could not fetch Image information from the Inventory database. | Check the Inventory Detailed Device Report to ensure that Inventory data exists for the device.  
If report generation fails, schedule an inventory collection job and perform Software Management recommendation. |
| SWIM0020    | Image Import option not supported for the selected devices                    | Image Import option is not supported because of device limitations.  
Check Software Management feature support matrix against the selected device platform. | None.                                                                                                     |
| SWIM0021    | Error encountered while parsing Job Data.                                     | Either the Job Data file could not be located or the data for Image Upgrade was not provided. | Check whether you have access permissions to Job Directory, or re-create the job.  
If the problem persists, send all log files under job directory to TAC. |
| SWIM0027    | Staging of the Image on the Remote Stage Device failed.                       | Image Copy to Remote Stage device failed because of SNMP Agent problems during transfer. | Check for any known bugs against the Image running on Remote Stage, or choose a different device.  
If the problem persists, send all log files under job directory to TAC. |
| SWIM0034    | Device reboot failed.                                                         | Either:  
- The device configuration for reboot is missing  
- The image downloaded onto the device is not suitable for the device to come up. | Check whether the snmp-server shutdown command is configured on the device.  
You can do any of the following:  
- Configure the devices and re-schedule the jobs.  
- Use NetConfig reload template to reload the devices.  
- Reload manually if you have only a few set of devices. |
<p>| SWIM0036    | Image addition to Software Library failed                                      | Either an invalid image was imported into library or the image is corrupted. | Check whether the image is downloaded completely in the directory                                        |
| SWIM0056    | Invalid Remote Stage device selected.                                         | Cannot use this device as Remote stage because of device limitations. | Check the Help documentation to see which devices can be used as Remote Stage.                         |
| SWIM0067    | System software analysis failed                                               | This is an unexpected runtime error. | contact Cisco TAC.                                                                                      |</p>
<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM0089</td>
<td>Could not perform Image Import from Cisco.com on the selected devices.</td>
<td>Add Image from Cisco.com not supported for the device. This is because Cisco.com could not find the device platform in the supported list.</td>
<td>Check the Software Management feature support matrix against the selected devices platform.</td>
</tr>
<tr>
<td>SWIM0092</td>
<td>Could not perform Image Import from Cisco.com on the selected devices because of insufficient data.</td>
<td>The device information needed to fetch images from Cisco.com does not exist in Inventory.</td>
<td>Check the Inventory Detailed Device Report to ensure that Chassis information exists for the device. If Chassis information is missing, schedule an inventory collection job and retry the import workflow.</td>
</tr>
<tr>
<td>SWIM0093</td>
<td>Could not get Image information from Cisco.com</td>
<td>Could not connect to Cisco.com from Cisco Prime Server either because of incorrect Cisco.com credentials or missing proxy configuration.</td>
<td>Check whether Cisco.com credentials are correct. If they are correct, check whether the proxy server is configured with right proxy credentials. To configure proxy, go to: Cisco Prime Home page &gt; Server &gt; Security &gt; Proxy Server Setup.</td>
</tr>
<tr>
<td>SWIM0101</td>
<td>The current version of the image on the device is different from the earlier version of the image.</td>
<td>This message is displayed when you retry a failed distribution job. This mainly happens when other jobs change the current running image of this device before scheduling the retry.</td>
<td>Try a new distribution job instead of retrying.</td>
</tr>
<tr>
<td>SWIM0118</td>
<td>Software Management application could not verify the inputs since there was no running image information. The device package may not have been installed. You can install it now and retry the task or you can install it before running the job. However, the results may not be accurate.</td>
<td>Advanced Distribution Flow: Either: • The selected device is not yet deployed in the network (pre-provisioned device) Or • It is still not supported by LMS.</td>
<td>Schedule the distribution job for a future date when the device is deployed Otherwise, the device package for this unsupported device will be installed and available in the LMS server.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM0119</td>
<td>Software Management application could not verify the Flash inputs since there was no Flash information available. Edit the expert input file and verify it again. If you do not want to edit the expert input file, you can continue with the task by clicking Next. However, the results may not be accurate.</td>
<td>The selected device does not have any Flash related information. Generally the Flash details are present in the Inventory. You can check the Detailed Device Report to see the Flash details. If there are no Flash details for this device, Software Management will allow the user to schedule a distribution job without verifying the Flash details.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM0120</td>
<td>Software Management application did not verify the inputs since there was no running image information. If you find that the device package is not installed, install it before running the job. The image distribution will proceed based on the unverified inputs. However, the results may not be accurate.</td>
<td>Advanced Distribution Flow: Either: • The selected device is not yet deployed in the network (pre-provisioned device) Or • It is still not supported by LMS.</td>
<td>Schedule the distribution job for a future date when the device is deployed. Otherwise, the device package for this unsupported device will be available and installed in the LMS server.</td>
</tr>
<tr>
<td>SWIM0121</td>
<td>Software Management application did not verify the Flash inputs as there was no Flash information. The image distribution will proceed based on the unverified inputs. However, the results may not be accurate.</td>
<td>The selected device does not have any Flash related information. Generally the Flash details are present in the Inventory. You can check the Detailed Device Report to see the Flash details. If there are no Flash details for this device, Software Management allows a user to schedule a distribution job without verifying the Flash details.</td>
<td>None.</td>
</tr>
</tbody>
</table>
### Message-ID | Error Message | Probable Cause | Possible Action |
--- | --- | --- | --- |
SWIM0122 | Software Management application could not verify the inputs since there was no running image information available. Update your inventory and retry the task. If you do not want to update the inventory, you can continue with the task by clicking Next. However, the results may not be accurate. | Either:  
- The selected device is not yet deployed in the network (pre-provisioned device)  
Or  
- It is still not supported by LMS. | Schedule the distribution job for a future date when the device is deployed. Otherwise, the device package for this unsupported device will be available and installed in the LMS server. |
SWIM0123 | Software Management application could not verify the inputs since there was no running image information. Update your inventory and retry the task. The image distribution will proceed based on the unverified inputs. However, the results may not be accurate. | Advanced Distribution Flow: The selected device is not yet deployed in the network (pre-provisioned device) or it is not supported by LMS. | Schedule the distribution job for a future date when the device is deployed. Otherwise, the device package for this unsupported device will be available and installed in the LMS server. |
SWIM0125 | An unexpected error has occurred. Contact Cisco support and attach the swim_debug.log file. | None. | Please contact Cisco TAC with the UI log available under:  
Windows:  
CSCOpx\logs\swim_debug.log  
Solaris and Soft Appliance:  
/var/adm/CSCOpx/log/swim_debug.log |
SWIM0126 | An unexpected error has occurred. Contact Cisco support and attach the swim_debug.log file. | None. | Please contact Cisco TAC with the UI log available under:  
Windows:  
CSCOpx\logs\swim_debug.log  
Solaris and Soft Appliance:  
/var/adm/CSCOpx/log/swim_debug.log |
<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM0138</td>
<td>Cannot connect to the Job Manager. Check whether the jrm process is running properly.</td>
<td>None</td>
<td>To check whether jrm is running, run command:</td>
</tr>
<tr>
<td></td>
<td>If it is not running, restart it and try scheduling the job again.</td>
<td></td>
<td><code>pdshow jrm</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If jrm is down, restart Cisco Prime.</td>
</tr>
<tr>
<td>SWIM0139</td>
<td>Running image information is not available in Inventory for Remote-Stage device Devicename.</td>
<td>Either:</td>
<td>If data is not available from the device (due to bug in the image), upgrade the device with the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Inventory is not updated</td>
<td>higher version image.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or</td>
<td><em>(This higher image populates the Detailed Device report with the required Flash data.)</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The image device running on the device is not populating the required Flash MIB information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Perform Update Inventory and check whether the required Flash data appears in the Detailed Device</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>report.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If it appears, retry the job; else, the data is not yet available from the device.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SWIM0141</td>
<td>There is not enough free space on the repository to store the selected files.</td>
<td>Disk space is not sufficient on the server.</td>
<td>Free up some disk space and retry the job.</td>
</tr>
<tr>
<td></td>
<td>Please free up some disk space and retry the job.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SWIM0142</td>
<td>RepositoryException while checking for disk space.</td>
<td>Disk space is not sufficient on the server.</td>
<td>Free up some disk space and retry the job.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SWIM0146</td>
<td>Could not get active image information.</td>
<td>A distribution job scheduled using Advanced flow for pre-provisioned devices has failed and you</td>
<td>Ensure that the device is deployed or the device package for this device is installed before a</td>
</tr>
<tr>
<td></td>
<td>Either the device is not reachable or the sysconfigName OID information is not provided by the device.</td>
<td>have tried a Retry task on this job.</td>
<td>distribution job is run on this device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The pre-provisioned devices does not have running images and so this error message is displayed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SWIM1001</td>
<td>The input parameters to the Image Distribution/Image Import/Image Activate are invalid.</td>
<td>You may have used incorrect Device Data for this task.</td>
<td>Check the application log file for more details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SWIM1002</td>
<td>An error occurred in staging Image Image Name.</td>
<td>There may not be correct permissions for the image in the software repository or for the directories</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>required for staging.</td>
<td>Retry the Image Upgrade option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1003</td>
<td>SNMP Agent does not support the required instrumentation to get information about the Flash File system.</td>
<td>The SNMP Agent on the device does not support CISCO-FLASH-MIB/OLD-CISCO-FLASH-MIB.</td>
<td>Check for any known bugs related to these MIBs for the image version running on the device.</td>
</tr>
<tr>
<td>SWIM1004</td>
<td>Cannot get details about the Flash File system on the device.</td>
<td>There may be a faulty implementation of the MIB on the device.</td>
<td>Check the Bug Toolkit application for any known issues on the running image version.</td>
</tr>
<tr>
<td>SWIM1005</td>
<td>Flash Device or Partition does not exist on the device.</td>
<td>Either the Inventory data on the device is stale, or the selected Flash Device or Partition is invalid.</td>
<td>Trigger inventory collection on the device.</td>
</tr>
<tr>
<td>SWIM1006</td>
<td>Flash Partition does not exist on the device.</td>
<td>Either the Inventory data on the device is stale, or the selected Flash Partition is invalid.</td>
<td>Update the inventory collection on the device.</td>
</tr>
<tr>
<td>SWIM1007</td>
<td>You have specified the storage location on the device in an invalid format.</td>
<td>None.</td>
<td>Enter a valid format.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>moduleName\flashPartitionName:partitionNumber:filename</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>In case of Andiamo devices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>flashDeviceName://flashPartitionName:filename</code></td>
</tr>
<tr>
<td>SWIM1008</td>
<td>You have specified an invalid format for the destination storage location.</td>
<td>None.</td>
<td>Enter a valid format.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>moduleName\\flashPartitionName:partitionNumber:filename</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>In case of Andiamo devices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>flashDeviceName://flashPartitionName:filename</code></td>
</tr>
<tr>
<td>SWIM1009</td>
<td>Inventory reported enough space on Flash partition, but the distribution task found that the space is insufficient and requires erasure.</td>
<td>The inventory data may be stale.</td>
<td>Update the inventory for the device and retry the job.</td>
</tr>
<tr>
<td>SWIM1010</td>
<td>The size of the partition selected to copy the image, is less than the image size.</td>
<td>None.</td>
<td>Select another partition to copy the image.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1011</td>
<td>Destination file size on storage location and the source file size are different.</td>
<td>This may be because of a network problem or a bug on the device.</td>
<td>Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.</td>
</tr>
<tr>
<td>SWIM1012</td>
<td>The file copied on the destination storage location is invalid.</td>
<td>The File Copy may have failed because of temporary network errors.</td>
<td>Retry the File Copy option.</td>
</tr>
<tr>
<td>SWIM1013</td>
<td>You have specified an invalid Job directory.</td>
<td>The destination directory that has been specified to copy the configuration file from the device is invalid.</td>
<td>Check whether the destination directory exists. If the directory exists, check whether there are write permissions. Also check whether there is enough disk space.</td>
</tr>
<tr>
<td>SWIM1014</td>
<td>Cannot generate configuration changes for Remote Stage option.</td>
<td>None.</td>
<td>Check for file permissions on the Job directory.</td>
</tr>
<tr>
<td>SWIM1015</td>
<td>Cannot generate configuration changes for activating the device.</td>
<td>None.</td>
<td>Check for file permissions on the Job directory.</td>
</tr>
<tr>
<td>SWIM1016</td>
<td>Cannot load new configuration to Remote Stage Device.</td>
<td>None.</td>
<td>Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.</td>
</tr>
<tr>
<td>SWIM1017</td>
<td>Cannot fetch configuration file from the device.</td>
<td>None.</td>
<td>Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.</td>
</tr>
<tr>
<td>SWIM1018</td>
<td>Cannot upload new configuration to the device during image activation.</td>
<td>None.</td>
<td>Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.</td>
</tr>
<tr>
<td>SWIM1019</td>
<td>Cannot reload the device. Device is not responding after the Reload command.</td>
<td>The image upgraded on the device has some issues.</td>
<td>Check the Bug Toolkit application for any known issues on the upgraded image version. Manually restore the device through the console.</td>
</tr>
<tr>
<td>SWIM1020</td>
<td>The device is not running the new image.</td>
<td>This may be because the new image is invalid or corrupted and the device has booted from another image.</td>
<td>Check the Bug Toolkit application for any known issues on the upgraded image version.</td>
</tr>
<tr>
<td>SWIM1021</td>
<td>Cannot get the IP Address of the server.</td>
<td>The DNS resolution of the LMS server may have failed.</td>
<td>Enable DNS resolution.</td>
</tr>
<tr>
<td>SWIM1023</td>
<td>Distribution task is not supported for this device.</td>
<td>The device packages that are installed may not be the correct package.</td>
<td>Check whether the correct device packages are installed on the server.</td>
</tr>
<tr>
<td>SWIM1024</td>
<td>Either the file already exists in the directory or the system cannot create this file.</td>
<td>Check whether another file with the same name already exists in the directory, or check whether there is enough disk space.</td>
<td>Create disk space and retry the task.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1025</td>
<td>The Configuration Register on the device does not allow you to boot the image from Flash.</td>
<td>The Configuration Register is not set to value 0x2102.</td>
<td>Change the Configuration Register on the device and retry the job.</td>
</tr>
<tr>
<td>SWIM1026</td>
<td>Cannot create a file and store the modified configuration.</td>
<td>There may not be sufficient permissions for the application to create the file, or there may not be enough disk space.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1027</td>
<td>Error while fetching inventory information.</td>
<td>The data required for the selected task is either incomplete or missing in Inventory.</td>
<td>Check whether the Inventory data exists for the device in the Inventory Detailed Device Report.</td>
</tr>
<tr>
<td>SWIM1028</td>
<td>Cannot get the required inventory information for the device.</td>
<td>Either there was no inventory collection for the device or the device is not responding.</td>
<td>Update inventory for the device and retry the task.</td>
</tr>
<tr>
<td>SWIM1030</td>
<td>This is a Run From Flash (RFF) device, but the application cannot find the running image on the Flash.</td>
<td>Either the inventory has not been updated or the Flash file is deleted from the Flash.</td>
<td>Update the inventory and retry the task.</td>
</tr>
<tr>
<td>SWIM1031</td>
<td>No Candidate Images found for the running software.</td>
<td>Either:</td>
<td>Check Admin preference or add images to software repository.</td>
</tr>
<tr>
<td>SWIM1032</td>
<td>Images obtained for Recommendation do not meet the hardware and software requirements of the selected device.</td>
<td>Either:</td>
<td>Check the Admin Preference or add more images to software repository and retry the job.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Candidate Images were filtered based on the selected Admin Preferences</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• They did not meet the Flash/RAM/BootROM needed to run on the device.</td>
<td></td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1033</td>
<td>Cannot find the Best-fit image for the device by applying compatibility checks.</td>
<td>Either:</td>
<td>Check the Admin Preference or add more images to software repository and retry the job.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Candidate Images were filtered based on the selected Admin Preferences</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• They did not meet the Flash/RAM/BootROM needed to run on the device.</td>
<td></td>
</tr>
<tr>
<td>SWIM1034</td>
<td>No applicable images found for the device from the configured image sources.</td>
<td>Either:</td>
<td>Check the Admin Preference or add more images to software repository and retry the job.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco.com is not included in the admin preferences</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There are no applicable images in the software repository or Cisco.com</td>
<td></td>
</tr>
<tr>
<td>SWIM1035</td>
<td>Error while performing Recommendation option.</td>
<td>None.</td>
<td>Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC).</td>
</tr>
<tr>
<td></td>
<td>Runtime error encountered while filtering images caused by a problem with a running image on the device.</td>
<td></td>
<td>The debug logs are available at this location:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>On Windows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NMSROOT/log/swim_debug.log</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>On Solaris and Soft Appliance:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM1036</td>
<td>Runtime error while performing Recommendation.</td>
<td>None.</td>
<td>Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The debug logs are available at this location:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>On Windows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NMSROOT/log/swim_debug.log</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>On Solaris and Soft Appliance:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM1037</td>
<td>Error while fetching Flash Partition information.</td>
<td>Either:</td>
<td>Update the inventory and retry the task. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Flash information cannot be got from Inventory</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There is a problem with the running image on the device.</td>
<td></td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>SWIM1038</td>
<td>No Read-Write Partition found on the device.</td>
<td>None.</td>
<td>Install a Flash device with a read-write partition and update the inventory.</td>
</tr>
<tr>
<td>SWIM1039</td>
<td>No Storage Recommendation is made for the device.</td>
<td>The selected device may not have sufficient free size partition to copy the image.</td>
<td>Check whether the selected device has the sufficient free size partition to copy the image.</td>
</tr>
<tr>
<td>SWIM1040</td>
<td>Cannot get the Flash information for the device.</td>
<td>Either: * The Flash information cannot be got from Inventory Or * There is a problem with the running image on the device.</td>
<td>Perform Inventory Collection and check whether the Flash information appears in the Detailed Device report. If so, retry the job. Else, data is not available from the device.</td>
</tr>
<tr>
<td>SWIM1041</td>
<td>This device upgrade requires opening an SSH/Telnet connection to the device.</td>
<td>Enable password is not configured correctly in Device and Credential Repository.</td>
<td>Make sure that the appropriate SSH/Telnet passwords are configured correctly in Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM1042</td>
<td>The amount of Bootflash on the device may not be enough to run the selected image.</td>
<td>The amount of Bootflash on the device may not be enough to run the selected image.</td>
<td>Specify the Bootflash size for the image by editing the attributes of the image stored in the software repository, increase the Bootflash size for the device, or select a different image for upgrading.</td>
</tr>
<tr>
<td>SWIM1043</td>
<td>Runtime error while performing Bootloader image verification.</td>
<td>Selected image version may not be in the standard version format.</td>
<td>Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: NMSROOT\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM1044</td>
<td>Bootflash partition will be erased before copying new image.</td>
<td>Selected Bootloader image does not fit in available space on Bootflash.</td>
<td>Select a different Bootloader image if available.</td>
</tr>
<tr>
<td>SWIM1046</td>
<td>Selected software does not fit in selected Flash partition.</td>
<td>Selected software image does not fit in the available space on Bootflash.</td>
<td>Select a different Flash partition for upgrading.</td>
</tr>
<tr>
<td>SWIM1047</td>
<td>Minimum software version required for MICA image upgrade is not known.</td>
<td>None.</td>
<td>Select the image in the software repository and update the minimum system software version using View/Edit Image Attributes option.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>SWIM1048</td>
<td>The system software that is active on the device, cannot run the selected image.</td>
<td>The system software that is active on the device, is not compatible with the selected image.</td>
<td>Select a different image that can be upgraded with the current system software or upgrade the system software to <em>Software Version</em>.</td>
</tr>
<tr>
<td>SWIM1049</td>
<td>The selected image requires Flash to be erased during image upgrade.</td>
<td>None.</td>
<td>Check whether you have performed the necessary backup.</td>
</tr>
<tr>
<td>SWIM1050</td>
<td>Read-Write SNMP community string is not in the Device and Credential Repository.</td>
<td>The Read-Write SNMP community string is not available in the Device and Credential Repository.</td>
<td>Add Read-Write community string for the device in the credentials repository.</td>
</tr>
</tbody>
</table>
| SWIM1051   | Credential information cannot be obtained for the device. | Either:  
• The device is not managed in the LMS server  
Or  
• The device credentials are not correct or the device access privileges are insufficient. | None. |
<p>| SWIM1052   | Enable password is not configured for the device. | For Run For Flash (RFF) partition software upgrades, the Enable password must be configured. | Configure the Enable password in the credentials repository. |
| SWIM1053   | Selected MICA Image is the same as the running image on the device. | The software version of the image is the latest on the device. | None. |
| SWIM1054   | Error while checking the Telnet credential of the device. | None. | Make sure that the Telnet credentials for the device are correct. |
| SWIM1055   | Selected Flash partition is ReadOnly. | Either the Flash partition is not write-enabled or the Read-Write partition does not exist. | Check whether the Read-Write partition exists. Set the Flash partition to be write-enabled. |
| SWIM1056   | The method to update the software on the selected storage device is unknown. | None. | Select a different Flash partition, if available. |
| SWIM1057   | The device will be put into Rxboot mode for the image upgrade. | None. | Select a different Flash device for the system software, if available. |</p>
<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM1058</td>
<td>The selected software version has some known problems in the Flash MIB options which will make this application unable to perform software upgrades on the device.</td>
<td>None.</td>
<td>Upgrade the device manually or select a later software version, if available.</td>
</tr>
<tr>
<td>SWIM1059</td>
<td>Ensure Dial Shelf runs a compatible software image with the newly loaded Router Shelf software image.</td>
<td>The Router shelf software image is not compatible with the Dial Shelf software image.</td>
<td>See the Release Notes for the Router Shelf software image to make sure the current Dial Shelf software is compatible. If not, upgrade the Dial Shelf software.</td>
</tr>
<tr>
<td>SWIM1060</td>
<td>Cannot obtain the file size of the selected image.</td>
<td>The selected image may have been removed from Cisco.com.</td>
<td>Select another image for upgrading.</td>
</tr>
<tr>
<td>SWIM1061</td>
<td>Image available at Cisco.com is selected for upgrade.</td>
<td>None.</td>
<td>Verify that connectivity to Cisco.com is available when the job is scheduled to run or select another image from the software repository.</td>
</tr>
<tr>
<td>SWIM1062</td>
<td>Selected image is already running on the device.</td>
<td>None.</td>
<td>Verify that this is the image you want to upgrade for the device. If so, no action is required. If this is not the image you want, select a different image.</td>
</tr>
<tr>
<td>SWIM1063</td>
<td>Minimum RAM requirement of the selected image cannot be determined.</td>
<td>RAM available on the device may not be enough to activate this image.</td>
<td>Update the minimum RAM value using View/Edit Image attributes or make sure that the device has enough RAM to activate the selected image or select a different image.</td>
</tr>
<tr>
<td>SWIM1064</td>
<td>RAM available on the device may not be large enough to activate the selected image.</td>
<td>RAM available on the device may not be large enough to activate the selected image.</td>
<td>Select another image or upgrade the RAM on the device and retry Upgrade.</td>
</tr>
<tr>
<td>SWIM1065</td>
<td>RAM available on the device may not be enough to activate the selected image.</td>
<td>RAM available on the device may not be enough to activate the selected image.</td>
<td>Specify the RAM size for the image by editing the attributes of the image stored in the software repository, increase the RAM size for the device, or select a different image for upgrading.</td>
</tr>
<tr>
<td>SWIM1067</td>
<td>Runtime error while performing verification of the selected image.</td>
<td>None.</td>
<td>Select another image for upgrading. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: NMSROOT\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1063</td>
<td>Minimum RAM requirement of the selected image cannot be determined.</td>
<td>RAM available on the device may not be enough to activate the selected image.</td>
<td>Update the minimum RAM value using View/Edit Image attributes or make sure that the device has enough RAM to activate the selected image or select a different image.</td>
</tr>
<tr>
<td>SWIM1068</td>
<td>Selected image does not have the minimum system software version required for the upgrade.</td>
<td>Selected image does not have the minimum system software version required for the upgrade.</td>
<td>Select another image with a version higher than 11.0.</td>
</tr>
<tr>
<td>SWIM1069</td>
<td>Feature subset of the running image cannot be determined. Select a different image.</td>
<td>This is a wrong message caused by a bug. The correct message is: Feature subset of the selected image is a subset or equal to running software feature set.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1070</td>
<td>Feature subset of the running image cannot be determined. Select a different image.</td>
<td>This is a wrong message caused by a bug. The correct message is: Feature subset of the selected image is a subset or equal to running software feature set.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1071</td>
<td>System software analysis failed.</td>
<td>Some unknown error has occurred during image analysis.</td>
<td>Please contact Cisco TAC with the UI log available under: Windows: CSCOpx\logs\swim_debug.log Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM1072</td>
<td>Boot loader analysis failed.</td>
<td>Some unknown error has occurred during analysis of the image.</td>
<td>Please contact Cisco TAC with the UI log available under: Windows: CSCOpx\logs\swim_debug.log Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM1074</td>
<td>The selected image does not have any requirement to be analyzed. The image can be used to upgrade the device.</td>
<td>None.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1075</td>
<td>Cannot find an image that is newer and can fit on the Bootflash.</td>
<td>None.</td>
<td>Add Bootloader images, to the Software Repository, with version greater than the running image version and that can fit into the Bootflash. Then retry the job.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1076</td>
<td>Cannot find a Read-Write Boot partition on the device.</td>
<td>Read-Write Boot partition is not available on the device.</td>
<td>Insert a read-write Bootflash on the device and update the inventory.</td>
</tr>
<tr>
<td>SWIM1077</td>
<td>Cannot find a Bootflash partition for the Bootloader image.</td>
<td>Bootflash partition is not available for the Bootloader image.</td>
<td>Insert a read-write Bootflash on the device and update the inventory.</td>
</tr>
<tr>
<td>SWIM1078</td>
<td>System and Bootloader images are getting upgraded to the same Flash partition.</td>
<td>System and Bootloader images are getting upgraded to the same Flash partition.</td>
<td>Select individual partitions for both, if available.</td>
</tr>
<tr>
<td>SWIM1079</td>
<td>Image version cannot be compared.</td>
<td>The image formats of both the images may not be compatible for comparison.</td>
<td>Check the format of the version. Select a different image for upgrading.</td>
</tr>
<tr>
<td>SWIM1080</td>
<td>Read-Write partition exists but you have selected the ReadOnly partition.</td>
<td>You may have selected Read only partition instead of Read-Write partition.</td>
<td>Select the Read-Write partition for upgrading.</td>
</tr>
<tr>
<td>SWIM1081</td>
<td>You have selected the Compressed System Image for Run From Flash (RFF) Upgrade.</td>
<td>Wrong image selected for Upgrade.</td>
<td>Select the correct image.</td>
</tr>
</tbody>
</table>
| SWIM1082   | Runtime error while comparing Modem Image.                                    | Either a wrong modem image is selected for comparison or the modem image formats or not compatible. | Select a different Modem Image for upgrading.  
If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC).  
The debug logs are available at this location:  
On Windows:  
%NMSROOT%\log\swim_debug.log  
On Solaris and Soft Appliance:  
/var/adm/CSCOpx/log/swim_debug.log |
<p>| SWIM1083   | Cannot find an image that is newer and fits in the Flash.                     | None.                                                                         | Add another image into software repository and retry the task.               |
| SWIM1084   | Cannot find a Minimum Flash Requirement for the device.                       | The Flash space available on the device may not be sufficient for the selected image. | Check whether the image fits on the device.                                   |
| SWIM1085   | The MinFlash Attribute is unknown for the selected image.                    | The selected image does not fit on the selected partition.                    | Check whether the image fits on the selected partition or select a different image. |
| SWIM1086   | Device not supported.                                                         | The required device packages may not be installed on the server.              | Check whether the appropriate device packages are installed correctly on the server. |</p>
<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM1087</td>
<td>Cannot get the device representation.</td>
<td>The required device packages may not be installed on the server.</td>
<td>Check whether the appropriate device packages are installed correctly on the server.</td>
</tr>
<tr>
<td>SWIM1088</td>
<td>Runtime error occurred while creating the device upgrade data.</td>
<td>None.</td>
<td>Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: \NMSROOT\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpv/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM1091</td>
<td>Minimum BootROM version of the selected image is not available in the software repository, or on Cisco.com.</td>
<td>The minimum BootROM value is not updated in View/Edit Image attributes for the selected image in software repository.</td>
<td>Update the minimum BootROM value using View/Edit Image attributes of the selected image in the software repository.</td>
</tr>
<tr>
<td>SWIM1092</td>
<td>Selected image does not have the minimum system software version required for system upgrade.</td>
<td>None.</td>
<td>Select an image that has a higher version than the minimum supported version. See the documentation for the Compatibility Matrix for Cisco IOS software.</td>
</tr>
<tr>
<td>SWIM1093</td>
<td>Cannot get Chassis Information from the inventory.</td>
<td>Check whether the Inventory data exists for the device in the Inventory Detailed Device Report.</td>
<td>If there is no inventory data for the device, schedule an Inventory Collection job and retry the task.</td>
</tr>
<tr>
<td>SWIM1094</td>
<td>SNMP-V3 parameters not in the Device and Credential Repository.</td>
<td>This could have been caused by any of the following: • The SNMP-V3 password is wrongly configured • The SNMP-V3 algorithm is wrongly configured • The SNMP-V3 engine ID is not configured in the Device and Credential Repository.</td>
<td>Check whether the SNMP-V3 password, SNMP-V3 algorithm, and SNMP-V3 engine ID is configured in the Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM1095</td>
<td>Error while checking the SNMP-V3 user name in the device context.</td>
<td>The SNMP-V3 credentials in the Device and Credential Repository is not up to date.</td>
<td>Update the SNMP-V3 credentials in the Device and Credential Repository and retry the task.</td>
</tr>
<tr>
<td>SWIM1096</td>
<td>Selected image is not applicable to this module.</td>
<td>The selected image is not applicable to this module.</td>
<td>Use the Cisco.com Upgrade Analysis feature to find an appropriate image.</td>
</tr>
<tr>
<td>SWIM1097</td>
<td>Selected Bootloader image is a lower version than the version of the Bootloader running on the device.</td>
<td>The Bootloader image version running on the device is the latest.</td>
<td>Check whether the higher version is available for upgrading.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1098</td>
<td>The selected image is lower than the running image on the device.</td>
<td>The image version running on the device is the latest.</td>
<td>Select a higher image for device software upgrade.</td>
</tr>
<tr>
<td>SWIM1099</td>
<td>Image Upgrade procedure may revert to the SSH/Telnet-based approach, based on the MIB instrumentation on the running image.</td>
<td>The SSH/Telnet passwords may not be configured in the Device and Credential Repository.</td>
<td>Make sure that appropriate SSH/Telnet passwords are configured in the Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM1100</td>
<td>Cannot find SNMP-V2 Read-Write Community String in the Device and Credential Repository.</td>
<td>The SNMP-V2 credentials may not be correctly configured in the Device and Credential Repository.</td>
<td>Check whether the SNMP-V2 credentials are configured correctly in the Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM1101</td>
<td>This Device Upgrade requires opening an SSH/Telnet connection to the device.</td>
<td>Enable password for the device is not configured in Device and Credential Repository.</td>
<td>Make sure that appropriate SSH/Telnet passwords are configured correctly in the Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM1102</td>
<td>This Device Upgrade requires opening an SSH/Telnet connection to the device.</td>
<td>There was an error while checking the credentials of the device.</td>
<td>Make sure that appropriate SSH/Telnet passwords are configured correctly in the Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM1103</td>
<td>Selected image may not be compatible to the device.</td>
<td>Image belongs to the same device family as the running image on the device. However, it is identified as non-compatible.</td>
<td>Check the Cisco.com documentation whether any caveats are identified for the selected image.</td>
</tr>
<tr>
<td>SWIM1104</td>
<td>The total space on the selected partition is not enough to upgrade all of the selected modules.</td>
<td>Multiple modules may be selected for upgrading on the same partition.</td>
<td>Select individual partitions for the selected modules, or deselect some modules.</td>
</tr>
<tr>
<td>SWIM1105</td>
<td>Image status for the selected image cannot be determined.</td>
<td>The selected image might be in the Deferred status.</td>
<td>Ensure that the image is not in the Deferred status. See the relevant documentation on Cisco.com before upgrading the images.</td>
</tr>
<tr>
<td>SWIM1106</td>
<td>Image selected for upgrade is compressed in .tar format. Flash will be overwritten while upgrading the image.</td>
<td>None.</td>
<td>Ensure that necessary backup jobs are completed before upgrading.</td>
</tr>
<tr>
<td>SWIM1107</td>
<td>This option requires devicename data in the inventory.</td>
<td>The required device information is not available in the inventory.</td>
<td>Perform Update Inventory and check whether the required data appears in the Detailed Device Report. If so, retry the job. Else the data is not retrieved from the device.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>SWIM1109</td>
<td>Image status for the selected image is either Deferred or Not Supported.</td>
<td>Image status for the selected image is either Deferred or Not Supported.</td>
<td>Ensure that the image is supported by Software Management application. Check the documentation on Cisco.com before upgrading the image.</td>
</tr>
<tr>
<td>SWIM1110</td>
<td>.bin images are not supported for Stack Upgrade.</td>
<td>The .bin image has been selected for Stack Upgrade.</td>
<td>Select a tar image for Stack Upgrade.</td>
</tr>
<tr>
<td>SWIM1111</td>
<td>The available free space is not enough for upgrading this type of image.</td>
<td>Insufficient space for image upgrade.</td>
<td>Select a different image or free up some space. Update the inventory and retry the job.</td>
</tr>
<tr>
<td>SWIM1112</td>
<td>This module can be upgraded if managed independently.</td>
<td>This module can be upgraded only if it is managed as a separate device.</td>
<td>Assign an independent IP Address to this module. Manage it as a separate device and select that device to upgrade this module.</td>
</tr>
<tr>
<td>SWIM1113</td>
<td>Device Reboot failed or Reboot Verification failed.</td>
<td>The device is not running the new image after it is rebooted.</td>
<td>Verify the configuration used to load the new image. Verify whether the new image exists on the device in a valid Flash partition.</td>
</tr>
</tbody>
</table>
| SWIM1114   | The device cannot be reached after the reboot. Number of attempts to verify the device status has exceeded the maximum retry count. | Either:  
- An invalid image has been loaded onto the device  
Or  
- There are network connectivity problems. | Use the device console to determine if the device has reloaded with the desired image. |
<p>| SWIM1115   | Device is booted from TFTP server. | The backup running image is not supported. | None. |
| SWIM1116   | Read-Write SNMP community string cannot be fetched from the Device Context. | The Read-Write community string is not available in the Device and Credential Repository for this device. | Add the Read-Write community string to the Device and Credential Repository. |
| SWIM1117   | The selected image is incompatible and cannot run on the selected device. | The selected image is incompatible and cannot run on the selected device. | Use the Cisco.com Upgrade Analysis feature to find an appropriate image. |
| SWIM1118   | Selected image has a lower version than the version of the running image. | The selected image has a lower version than the version of the running image. | Verify whether the correct image is running on the device. If so, no action is required. If not, select a different image. |
| SWIM1119   | Telnet credentials are not present for this device. There was an error while checking the credentials of the device. | The SSH/Telnet passwords are not configured correctly in the Device and Credential Repository. | Ensure that appropriate SSH/Telnet passwords are configured correctly in the Device and Credential Repository. |</p>
<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWIM1120</td>
<td>Cannot obtain the sysObjectID of the device.</td>
<td>Either:</td>
<td>Manually enter the device type information in the Device and Credential Repository.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The device did not respond when you added it to LMS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The device cannot be added correctly.</td>
<td></td>
</tr>
<tr>
<td>SWIM1122</td>
<td>Runtime error found during verification.</td>
<td>None.</td>
<td>Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: NMSROOT\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log</td>
</tr>
<tr>
<td>SWIM1123</td>
<td>Telnet username not present for this device.</td>
<td>Either:</td>
<td>Check whether the primary username is configured for the selected device, in Device and Credential Repository.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Primary Credentials is not configured</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• It not configured properly for the selected device in the Device and Credential Repository.</td>
<td></td>
</tr>
<tr>
<td>SWIM1124</td>
<td>Cannot copy the image from Flash with return code of Code.</td>
<td>None.</td>
<td>Retry the job. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.</td>
</tr>
<tr>
<td>SWIM1125</td>
<td>Cannot copy the image from Flash with return code of Code.</td>
<td>None.</td>
<td>Retry the job. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.</td>
</tr>
<tr>
<td>SWIM1126</td>
<td>Image copy to module failed with return code of Code.</td>
<td>None.</td>
<td>Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: NMSROOT\files\rme\jobs\swim\JobID On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/jobs/swim/JobID</td>
</tr>
<tr>
<td>SWIM1127</td>
<td>Cannot connect to device through SSH/Telnet because of Device.</td>
<td>The SSH/Telnet credentials may not be correctly configured in the Device and Credential Repository.</td>
<td>Check whether the SSH/Telnet credentials are correctly configured in the Device and Credential Repository.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>SWIM1128</td>
<td>Cannot disconnect from device because of Device</td>
<td>the SSH/Telnet credentials may not be correctly configured in the Device and Credential Repository</td>
<td>Check whether the device is configured correctly.</td>
</tr>
<tr>
<td>SWIM1139</td>
<td>Select any available Boot flash partition, for bootldr upgrade. We recommend that you use boot flash for bootldr upgrade.</td>
<td>This happens when the user has selected a Bootloader image for Distribution and a storage location other than Bootflash.</td>
<td>Select any available boot flash partition for bootldr upgrade.</td>
</tr>
<tr>
<td>SWIM1150</td>
<td>Could not get Command Service instance for device DeviceName because of CmdSvc Exception.</td>
<td>Either: • The device login credentials in DCR are wrong or empty. Or • The SSH option is selected in the Swim Admin pane and the target device does not support SSH.</td>
<td>Check whether the Login credentials in DCR and Login credentials specified during job scheduling are correct.</td>
</tr>
<tr>
<td>SWIM1151</td>
<td>Could not connect to the device DeviceName because of CmdSvcException.</td>
<td>Either: • The device login credentials in DCR are wrong or empty. Or • The SSH option is selected in the Swim Admin pane and the target device does not support SSH.</td>
<td>Check whether the Login credentials in DCR and Login credentials specified during job scheduling are correct.</td>
</tr>
<tr>
<td>SWIM1161</td>
<td>RXBOOT credentials are not configured for the device. If TACACS is used by the device, configure RXBOOT Mode credentials in the credentials repository. This will be used to contact the device in RXBOOT Mode (if configured) for Run From Flash (RFF) devices.</td>
<td>RXBOOT credentials are not configured for the device in Device Credentials Repository (DCR). This will be used for Run From Flash (RFF) devices when connecting in RX boot mode.</td>
<td>If TACACS is used by the device, configure RXBOOT Mode credentials in the Device credentials repository.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1162</td>
<td>Error when recommending image for the device.</td>
<td>Swim recommends the image based on device ROM, RAM and Flash which it collects from LMS Inventory module. If the device is having a faulty hardware (FLASH) then this will not be available in inventory.</td>
<td>Check the Inventory Detailed Device Report to ensure that Inventory data exists for the device (like Flash Partition size). If not, check the device for a faulty hardware or a bug in device software.</td>
</tr>
<tr>
<td>SWIM1163</td>
<td>Image Import from Device failed because of some unexpected error.</td>
<td>None.</td>
<td>Please contact Cisco TAC with the Job logs available under: Windows: NMSROOT\files\rme\jobs\swim\jobID Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/jobs/swim/jobID</td>
</tr>
<tr>
<td>SWIM1164</td>
<td>Image Distribute to Device failed because of some unexpected error.</td>
<td>None.</td>
<td>Please contact Cisco TAC with the Job logs available under: Windows: NMSROOT\files\rme\jobs\swim\jobID Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/jobs/swim/jobID</td>
</tr>
<tr>
<td>SWIM129</td>
<td>Selected image does not fit on the free Flash size on the device. Selected storage partition will be erased during the distribution.</td>
<td>Either: The boot loader image is selected for upgrade (and no system software image is selected along with it) or The storage location is not erased for the boot loader image to be copied.</td>
<td>Since the system software is not selected for upgrade, ensure that running system software is not in the selected storage partition. Back up the running system software and ensure that the device boots from the backed up image in case the job fails.</td>
</tr>
<tr>
<td>SWIM1501</td>
<td>Supervisor cannot be downgraded to an image version less than 4.1(1).</td>
<td>This happens when you try to distribute a CATOS image lesser than 4.1(1).</td>
<td>If you continue to downgrade, the device may lose its configuration. Use a higher version.</td>
</tr>
<tr>
<td>SWIM1506</td>
<td>Cannot move file from Location 1 to Location 2.</td>
<td>There may not be sufficient permissions for the application to move or copy the file, or there may not be enough disk space.</td>
<td>None.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>SWIM1507</td>
<td>Cannot back up the running image.</td>
<td>Either the file name or the storage partition name specified for backup is invalid.</td>
<td>You can stop the job, manually back up the running image, and retry the job.</td>
</tr>
<tr>
<td>SWIM1508</td>
<td>Cannot copy image <code>Imagename</code> to storage partition <code>Partitionname</code>.</td>
<td>Either the filename or the storage destination is invalid or the device does not provide the required MIB instrumentation for copying an image.</td>
<td>Retry the job. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.</td>
</tr>
<tr>
<td>SWIM1510</td>
<td>Runtime error while performing Reload on a device.</td>
<td>None.</td>
<td>Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: <code>\NMSROOT\files\rme\jobs\swim\JobID</code> On Solaris and Soft Appliance: <code>/var/adm/CSCOpx/files/rme/jobs/swim/JobID</code></td>
</tr>
<tr>
<td>SWIM1518</td>
<td>Runtime error during configuration upload.</td>
<td>None.</td>
<td>Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: <code>\NMSROOT\files\rme\jobs\swim\JobID</code> On Solaris and Soft Appliance: <code>/var/adm/CSCOpx/files/rme/jobs/swim/JobID</code></td>
</tr>
<tr>
<td>SWIM1525</td>
<td>Unknown package type.</td>
<td>None.</td>
<td>Check whether the module is supported in the Software Management Function and Device Support Matrix on Cisco.com.</td>
</tr>
<tr>
<td>SWIM1529</td>
<td>There is no module information available in the inventory for <code>devicename</code>.</td>
<td>There is no module information available in the inventory for <code>devicename</code>.</td>
<td>Update the inventory and retry the task.</td>
</tr>
<tr>
<td>SWIM1530</td>
<td>Storage not applicable for the module <code>modulename</code>.</td>
<td>This module does not support storage.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1532</td>
<td>No read-write partition exists on the device to accommodate the selected image.</td>
<td>None</td>
<td>Create some free space.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM1542</td>
<td>Minimum supported version for Supervisor is 3.8.</td>
<td>None.</td>
<td>Select a higher version of the image to upgrade.</td>
</tr>
<tr>
<td>SWIM1543</td>
<td>Selected image has the same or a lower version than the version of the running image.</td>
<td>The selected image has the same or a lower version than the version of the running image.</td>
<td>Verify whether the correct image is running on the device. If so, no action is required. If not, select a different image.</td>
</tr>
<tr>
<td>SWIM1546</td>
<td>The NVRAM size on the device may not be large enough to run the image.</td>
<td>The NVRAM size on the device may not be large enough to run the image.</td>
<td>Select a different image or upgrade the NVRAM on the device and retry the Upgrade option.</td>
</tr>
<tr>
<td>SWIM1547</td>
<td>Available NVRAM size on the selected image cannot be determined.</td>
<td>RAM size on this module may not be large enough to store this image.</td>
<td>Make sure the module has enough NVRAM to run the selected image. Else, select a different image or upgrade the RAM on the module.</td>
</tr>
<tr>
<td>SWIM1548</td>
<td>There are no software requirements found for the selected image.</td>
<td>None.</td>
<td>Select a different image.</td>
</tr>
<tr>
<td>SWIM1549</td>
<td>Verify that the new software selected is compatible.</td>
<td>Software Management cannot determine the features in the ATM software.</td>
<td>Check the Release Notes for the new software to determine if all the features in the old software are available in the new software.</td>
</tr>
<tr>
<td>SWIM1554</td>
<td>The selected image cannot be used to upgrade the device.</td>
<td>The device does not have any module that can run the selected image.</td>
<td>Select a different image.</td>
</tr>
<tr>
<td>SWIM1556</td>
<td>Select the Storage partition.</td>
<td>None.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM1560</td>
<td>Slot number corresponding to the module cannot be got from inventory.</td>
<td>None.</td>
<td>Update Inventory and retry the task.</td>
</tr>
<tr>
<td>SWIM2001</td>
<td>Telnet error while connecting to the device.</td>
<td>Invalid access information in the inventory.</td>
<td>Verify the username and the passwords in Device and Credential Repository and retry the task.</td>
</tr>
<tr>
<td>SWIM2002</td>
<td>Cannot get details about Flash File system on the device.</td>
<td>Either the Flash device is not available or the Flash information format has changed.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM2503</td>
<td>Different images have been selected for upgrade of the Active and Stand-by processors. This may make the device unavailable.</td>
<td>None.</td>
<td>Select the same image for upgrade of Active and Stand-by CPUs.</td>
</tr>
<tr>
<td>SWIM3501</td>
<td>Cannot fetch device credentials for the selected device.</td>
<td>The credentials may not be configured correctly in Device and Credential Repository.</td>
<td>Check whether there are credentials are configured correctly in Device and Credential Repository.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM502</td>
<td>Cannot fetch the credentials of the parent device, for the selected device.</td>
<td>The NAM device Supervisor is not recognized by the LMS Inventory.</td>
<td>Add the Supervisor of the NAM device to the LMS Inventory.</td>
</tr>
<tr>
<td>SWIM503</td>
<td>Telnet credentials are not present for the parent device.</td>
<td>The Telnet credentials are not properly configured for the parent device.</td>
<td>Check whether the Telnet credentials are configured for the parent device.</td>
</tr>
<tr>
<td>SWIM504</td>
<td>If Auto Logout is enabled on the parent device, it may get disconnected during upgrade. Configure No Auto Logout for the parent device.</td>
<td>None.</td>
<td>None.</td>
</tr>
<tr>
<td>SWIM505</td>
<td>NAM images are large.</td>
<td>The disk space available is insufficient.</td>
<td>Ensure that there is enough disk space available in the htdocs/swimtemp directory under the Cisco Prime install directory.</td>
</tr>
<tr>
<td>SWIM505</td>
<td>Selected image does not have the minimum system software version required for system upgrade.</td>
<td>None.</td>
<td>Select a different Image with a version higher than 11.3(0).</td>
</tr>
<tr>
<td>SWIM505</td>
<td>This NRP2 is in ROMMON state. Cannot perform software upgrade on this device.</td>
<td>The NRP2 device is not in normal mode.</td>
<td>Manually bring the device into the normal mode and retry the task.</td>
</tr>
<tr>
<td>SWIM5001</td>
<td>Cannot connect to the device devicename using protocol.</td>
<td>The device may not be reachable or there is invalid access information in the Device and Credential Repository.</td>
<td>Verify whether the device is reachable and the credentials in Device and Credential Repository are correct and retry the job.</td>
</tr>
<tr>
<td>SWIM5002</td>
<td>Cannot get details about Flash File system on the device.</td>
<td>Either the Flash device is not available or the Flash information format has changed.</td>
<td>Done.</td>
</tr>
<tr>
<td>SWIM5002</td>
<td>Only image versions 6.2 or above are supported through AUS.</td>
<td>The image version in the device is less than 6.2.</td>
<td>Manually upgrade the device to a version higher than 6.2.</td>
</tr>
<tr>
<td>SWIM4800</td>
<td>The version running on the device is less than the minimum supported version.</td>
<td>None.</td>
<td>Manually upgrade the device to the minimum supported version or higher.</td>
</tr>
<tr>
<td>SWIM5003</td>
<td>Cannot copy the image.</td>
<td>Either the server address is incorrect or the image is inaccessible to the device.</td>
<td>Check whether the server address is correct and whether the image is accessible to the device.</td>
</tr>
<tr>
<td>Message-ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWIM5004</td>
<td>Cannot initiate SNMP set option.</td>
<td>The SNMP Write Community String might be wrong.</td>
<td>Check whether the correct SNMP Write Community String is entered in Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM5005</td>
<td>Device reboot option failed.</td>
<td>The device is not configured for reboot. The command, <code>snmp-server system-shutdown</code>, should be in the running configuration on the device.</td>
<td>Modify the device configuration and retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: <code>NMSROOT\log\swim_debug.log</code> On Solaris and Soft Appliance: <code>/var/adm/CSCOpx/log/swim_debug.log</code></td>
</tr>
<tr>
<td>SWIM5006</td>
<td>Device reboot option failed.</td>
<td>The device is not configured for reboot. The SNMP Write Community string might be wrong.</td>
<td>The command SNMP server system shutdown should be in the running configuration on the device. Modify the device configuration and check whether the Write Community string is configured on the device is same as the one that is entered in Device and Credential Repository.</td>
</tr>
<tr>
<td>SWIM5007</td>
<td>CPU switchover failed.</td>
<td>Either the SNMP set failed or the device is not in hot standby mode or the two CPUs are not running similar images.</td>
<td>Do any of the following: • Check the SNMP credentials in the Device and Credential Repository • Ensure that the device is in hot standby mode, • Ensure that the two CPUs are running similar images, before attempting the switchover.</td>
</tr>
<tr>
<td>SWIM5008</td>
<td>Device not responding after running the <code>switch cpu</code> command.</td>
<td>—</td>
<td>Check the Bug Toolkit application for any known issues on the running image version.</td>
</tr>
<tr>
<td>SWIM5009</td>
<td>Device is not in HotStandby Mode. Switch Operation terminated.</td>
<td>The Standby CPU may be down.</td>
<td>Bring up the standby CPU and retry the job.</td>
</tr>
</tbody>
</table>

**Message-ID Error Message Probable Cause Possible Action**
## Job Approval

This section provides the troubleshooting information for the Job Approval application:

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>JBAP0001</td>
<td>Cannot enable approval for applications that do not have an Approver-List assigned to them</td>
<td>You have attempted to enable Approval without assigning a list to the application.</td>
<td>Go to the Approval &gt; AssignLists screen and assign a list to the application. Enable Approval again.</td>
</tr>
<tr>
<td>JBAP0002</td>
<td>Specify a valid E-mail address.</td>
<td>You have entered an invalid E-mail-address.</td>
<td>Enter a valid E-mail address</td>
</tr>
<tr>
<td>JBAP0003</td>
<td>Select at least one job.</td>
<td>You have attempted to perform an action on a job without selecting a job</td>
<td>Select a job before performing an action on it.</td>
</tr>
<tr>
<td>JBAP0004</td>
<td>Select only one job.</td>
<td>You have attempted to view JobDetails, with more than one job selected</td>
<td>Select only one job.</td>
</tr>
<tr>
<td>JBAP0005</td>
<td>List {0} has no users. To save the list successfully, add users and click Save</td>
<td>This is not an error. This is an Information message when you add a list for the first time.</td>
<td>Add users before saving the list</td>
</tr>
<tr>
<td>JBAP0006</td>
<td>{0} is not a valid Approver. Enter a user with Approver role</td>
<td>You have attempted to add a user who has not been added as Approver in CMF.</td>
<td>You must first add the user as Approver into CMF. Only then can you add this user into LMS.</td>
</tr>
<tr>
<td>JBAP0007</td>
<td>Select an Approver, to change E-mail.</td>
<td>You are trying to save without selecting a user.</td>
<td>Go back and select a user.</td>
</tr>
<tr>
<td>JBAP0008</td>
<td>List {0} already exists.</td>
<td>You have attempted to add a list that already exists.</td>
<td>Add the list with a different list name.</td>
</tr>
<tr>
<td>JBAP0009</td>
<td>Could not approve/reject the job {0}. Verify that the database and mail server are running.</td>
<td>Either approve/reject mails cannot be sent, or the database is not running.</td>
<td>Make sure mail server is configured properly and that the database is running.</td>
</tr>
<tr>
<td>JBAP0010</td>
<td>Cannot reject a job without comments.</td>
<td>You have attempted to reject a job without giving reasons for rejecting</td>
<td>Add comments if you want the job to be rejected.</td>
</tr>
<tr>
<td>JBAP0011</td>
<td>Select a future start date.</td>
<td>You have selected a past date while changing a job schedule</td>
<td>Select a future date.</td>
</tr>
<tr>
<td>JBAP0012</td>
<td>Job {0} is changed successfully.</td>
<td>Not an error message</td>
<td>None.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Error Message</td>
<td>Probable Cause</td>
<td>Possible Action</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>JBAP0013</td>
<td>Are you sure you wish to delete? Approval will be disabled for applications to which {list-name} is assigned.</td>
<td>Alert message before deleting – not an error message.</td>
<td>None.</td>
</tr>
<tr>
<td>JBAP0014</td>
<td>Enter a valid Approver-List name.</td>
<td>You may have entered invalid characters such as spaces in the Approver name.</td>
<td>Add a valid user-name</td>
</tr>
<tr>
<td>JBAP0015</td>
<td>{list-name} already exists.</td>
<td>You have attempted to add a list name that already exist</td>
<td>Select a different name</td>
</tr>
<tr>
<td>JBAP0016</td>
<td>{user-name} already exists.</td>
<td>You have attempted to add a user name that already exists.</td>
<td>Add a new user name. This field is case-sensitive.</td>
</tr>
<tr>
<td>JBAP0017</td>
<td>Are you sure you wish to delete? This will disable approval for applications having {user-name} as the sole approver.</td>
<td>Warning message for deleting a user. If you have enabled Approval for an application whose sole approver is this user, it will be disabled.</td>
<td>None.</td>
</tr>
<tr>
<td>JBAP0018</td>
<td>You have attempted an action without selecting a user. Select a user before performing the action.</td>
<td>User not selected.</td>
<td>Select a user before performing the action.</td>
</tr>
<tr>
<td>JBAP0019</td>
<td>You have attempted an action without selecting a list. Select a list before performing the action</td>
<td>List not selected.</td>
<td>Select a list before performing the action.</td>
</tr>
<tr>
<td>JBAP0021</td>
<td>Cannot save a list that has no approvers in it.</td>
<td>No approver available for the selected list.</td>
<td>Add approvers before trying to save the list.</td>
</tr>
<tr>
<td>JBAP0022</td>
<td>Cannot change schedule for {0}. A runtime error occurred when you tried to change the schedule of the job.</td>
<td>None.</td>
<td>This exception will appear in the MakerChecker.log in the following location: NMSROOT/log (On Solaris and Soft Appliance) NMSROOT\log (On Windows) where NMSROOT is the Cisco Prime install directory. Contact Cisco Technical Assistance Center (TAC) with this log file.</td>
</tr>
<tr>
<td>JBAP0024</td>
<td>Cannot send approval E-mails. Make sure that SMTP Server is configured correctly.</td>
<td>None.</td>
<td>Go to Admin &gt; System &gt; System Preferences and configure SMTP Server correctly.</td>
</tr>
</tbody>
</table>
## cwcli config

This section provides the troubleshooting information for the `cwcli config` commands:

<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
</table>
| CCLI0001   | Could not get any devices to work on. | This problem occurred because of any of the following:  
- Specified devices is not managed by LMS.  
- You have not used the correct Device Display name  
- DCR server is down | Do any of the following, depending on what caused the problem:  
- Specify valid devices that are managed by LMS  
- Use a valid Device Display name.  
- Use the `pdshow` command to verify whether the DCR server is running. |
| CCLI0002   | The job could not be created since no device is available. | This problem occurred because of any of the following:  
- You have entered invalid arguments for the command.  
- You have entered devices that are not managed by LMS.  
- CTMJrmServer and jrm are down.  
- ConfigMgmtServer process is down. | Do any of the following, depending on what caused the problem:  
- Enter valid arguments.  
- Verify that the devices you have entered are managed by LMS.  
- Use the `pdshow` command to verify whether the CTMJrm server and jrm are running.  
- The ConfigMgmtServer process should be up for the configuration Download and Fetch options. |
| CCLI0003   | Could not get results for devices within the specified time interval | Less timeout is configured | Either:  
- Increase the timeout value using the `-timeout` option.  
Or  
- Use Configuration Archive Job Browser to see the results. |
| CCLI0004   | Could not retrieve the Device Identification number for the device. | This problem occurred because of any of the following:  
- Specified devices are not managed by LMS.  
- You have not used the correct Device Display name  
- DCR server is down | Do any of the following, depending on what caused the problem:  
- Specify valid devices that are managed by LMS.  
- Use a valid Device Display name.  
- Use the `pdshow` command to verify whether the DCR server is running. |
| CCLI0005   | There are no archived configurations for this device | Sync Archive has not happened for the specified device. | Archive the configuration using the Sync Archive feature.  
For details on using the Synch Archive feature, see the Online Help. |
### Troubleshooting Tips and FAQs

<table>
<thead>
<tr>
<th>Message-ID</th>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCLI0006</td>
<td>Cannot create a temporary file to store the running configuration.</td>
<td>This problem occurred because of any of the following:</td>
<td>Do any of the following, depending on what caused the problem:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There is not enough space to create a file in your file system.</td>
<td>• Verify whether there is enough space to create a file in your file system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You do not have permissions to create a file in the specified location.</td>
<td>• Verify whether you have permissions to create a file in the specified location.</td>
</tr>
<tr>
<td>CCLI0007</td>
<td>Cannot retrieve the configuration file from the archive.</td>
<td>The specified version does not exist in the archive.</td>
<td>Verify whether the specified version exists in the archive. Use the <code>listversions</code> command to see the available versions.</td>
</tr>
<tr>
<td>CCLI0008</td>
<td>Could not create a temporary file in DCMA temporary directory.</td>
<td>This problem occurred because of any of the following:</td>
<td>Do either of the following, depending on what caused the problem:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There is not enough space to create a file in your file system.</td>
<td>• Verify whether there is enough space to create a file in your file system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You do not have permissions to create a file in the specified location.</td>
<td>• Verify whether you have permissions to create a file in the specified location.</td>
</tr>
<tr>
<td>CCLI0009</td>
<td>Cannot get running configuration.</td>
<td>The archive does not contain any versions for the device.</td>
<td>Verify whether the specified version exists in the archive. Use the <code>listversions</code> command to see the available versions.</td>
</tr>
<tr>
<td>CCLI0010</td>
<td>Device has only one version archived.</td>
<td>Synch Archive has not happened for the specified device</td>
<td>Archive the configuration using the Synch Archive feature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For details on using the Synch Archive feature, see the Online Help.</td>
</tr>
<tr>
<td>CCLI0011</td>
<td>The specified version of the configuration does not exist.</td>
<td>You have entered an invalid version of the configuration.</td>
<td>Use the <code>listversions</code> command to see the available versions and enter an existing version</td>
</tr>
<tr>
<td>CCLI0012</td>
<td>No baseline templates exist for this device.</td>
<td>None.</td>
<td>Use the <code>listversions</code> command to see the available baseline templates.</td>
</tr>
<tr>
<td>CCLI0013</td>
<td>Data file does not contain any device.</td>
<td>None.</td>
<td>Add the devices in the data file and try again</td>
</tr>
<tr>
<td>CCLI0014</td>
<td>The job could not be created because of the errors reported.</td>
<td>This problem occurred because of any of the following:</td>
<td>Do either of the following, depending on what caused the problem:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You have entered invalid arguments.</td>
<td>• Verify whether you have entered valid arguments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The data file is missing some parameters.</td>
<td>• Update the data file if there are missing parameters.</td>
</tr>
<tr>
<td>CCLI0015</td>
<td>You should not use the <code>-f</code> option with more than one device.</td>
<td>Multiple devices are specified for the command to be executed along with <code>-f</code> option</td>
<td>Use the <code>-input</code> option to specify the file for every device</td>
</tr>
</tbody>
</table>
Appendix C  Troubleshooting Tips and FAQs

Cwcli Export

This section provides the FAQs for the cwcli export tool:

- Q. What does cwcli export do?
- A. Cwcli export is a command line tool that also provides servlet access to export inventory, configuration and change audit data. You can use this tool to export inventory, configuration archive, and change audit data for devices in LMS, in the XML format.

You can use the cwcli export command to generate the Inventory and Configuration data in XML format. In addition to this, you can also export Change Audit data.

See these topics in the Configuration Management Help:
- Running cwcli export changeaudit for the usage and XML schema details.
- Running cwcli export config for the usage and XML schema details.
- Running cwcli export inventory Command for the usage and XML schema details.

Q. What is ComputerSystemPackage Class?
A. It is the class that contains the InstanceIDs of Cisco-Chassis and Cisco-NetworkElement, and relates the two.

Q. Where does cwcli export collect the configuration information from?
A. Cwcli export collects the running configuration data from the latest configuration in the Config Archive.

Q. Is the containment hierarchy in inventory schema exactly the same as that in CIM?
A. No. Although the containment hierarchy in inventory schema is based on Common Information Model (CIM), it does not follow the exact containment hierarchy because of the limitations in the LMS database schema.
Q. What is an XSD file?
A. XSD file is an XML based alternative to Document Type Definition (DTD). It is based on XML schema language which describes the structure of an XML document. An XML schema defines the legal building blocks of an XML document, just like a DTD.

An XML Schema:
- Defines elements that can appear in a document.
- Defines attributes that can appear in a document.
- Defines which elements are child elements.
- Defines the order of child elements.
- Defines the number of child elements.
- Defines whether an element is empty or can include text.
- Defines data types for elements and attributes.
- Defines default and fixed values for elements and attributes.

Q. What is the AdditionalInformation tag in the inventory schema used for?
A. The AdditionalInformation tag is provided to define information that is specific to a device. The inventory schema may not contain information for all the elements in all the devices supported by cwcli export. The AdditionalInformation tag addresses scenarios where the inventory schema does not have tags to define information that you want to collect for some of the elements in a particular device.

Q. How do I know what fields come under AdditionalInformation?
A. For this information, see the topic, Additional Information Table, in the Configuration Management Online Help.

Q. Where can I find information specific to a particular node which I can see in detailed device information but not in cwcli export?
A. For this information, see the topic, Additional Information Table, in the Configuration Management Online Help.

Q. How can I make use of the servlet interface?
A. You must write customized scripts which could connect to the servlet. The arguments and options have to be specified in XML format.

For more details, see the section, Using cwcli Commands in the Configuration Management Online Help.

Q. How can I get data for some particular entity from devices which are managed by different LMS servers?
A. You have to write a script to connect to different LMS servers and aggregate all data into a single file. After you get the aggregated data, you can parse it and get the data for any required entity.

Q. While using the -m option, can I use more than one E-mail id?
A. No. You can use only one E-mail address at a time, when you use the -m option of the cwexport command.
Q. Where can I get the descriptions of each node in the schema?
A. You can find the descriptions in the Configuration Management Online help. See the topic Overview: cwcli export and sub-topics.

Q. Why am I getting parse error when trying to parse some of the output files?
A. Some of the classes in IDU and Optical switches contains some special characters with ASCII code larger than 160. Most of the XML parsers does not support these characters and hence fails to parse these characters.

To overcome this, you have to manually search for those elements with special characters and append CDATA as given in the example below:
If there is an element,
```
checksum €º /checksum
```
you must change it to
```
checksum <![CDATA[€º ]]> /checksum
```

VRF Lite

Q. What is VRF Lite?
A. VRF Lite is an application that allows you to pre-provision, provision and monitor Virtual Routing and Forwarding-Lite (VRF-Lite) technology on an enterprise network.

Q. What is Network Virtualization?
A. Virtualization deals with extending a traditional IP routing to a technology that helps companies utilize network resources more effectively and efficiently. Using virtualization, a single physical network can be logically segmented into many logical networks. The virtualization technology supports multiple virtual routing instances of a routing table to exist within a single routing device and work simultaneously.

Q. What is VRF-Lite?
A. Virtual Routing and Forwarding - Lite (VRF - Lite) is the one of the simplest form of implementing virtualization technology in an Enterprise network. A Virtual Routing and Forwarding is defined as VPN routing/forwarding instance. A VRF consists of an IP Routing table, a derived forwarding table, a set of interfaces that use the forwarding table and set of routing protocols that determine what goes into the forwarding table.

Q. What are the pre-requisites to manage a device using VRF Lite?
A. The pre-requisites to manage a device in VRF Lite are:
1. The device must be managed by LMS.
2. The device must either be L2/L3 or L3 device
3. The devices failing to satisfy pre-requisite # 1 or #2, are not displayed in VRF Lite.
   The device must have the necessary hardware support. For more information on hardware support, see http://www.cisco.com/en/US/products/sw/cscowork/ps563/products_device_support_tables_list.html.
   If the device hardware is not supported then the device will be classified as Other devices
4. If a device does not support MPLS VPN MIB, it is classified as a capable device.
5. VTP Server must be support MPLS VPN MIB. If the VTP Server does not support MPLS VPN MIB, LMS will not manage VTP Clients.

Q. The device must be managed by LMS to exercise all the functionality of VRF. The desired device is not listed in the device selector for the VRF configuration workflows. What is the reason for a device not listed in the device selector?

A. A device is not listed in the device selector due to the following reasons:

All VRF Lite Configuration workflows like Create, Edit, Extend, Delete VRF and Edge VLAN Configuration.

A device will not be listed in the Device Selector, if a device does not satisfy the pre-requisites as mentioned in the Pre-requisites.

If VRF Lite Configuration workflow is either Edit VRF, or Delete VRF or Edge VLAN Configuration then a device will not be listed in the Device Selector, if a device is not participating in the selected VRF.

In the Readiness Report, a device listed as a supported device may be because it is not managed by LMS. You can check if a device is managed by LMS using the Device Management State Summary. You can access the Summary by selecting Device Management option.

In Extend VRF workflow, the devices listed in the Device Selector are the devices that are not participating in the selected VRF.

In Edge VLAN Configuration workflow, the devices listed in the Device Selector are only L2/L3 devices that are not participating in the selected VRF.

Q. What are the different categories in which the devices are managed by VRF Lite? Or what criteria are used by VRF Lite to categorize the devices in the network?

A. VRF Lite identifies the devices based on the minimum hardware and software support required to configure VRF on the devices.

Based on the available hardware and software support in the devices, VRF Lite classifies the devices into following categories:

- VRF Supported Devices– Represents the devices with required hardware and software support available to configure VRF on the devices.

- VRF Capable Devices – Represents the devices with required hardware support available. But the device software must be upgraded to support MPLS VPN MIB. For information on the IOS version that supports MPLS VPN MIB, refer [http://tools.cisco.com/ITDIT/MIBS/MainServlet](http://tools.cisco.com/ITDIT/MIBS/MainServlet).

VRF Lite classifies all the devices from Cat 3k and Cat 4k family of devices as VRF Capable devices as these devices do not have the required MPLS VPN MIB support.

- Other – Represents the devices without required hardware support to configure VRF. SysOID of the device needs to be checked.
Q. While performing the VRF Lite Configuration, VRF Lite application prompts the following messages:

“The device(s) with display name(s) are already locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time Or Ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

Or

Selected Device(s) are locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time Or Ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

The above messages appear even if no VRF Lite configuration is performed parallelly. Why do I get these messages?

A. The VRF Lite application prompts with these messages when some other configurations are performed simultaneously.

You can check the status of the configuration workflow using Resource Browser. The JOB Id/Owner column will give the details of the workflows currently running in the application.

These messages also appear if any VRF Lite configuration workflow is abruptly ended or an error has occurred while unlocking the device. You can release the locked devices only after ensuring that no other configuration workflows are running simultaneously. You can release the locked device using the Resource Browser option.

Note: If you unlock a device which is participating in a configuration workflow, the configurations details will be overwritten or corrupted. By default, a lock will be released after two hours.

Q. Sometimes, while performing VRF Lite configuration, I get the following message:

The device(s) with display name(s) are already locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time Or Ensure the devices are not used by configuration workflows and free the devices from **CS > Admin > Resource Browser**.

Or

Selected Device(s) are locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time OR Ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

Can I get the details of the user who has locked the devices to perform VRF Lite configuration?

A. You cannot get the details of user who has locked the devices to perform VRF Lite configurations.
Q. In the Create, Edit, or Extend workflow, the application do not list the Routing Protocols used while configuring VRF. The Routing Protocol information displayed is NA. What do I need to do to get the routing protocol configurations details?

A. When the Routing Protocol information displayed is NA, it means that the configuration details are not fetched successfully in LMS. You can schedule the Sync Archive job from Configuration > Configuration Archive > Synchronization.

Q. What are the details of the VRF Lite log files? In which location are the VRF Lite log files located?

A. The following are the details of the VRF Lite log files:
   1. Vnmserver.log – This log file logs the messages pertaining to the VNMServer process.
   2. Vnmcollector.log – This log file logs the messages pertaining to the VRF collection.
   3. Vnmclient.log – This log file logs the messages related to the User Interface.
   4. Vnmutils.log – This log file logs the messages pertaining to the utility classes used by VRF client and server.

The above-mentioned VRF Lite log files are located in the following location:

   In Solaris and Soft Appliance: /var/adm/CSCOpx/log/
   In Windows: NMSROOT\logs

Q. When is the VRF Collection process triggered?

A. Manually:
   You can manually schedule to run the VRF Collection process by:
   Providing the setting details using Admin > Collection Settings > VRF Lite.

   Automatically:
   If you enable the Run VRF Collector After Every Data Collection in the VRF Collector Schedule page. The VRF Collection process will be automatically triggered after the completion of Data Collection.
   You can reach the VRF Collector Schedule page using Admin > Collection Settings > VRF Lite.

Q. After the completion of the Data collection process, the VRF Lite Collector failed to run. What is the reason for failure?

A. Check if the Run VRF Collector After Every Data Collection option is enabled in the VRF Collector Schedule page. You can reach the VRF Collector Schedule page from Admin > Collection Settings > VRF Lite page.
Q. What is the reason for VLANs not getting populated in the VLAN to VRF Mapping page in the Create VRF and Extend VRF workflows?

A. The VLAN to VRF Mapping page lists the links connecting the source and the destination device. The VLANs are not listed in fields displaying the links in the VLAN to VRF Mapping page because VRF Lite tries to find a free VLAN in the devices connected using a link based on the following procedure:

1. An SVI, VRF Lite searches for free VLANs in the range 1-1005
2. An SI, VRF Lite searches for free VLANs in the range 1006-4005

Q. Why do I see the VRF description for all VRF(s) in home page as “Discovered by VRF Lite”?

A. While creating or extending VRF, the description that you have provided is deployed to the selected devices on which VRF is configured. But, the description provided while configuring or extending, is not read by the VRF Lite application. Instead, the VRF Lite application provides the default description for all VRFs as “Discovered by VRF Lite”.

Q. Why some port-channels are not discovered in LMS?

A. VRF Lite does not support port-channel and GRE Tunnel. Also, Currently VRF Lite supports only 802.1Q

Q. What is the tested number of devices support in VRF Lite?

A. In an Enterprise network, VRF Lite is tested to support the configuration of 32 VRFs with VRF configuration supported in 550 devices in your network. However, at a given time, you can select up to 20 devices and configure VRF using the Create, Edit and Extend VRF workflow.

Q. What are the property files associated with VRF Lite?

A. The following property files are associated with VRF Lite:

1. The property file used to provide the settings for Purge and Home page auto Refresh is:
   
   \textit{NMSROOT/vnm/conf/VNMClient.properties} (On Solaris and Soft Appliance) \\
   \textit{NMSROOT\vnm\conf\VNMClient.properties} (On Windows)

2. The property file used to provide the SNMP and VNMServer settings is:
   
   \textit{NMSROOT/vnm/conf/VNMServer.properties} (On Solaris and Soft Appliance) \\
   \textit{NMSROOT\vnm\conf\VNMServer.properties} (On Windows)

3. The property file that stores the SNMP Timeout and Retries that you have configured is:
   
   \textit{NMSROOT/vnm/conf/VRFCollectorSnmp.conf} (On Solaris and Soft Appliance) \\
   \textit{NMSROOT\vnm\conf\VRFCollectorSnmp.conf} (On Windows)
Q. In the Interface to VRF Mapping page for the Create, Edit and Extend VRF workflow, why are values for the IP Address and SubnetMask fields empty?
A. If the physical interface that links two devices is not configured with an IP Address, then the IP Address and the SubnetMask fields are empty.

Q. What is protocol ordering for configuration workflows?
A. Configuration workflow uses the protocol ordering similar to ordering used by NetConfig.
   Choose the NetConfig as Application Name from using Admin > Collection Settings > Config > Config Transport Settings page. You can view the protocol ordering in the Transport Settings page.

Q. What is protocol ordering for troubleshooting?
A. Troubleshooting VRF workflow uses the protocol ordering similar to ordering used by NetShow in LMS.
   Choose the NetShow as Application Name from using Admin > Collection Settings > Config > Config Transport Settings page. You can view the protocol ordering in the Transport Settings page.

Q. If you configure commands to be deployed to two different devices, will the commands be deployed parallelly or serially?
A. The commands will be deployed to multiple devices parallelly, whereas a series of commands with-in a single device, will be deployed in serial manner.

Q. Which VRF Lite configuration jobs that are failed can be retried?
A. You can retry all the VRF Lite Configuration jobs which are failed. VRF Lite Configuration jobs are the jobs pertaining to Create, Edit, Extend, Delete VRF and Edge VLAN Configuration workflow.

Q. In the Troubleshooting VRF page, after selecting the source device, no VRFs are listed in the VRF List to troubleshoot. Why?
A. Initially, check if a VRF is configured on the selected source device. The VRF list in the Troubleshooting page enlists the VRF(s) configured in the selected source device as well as in the Global Table, which refers to the global routing table.

Q. Which interfaces are displayed in the Troubleshooting VRF page
A. When a VRF is selected then all the interfaces that are configured with the selected VRF in the corresponding device is listed.
   If you select VRF as “Global Table”, then the application displays all the interfaces that are not configured to any VRF
Q. In some scenarios, the VRF configuration commands are pushed to unselected devices. What is the reason?

A. In the following scenarios, the VRF configuration commands are pushed to unselected devices:

The VLANs are created in the VTPServer by default. In any VRF Lite Configuration workflow, if you create a VLAN in VTP Client devices, then VRF Lite application finds the corresponding VTP Server and create VLANs in that device.

In Delete VRF workflow, the virtualized interface in the connecting device will also be deleted, even if the device is not selected.

Q. Why the FHRP and DHCP configurations are not shown in VRF Lite?

A. VRF Lite does not fetch the details for the FHRP or DHCP configuration from the device. Also, VRF Lite won’t put the list of vlan(s) allowed on a trunk

The Protocols and DHCP Server details for existing or newly created SVIs are not fetched from the selected devices.
INDEX

A

access
  privileges for NetConfig jobs, assigning 5-4
  Telnet and SSH, configuring 9-40
Adhoc task, in NetConfig
  about 5-40
  using 5-34
applications
  Config Editor 8-1
  Configuration Management 6-1, 7-1
  NetConfig 5-1
  Software Management 9-1
Archive Management (part of Configuration Management)
  archive status, checking 6-3
  custom search queries
    creating 6-25
    deleting 6-27
    editing 6-27
    running 6-26
  search report, displaying 6-28
Authentication Proxy task in NetConfig 5-41
authorizing a distribution job, in Software Management 9-51

B

Banner task in NetConfig 5-43
baseline configurations
  Baseline Compliance report 7-27
  Baseline Configs window 7-5
  commands, deploying 7-28
  compliance jobs, deleting 7-40
  non-compliance report, running 7-37
baseline configuration templates 7-11
  creating
    advanced 7-16
    deleting 7-11
    editing 7-9
    exporting 7-10
    importing 7-24

C

CA (Certification Authority) task in NetConfig 5-46
Cable BPI/BPI+ task in NetConfig 5-95
Cable DHCP-GiAddr and Helper task in NetConfig 5-97
Cable Downstream task in NetConfig 5-98
Cable Interface Bundling task in NetConfig 5-104
Cable Spectrum Management task in NetConfig 5-104
Cable Trap Source task in NetConfig 5-106
Cable Upstream task in NetConfig 5-100
Catalyst devices
  1900/2820 device upgrade recommendations 9-95
  upgrade recommendations, understanding 9-94
cautions regarding
  NetConfig’s Adhoc task 5-40
  NetConfig commands in a user-defined template 5-26
CDP task in NetConfig 5-44
Change Audit, using
troubleshooting C-73
CIP microcode image types, and software image upgrades 9-49
Cisco.com
  adding images from 9-12
  Software Management tasks, and 9-5
software repository, synchronizing with 9-23
Cisco IOS device upgrade recommendations 9-93
CiscoWorks Server, and Software Management 9-4
CLI utilities
cwcli A-1
PTT A-110
commands A-113
PTT features A-110
SWIMcli A-116
execute SWIM cli remotely A-119
running swim cli commands A-116
syslogConf A-114
syslogConf.pl utility A-114
CLI utilities (see cwcli config) A-1
command reference
(see also cwcli config, using) A-1
command-line tool
see cwcli netconfig command 5-128
Compliance and Audit Manager
managing policy profiles 4-8
adding policy profiles 4-8
deleting policy profiles 4-10
duplicating policy profiles 4-9
running compliance check 4-10
viewing job history 4-11
config_DeployBaselineTempUI 7-28
Config CLI, troubleshooting C-75
Config Editor
editor manager, working with
in processed mode 8-10
Config Editor, using
benefits of 8-3
changes in this release 8-8
configuration files
closing 8-20
downloading 8-33
editing 8-9
exporting to HTML format 8-17
opening 8-26
removing 8-13
saving 8-14
configuration restore operation 8-32
configuration tools 8-20
to check syntax 8-23
to compare versions 8-22
to display changes 8-23
downloading configuration files 8-33
files, selecting 8-35
job password policy 8-40
job scheduling 8-36
job status, viewing 8-40
starting a job 8-33
work orders, reviewing 8-39
editor manager, working with 8-9
Config Editor, using jobs, in 8-11
credentials, modifying with 8-12
processed mode 8-10
open files, viewing list of 8-25
opening a file 8-26
by device and version 8-26
from an external location 8-31
viewing a list of open files 8-25
preferences, setting up 8-8
printing a file 8-16
restore operation 8-32
search and replace in configuration files 8-15
tasks in 8-2
undoing all edits 8-15
Config Editor application
troubleshooting C-11
Configuration Archive
archive searches 6-24
configuration files
changes to
displaying 8-23
closing 8-20
currently open, viewing list of 8-25
downloading 8-33
files, selecting 8-35
job password policy 8-40
job scheduling 8-36
job status, viewing 8-40
starting a new job 8-33
work orders, reviewing 8-39
editing 8-9
exporting to HTML format 8-17
opening 8-26
by baseline 8-29
by device and version 8-26
by pattern search 8-27
external files 8-31
printing 8-16
removing 8-13
saving 8-14
syntax checking 8-23
about 8-23
external interface 8-23
versions of, comparing 8-22
Configuration Management, using 6-1, 7-1
archival reports 6-4
Failed Devices report 6-5
Partially Successful Devices report 6-6
Successful Devices report 6-5
Archive Management Job Browser
deleting a job 6-49
job details, viewing 6-50
retrying a job 6-46
stopping a job 6-48
archive searches with custom queries 6-24
creating queries 6-25
deleting queries 6-27
editing queries 6-27
running queries 6-26
search report, displaying 6-28
archive status, checking 6-3
comparing configurations 6-33
base config with latest config of multiple devices 6-38
Config Diff Viewer 6-41
running versus latest archived 6-34
startup versus running 6-33
two versions of different 6-36
two versions of same 6-35
Config Editor option
functional flow (figure) 8-3
tasks (table) 8-3
Configuration Archive Job Browser 6-44
collection version tree 6-12
Config Viewer 6-13
job scheduling
Sync Archive 6-7
Sync on Device 6-10
labels, configuring 6-20
creating 6-21
deleting 6-24
editing 6-22
purging 6-24
viewing 6-23
Quick Configuration Download feature
about 6-12
using 6-18
reports
archive search report 6-28
Configuration Version summary 6-16
Device Configuration Quick View 6-30
Out-of-Sync report 6-10
Search Archive Result 6-30
troubleshooting C-1
configuring
inter-VLAN routing 11-30
on an external router 11-32
on RSM, MSFC3, and L2/L3 devices 11-31
Configuring VRF 12-2
Routing Protocol Configuration 12-9
Summary 12-11
Create VRF
    Interface Mapping to VRF
        Preferred Virtual Interfaces  12-5
Crypto Map task in NetConfig  5-47
cwcli config, using  A-1
    batch processing  A-2, A-7
    CLI framework  A-2, A-7
    command parameters  A-11
        all commands  A-13
        compare command  A-11
        delete command  A-13
    core options and nmconfig equivalents  A-19
    examples of cwcli config and nmconfig equivalents  A-20
    getting started  A-8
    man page information  A-20
        arguments and options, about  A-22
        function-dependent options  A-22
        function-independent options  A-22
        function-specific options  A-23
        input list file format  A-25
        mandatory arguments  A-22
        -view option arguments  A-25
    man page information for subcommands  A-25
        compare  A-26
        compareanddeploy  A-27
        comparewithbaseline  A-27
        delete  A-27
        deploybaseline  A-28
        export  A-28
        get  A-28
        import  A-29
        listlock  A-29
        put  A-29
        reload  A-30
        run2start  A-30
        start2run  A-30
        write2run  A-31
        write2start  A-31
    overview  A-2, A-7
    running  A-10
        additional information  A-11
        on multiple devices  A-11
    syntax examples  A-15
    uses  A-8
        comparing configurations  A-10
        deleting configurations  A-10
        device and archive updates  A-8
        remote access  A-10
cwcli netconfig command  5-128
    man page  5-128

D
deleting
    images from the software repository  9-24
devices, managing
    configurations, verifying  5-3
    credentials, verifying  5-3
    images from, adding to the software repository  9-15
    prompts, verifying  5-4
device security, modifying  5-3
DNS task in NetConfig  5-49
downloading configuration files  8-33
    files, selecting  8-35
    job password policy  8-40
    job scheduling  8-36
    job status, viewing  8-40
    starting a job  8-33
    work orders, reviewing  8-39

E
Edge VLAN Configuration  12-31
    Layer 3 Features  12-35
    Summary  12-36
    Trunk Configuration  12-35
VLAN to VRF Mapping 12-33
Editing VRF 12-13
editor manager (see under Config Editor) 8-9
eem
  EEM NetConfig tasks
    EEM environmental variable task 5-116
    embedded event manager task 5-117
Enable  C-4
Enable Password task in NetConfig 5-50
EtherChannel 11-46
  configuring 11-46
  understanding 11-46
  using 11-46
Ethernet VLANs
  about 11-15
  creating 11-16
exporting
  configuration files, to HTML format 8-17

F
files
  configuration (see configuration files) 8-9
Software Management, locating 9-105

G
gold
  NetConfig tasks for GOLD
    GOLD boot level task 5-123
    GOLD monitoring test task 5-124

H
How  C-2
HTML format, exporting a configuration file to 8-17
HTTP, configuring for software image upgrades 9-49
HTTP Server task in NetConfig 5-53

I
IGMP Configuration task in NetConfig 5-57
IKE (Internet Key Exchange) Configuration task in NetConfig 5-59
images
  adding to software repository 9-11
    from a file system 9-17
    from a URL 9-19
    from Cisco.com 9-12
    from devices 9-15
    from the network 9-21
attributes 9-26
  default attribute values, understanding 9-28
  editing and viewing 9-28
  finding missing attribute information 9-28
  understanding 9-27
  deleting 9-24
  distribution by 9-60
  searching for 9-26
Interface IP Address Configuration task in NetConfig 5-58
IVR (inter-VLAN routing)
  configuring 11-30
    on on external router 11-32
    on RSM, MSFC3, and L2/L3 devices 11-31
  understanding 11-30
  using 11-30

J
Job Approval, using
  troubleshooting  C-73

L
Local Username task in NetConfig 5-54
Login  C-3
MICA portware image types, and software image upgrades 9-49
microcode and modem firmware requirements for software image upgrades 9-49
Microcom firmware image types, and software image upgrades 9-49

N

NetConfig, using 5-1
before you begin 5-3
device configurations, verifying 5-3
device credentials, verifying 5-3
device prompts, verifying 5-4
device security, modifying 5-3
job approval, enabling 5-4
job policies, default, configuring 5-4
task access privileges, assigning 5-4
cwcli netconfig command description 5-128
interactive commands, handling 5-33
.ini file 5-34
user-defined templates 5-34
jobs, browsing and editing 5-18
job details, viewing 5-23
multi-line commands, viewing 5-34
port based system-defined tasks
Catalyst Integrated Security Features task 5-114
Manage Auto Smartports task 5-111
PoE task 5-113
Smartports task 5-112
rolling back configuration changes 5-5
rollback commands, creating 5-5
rollback on failure, configuring 5-5
system-defined tasks 5-35
Adhoc tasks 5-40
Authentication Proxy task 5-41
Auto Smartports task 5-107
Banner task 5-43
Cable BPI/BPI+ task 5-95
Cable DHCP-GiAddr and Helper task 5-97
Cable Downstream task 5-98
Cable Interface Bundling task 5-104
Cable Spectrum Management task 5-104
Cable Trap Source task 5-106
Cable Upstream task 5-100
CDP task 5-44
Certification Authority (CA) task 5-46
Crypto Map task 5-47
dialog box, understanding 5-39
DNS task 5-49
Enable Password task 5-50
HTTP Server task 5-53
IGMP Configuration task 5-57
IKE Configuration task 5-59
Interface IP Address Configuration task 5-58
Local Username task 5-54
RADIUS Server Configuration task 5-63
RCP Configuration task 5-66
Reload task 5-67
SNMP Community Configuration task 5-68
SNMP Security Configuration task 5-70
SNMP Traps Configuration task 5-72
SSH Configuration task 5-87
Syslog task 5-83
TACACS+ Configuration task 5-89
TACACS Configuration task 5-88
Telnet Password Configuration task 5-91
Transform task 5-92
User-Defined Protocol task 5-94
Web User task 5-94
tasks 5-2
tasks, assigning to users 5-33
troubleshooting C-9
user-defined tasks, creating and editing 5-25
user permissions, understanding 5-5
administrator task permissions 5-6
job approval permissions 5-6
job editing permissions 5-6
user-defined task permissions 5-6
NTP Server Configuration task in NetConfig 5-61

O

overviews
  editing a configuration file in Config Editor 8-9
  of cwcli config A-2, A-7
  opening a configuration file 8-26
  syntax checking in Config Editor 8-23

P

Pari
  managing policy groups 4-1
    adding policy groups 4-1
    deleting policy 4-7
    deleting policy groups 4-7
    duplicating policy groups 4-5
    editing policy groups 4-6
PIX Firewall devices, upgrade recommendations, understanding 9-95
PVLAN (private VLAN)
  creating
    about 11-26
    primary 11-26
    promiscuous ports, configuring 11-28
    secondary 11-27
    secondary, associating ports with 11-28
  deleting 11-29
  types 11-24
    promiscuous ports 11-24
    PVLAN host ports 11-24
    PVLAN trunk ports 11-25
  understanding 11-24
  using 11-25

R

RADIUS Server Configuration task in NetConfig 5-63
rcp
  configuring for software image upgrades 9-43
    on Solaris 9-43
  selecting as active file transfer method 9-45
RCP Configuration task in NetConfig 5-66
  rolling back configuration changes in NetConfig 5-5
  rollback commands, creating 5-5
  rollback on failure, configuring 5-5
Route Distinguisher 12-4

S

searching for images 9-26
security
  advantages of VLANs in 11-3
  security warning regarding -p A-23
Smart Call Home
  NetConfig tasks
    Smart Call Home task 5-76
SNMP
  SNMP Community Configuration task in NetConfig 5-68
  SNMP Security Configuration task in NetConfig 5-70
  SNMP Traps Configuration task in NetConfig 5-72
Software Management, using 9-1
  distribution by devices 9-51
  distribution by images 9-60
  distribution job, authorizing 9-51
  environment, setting up 9-4
    Cisco.com, logging into 9-5
    CiscoWorks Server 9-4
  files, locating 9-105
  Job Approval 9-6
  patch distribution 9-67
    by device 9-67
by patch 9-71
remote staging and distribution 9-75
software distribution 9-29
  methods 9-35
  upgrade analysis 9-29
  Upgrade Analysis report, understanding 9-32
  upgrades, configuring devices for 9-38, 9-47
  upgrades, planning 9-37
  upgrades from Cisco.com, planning 9-30
  upgrades from the software repository, planning 9-31
software image repository, maintaining 9-38
Software Management jobs 9-95
  deleting 9-100
  failed job, retrying 9-98
  schedule, changing 9-97
  stopping 9-100
  successful, undoing 9-99
software repository 9-7
  image attributes 9-26
  images, adding 9-11
  images, deleting 9-24
  searching 9-26
  synchronization 9-8
  synchronization jobs, removing 9-11
  synchronization report, scheduling 9-10
  synchronization report, viewing 9-11
  synchronizing with Cisco.com 9-23
support for IOS software modularity 9-65
troubleshooting C-13
upgrade recommendations, understanding 9-93
  for Catalyst devices 9-94
  for Catlyst 1900/2920 devices 9-95
  for Cisco IOS devices 9-93
  for PIX Firewall devices 9-95
  for VPN 3000 series devices 9-95
upgrades, scheduling 9-50
user-supplied scripts, understanding 9-102
Syslog task in NetConfig 5-83

T
TACACS+ Configuration task in NetConfig 5-89
TACACS Configuration task in NetConfig 5-88
TACACS credentials, interpreting C-2
  custom TACACS prompts, troubleshooting C-5
  enable login authentication
    in SSH mode C-4
    in Telnet mode C-4
  login authentication
    in SSH mode C-3
    in Telnet mode C-3
Telnet
  Telnet Password Configuration task in NetConfig 5-91
Template Center 3-1
  accessing template center 3-2
    system-defined templates 3-2
  assigning templates to user 3-26
  deploying templates 3-15
  guidelines 3-31
  job browser 3-27
  managing templates 3-18
    deleting 3-20
    editing 3-19
    exporting 3-20
    importing 3-22
    importing from Cisco Configuration Professional file 3-23
    importing from XML file 3-22
    importing running config from device 3-25
    viewing template details 3-21
  multi-line commands, handling 3-21
TFTP, configuring for software image upgrades 9-47
  on Solaris 9-47
  on Windows 9-47
token ring bridge relay function VLANS (see trCRF VLANS) 11-18
Transform task in NetConfig 5-92
trBRF VLANS
creating 11-17
trCRF VLANS
creating 11-18
troubleshooting C-1
Change Audit C-73
Config CLI C-75
Config Editor C-11
Config Management C-1
Job Approval C-73
NetConfig C-9
Software Management C-13
trunking 11-40
characteristics of trunks 11-41
considerations in 11-40
DTP (Dynamic Trunking Protocol) 11-40
encapsulation types 11-42
trunk encapsulation 11-41

U
upgrades
analyzing prerequisites and impact 9-29
configuring devices for 9-38
  additional requirements, meeting 9-39
  additional SFB checks 9-40
HTTP 9-49
  microcode requirements 9-49
minimum requirements, meeting 9-39
modem firmware requirements 9-49
rcp, configuring 9-43
SCP, configuring 9-42
Telnet and SSH access, configuring 9-40
TFTP, configuring 9-47
distributing by devices
  advanced 9-55
  basic 9-51
distributing by images 9-60
distribution job, authorizing 9-51
distribution methods 9-35
planning 9-37
  from Cisco.com 9-30
  from the software repository 9-31
  identifying possible changes 9-37
  prerequisites, satisfying 9-37
  software repository, maintaining 9-38
  testing the new images 9-38
recommendations, understanding 9-93
  for Catalyst 1900/2820 devices 9-95
  for Catalyst devices 9-94
  for Cisco IOS devices 9-93
  for PIX Firewall devices 9-95
  for VPN 3000 devices 9-95
remote staging and distribution 9-75
  scheduling 9-50
Upgrade Analysis report, understanding 9-32
User-Defined Protocol task in NetConfig 5-94
user-supplied scripts for software management 9-102

V
viewing
  Software Management synchronization reports 9-11
Virtual Switching System
  about Virtual Switching System (VSS) 10-1
  configuration process 10-2
  prerequisites 10-2
  standalone to VSS mode 10-5
  support for VSS 10-9
  Virtual to standalone 10-11
VLAN and VTP management 11-1
  (see also VLANS) 11-2
EtherChannel 11-46
  configuring 11-46
  understanding 11-46
Index

using 11-46
inter-VLAN routing
configuring 11-30
understanding 11-30
using 11-30
PVLAN (private VLAN)
creating 11-26
deleting 11-29
types 11-24
understanding 11-24
using 11-25
reports 11-21
trunking 11-40
characteristics of trunks 11-41
considerations in 11-40
DTP (Dynamic Trunking Protocol) 11-40
capsulation types 11-42
trunk encapsulation 11-41
VLAN Port Assignment (see VLAN Port Assignment) 11-47
VTP (see VTP) 11-33
VLAN Port Assignment 11-47
starting 11-48
understanding 11-48
using 11-49
VLANs
about 11-2
advantages of 11-2
in adds, moves, and changes 11-2
in broadcast activity 11-2
in security 11-3
components of 11-3
deleting 11-19
types supported by Campus Manager
trCRF VLANs 11-18
types supported by LMS 11-4
Ethernet VLANs 11-15
VPN 3000 devices, upgrade recommendations,
understanding 9-95

VRF Lite 12-1
VTP (VLAN trunking protocol) 11-33
domain components 11-34
domains, about 11-34
using 11-37
reports, displaying 11-37
views, using 11-39
version 3 11-35

W

warnings
regarding security and -p A-23
Web User task in NetConfig 5-94
What C-5
what’s new in this release
in Config Editor 8-8
Windows, and the NetConfig .ini file 5-34