



Cisco LAN Management Solution 2.5 Deployment Guide

Corporate Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<http://www.cisco.com/en/US/products/netmgts/index.html>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 526-4100



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PDx, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Cisco LAN Management Solution 2.5 Deployment Guide
Copyright © 2005 Cisco Systems, Inc. All rights reserved



CONTENTS

CHAPTER 1

Cisco LAN Management Solution 2.5 Deployment Guide 1-1

- Introduction 1-1
 - Applications Included in LMS 2.5 1-1
 - Versions Available for LMS 2.5 1-2
 - Upgrading From LMS 2.x to LMS 2.5 1-2
- LMS 2.5 Architecture 1-3
 - Common Services and DCR 1-3
- Device and LMS Workflow 1-4

CHAPTER 2

Setting Up Devices on the Network 2-1

- Device Setup Elements 2-1
 - System Name 2-1
 - Domain Name 2-2
 - SNMP Settings 2-2
 - Enabling SNMP v3 on Cisco IOS Devices 2-2
 - Enabling SNMP v3 on Catalyst OS Devices 2-3
 - Enabling SNMP v1 or v2c on Cisco IOS Devices 2-3
 - Enabling SNMP v1 or v2c on Cisco Catalyst OS Devices 2-3
 - Enabling Traps in Catalyst OS Devices to Be Sent to a Particular Host 2-3
 - Enabling Traps in IOS Devices to Be Sent to a Particular Host Using SNMP v2c 2-3
 - System Reload 2-4
 - Command Line Prompts 2-4
 - Telnet/SSH 2-4
 - Syslog Messages 2-5
- Configuring Protocols 2-6
 - Cisco Discovery Protocol (CDP) 2-6
 - Enabling or Disabling CDP on Cisco IOS Devices 2-6
 - Enabling or Disabling CDP on Cisco Catalyst OS Devices 2-6
 - Remote Copy Protocol 2-7
 - Secure Copy Protocol (SCP) 2-7
 - HTTP and HTTPS Servers 2-8
 - Configuring Multiple Spanning-Tree 2-9
 - Configuring Multiple Instance Spanning-Tree 2-10
 - Configuring Per-VLAN Spanning Tree+ 2-11

For More Information on the Spanning Tree Protocol	2-12
Default Values for PVST+ Configuration	2-12
Configuring VLAN Trunk Protocol (VTP)	2-13
Best Practice Recommendations	2-14
Enabling Trunking on Catalyst Switch Ports	2-14

CHAPTER 3

Cisco LAN Management Solution 2.5 Installation Requirements 3-1

Solaris OS Installation Requirements	3-1
Recommended Solaris Disk Layout	3-1
Backup Recommendations	3-2
Windows OS Installation Requirements	3-2
Recommended Order for Installing LMS Applications	3-2
Ports Used by LMS Applications	3-3
Licensing Terminology and Process	3-4

CHAPTER 4

Initial Setup of the LAN Management Solution 2.5 Server 4-1

Application Mode Settings in LMS Applications	4-1
Protocol Setup	4-2
Configuration Management	4-2
Set Up Protocol Ordering	4-3
Software Image Management	4-3
Setting Up Security	4-4
Certificate Setup	4-4
Setting Up the System Identity User	4-4
Setting Up a Peer Server Account	4-4
Enabling HTTPS on an LMS Server	4-5
Notes	4-5
Single Sign-On	4-5
Setting Up the Cisco Secure Access Control Server	4-6
Integrating LMS Servers with ACS	4-6
Set Up the System Identity and Peer Server Account Users in the LMS Server	4-6
Set Up the ACS Server	4-6
Set Up the LMS Server to Communicate with the ACS Server	4-7
Configure the System Identity User in the ACS Server	4-7
Configure the ACS Server to Change Default Permissions and Task to Role Mapping (Optional)	4-8
Create Network Device Groups, User Groups and Assign Roles to Network Device Groups in the ACS Server	4-8
Setting Permissions for Performing Tasks on Devices	4-9

CHAPTER 5**Populating Devices in Cisco LAN Management Solution 2.5 5-1**

- Campus Manager Device Discovery 5-1
- Defining a Seed Device in Campus Manager 5-2
- Bulk Device Import to Device and Credentials Repository 5-2
- Device Credentials Update 5-3
- Device Management 5-4
 - Adding Devices to RME From DCR 5-4
 - Viewing Configuration Collection Status in RME 5-4
 - Collecting Devices' Startup and Running Config 5-4
 - Verification of Device Import Status in LMS Applications 5-5
 - Resource Manager Essentials 5-5
 - Campus Manager 5-5
 - Device Fault Manager 5-5

CHAPTER 6**Server Administration in Cisco LAN Management Solution 2.5 6-1**

- Common Services 6-1
 - Creating User Defined Groups 6-2
- Backing Up LMS Data 6-2
- Restoring LMS Data 6-3
- Campus Manager 6-3
 - Campus Manager Device Discovery 6-3
 - Optimizing Network Discovery 6-4
 - Campus Manager Data Collection 6-4
 - Optimizing Data Collection 6-5
 - User Tracking Module 6-5
 - Initiating a UT Major Discovery 6-5
 - Purge Policies 6-6
 - Hierarchical Groups in Campus Manager 6-6
- Resource Manager Essentials 6-7
 - Inventory Collection and Polling 6-7
 - Changing the Job Schedule Default Settings 6-7
 - Configuration File Collection and Polling 6-7
 - Default Protocols Used for Configuration Fetch and Deploy 6-8
 - RME Purge Policies 6-8
 - Specifying When to Purge Configuration Files 6-8
 - Periodic Purging of Syslog Messages 6-9
 - Purging Change Audit Data 6-9
 - Defining Syslog Message Filters 6-10

Change Audit	6-10
Setting Up Inventory Filters	6-10
Defining Exception Periods	6-10
SWIM Baseline Collection	6-11
Synchronizing the Software Repository	6-11
Managing RME Jobs	6-11
Importing Devices Into Internetwork Performance Monitor	6-13
Device Fault Manager	6-13
Daily Purging Schedule	6-14
Forwarding SNMP Traps	6-14
Receiving SNMP Traps	6-14
Default SMTP Server	6-14
Rediscovery	6-14
Group Administration	6-15
Setting Polling and Threshold Parameters	6-15
Creating Views	6-15
CiscoView	6-15
Device Center	6-16
Launching Debugging Utilities	6-16

CHAPTER 7

Network Management in Cisco LAN Management Solution 2.5 7-1

Fault Monitoring	7-1
Set Up Tasks	7-1
Fault and Alerts Notification Services	7-2
Fault History	7-3
Alerts and Activities	7-3
Baseline Configuration	7-3
Data Extraction from LMS Applications	7-3
Campus Data Extraction Engine	7-3
The cmexport Utility	7-4
Core Commands	7-4
Archival Locations	7-4
Possible Combinations of cmexport Commands	7-5
Layer 2 Topology or Discrepancy Commands	7-5
Servlet Access to the Data Extraction Engine	7-6
Resource Manager Essentials Data Extraction Engine	7-8
Command-Line Syntax	7-9
Data Archiving Location	7-9
RME Servlet	7-10

Internetwork Performance Monitor Export	7-11
The IPM Export Command	7-12
The DCR Command Line Interface	7-12
User Tracking Reports	7-13
Configuring Syslog on Devices	7-13
VLAN Recommendations	7-14
Viewing the Least Depth Spanning Tree Recommendation	7-14
Ether Channel and Trunk Deployment	7-15
Ether Channel Configuration	7-15
Trunk Configuration	7-15
Configuration File Change Management	7-16
RME Config Editor	7-16
NetConfig Templates	7-16
Change Audit Reports	7-16

INDEX



Cisco LAN Management Solution 2.5 Deployment Guide

Introduction

Network management is critical in today's networks, helping enterprises deploy and manage solutions. With increasing reliance on networks to increase productivity, enterprises are confronted with an ever growing network size. Such increase in the number of network elements creates a challenge for network administrators. How does an enterprise effectively deploy and maintain their network devices?

CiscoWorks LAN Management Solution (LMS) provides the integrated management tools needed to simplify the configuration, administration, monitoring, and troubleshooting of Cisco networks. It provides IT organizations an integrated system for sharing device information across management applications, automation of device management tasks, visibility into the health and capability of the network, and identification and localization of network trouble. By using common centralized systems and network-inventory knowledge, CiscoWorks LMS delivers a unique platform of cross-functional management capabilities that reduces network administration overhead and provides upper-layer systems integration.

This deployment guide considers scenarios where all applications reside on a single server and provides tips and suggestions on configuring the server. Some concepts related to multi-server deployment that have been introduced in LMS 2.5 will also be discussed.

Applications Included in LMS 2.5

LAN Management Solution (LMS) 2.5 includes the following components:

- CiscoWorks Common Services 3.0

Common Services 3.0 provides a set of shared application services that are used by all LMS applications. Common Services 3.0 includes both CiscoView 6.1 and Integration Utility 1.6.

- CiscoView 6.1 provides “front panel” graphical displays of Cisco devices, allowing users to easily interact with device components to change configuration parameters and monitor statistics.
- Integration Utility 1.6 is an integration module that supports third-party network management systems.

- Resource Manager Essentials (RME) 4.0

To support life cycle management, RME provides the ability to manage device inventory and audit changes, configuration files, and software images—as well as Syslog analysis.

- Campus Manager (CM) 4.0

Campus Manager provides the ability to visualize network topology, manage VLANs, detect network discrepancies, and provide Layer 2 and Layer 3 data and voice traces and end-host user information.

- Device Fault Manager (DFM) 2.0

Device Fault Manager provides the ability to monitor device faults in real-time and determine the root cause by correlating device-level fault conditions. DFM can issue notifications of critical network conditions via email or pager. Fault History lets the operator store and access historical information about alerts and faults that are detected and processed by DFM.

- Internetwork Performance Monitor (IPM) 2.6

Internetwork Performance Monitor measures network performance based on the *synthetic traffic generation* technology within the Cisco IOS® software, which is known as Cisco IOS IP SLA. Using synthetic traffic gives the network manager a high degree of flexibility in selecting the end points in a network between which network performance will be measured. This flexibility makes IPM a highly effective performance-troubleshooting tool.

IPM takes advantage of Cisco IOS IP SLA technology by configuring network performance agents, called *collectors*, in the router. These collectors, as part of their configuration, include a *source* router, a *target* device and an *operation* type.

Versions Available for LMS 2.5

You can select one of the following two versions of LMS 2.5:

- Restricted Version

The Restricted version of LMS 2.5 is for customers transitioning from LMS 1.x Unlimited version or from LMS 2.x to LMS 2.5. The device limit for this version is 300 devices.

- Large Enterprise Version

The Large Enterprise version is for customers transitioning from LMS 1.x Unlimited version or from LMS 2.x to LMS 2.5. This version has no limit on the number of devices it can support.

Upgrading From LMS 2.x to LMS 2.5

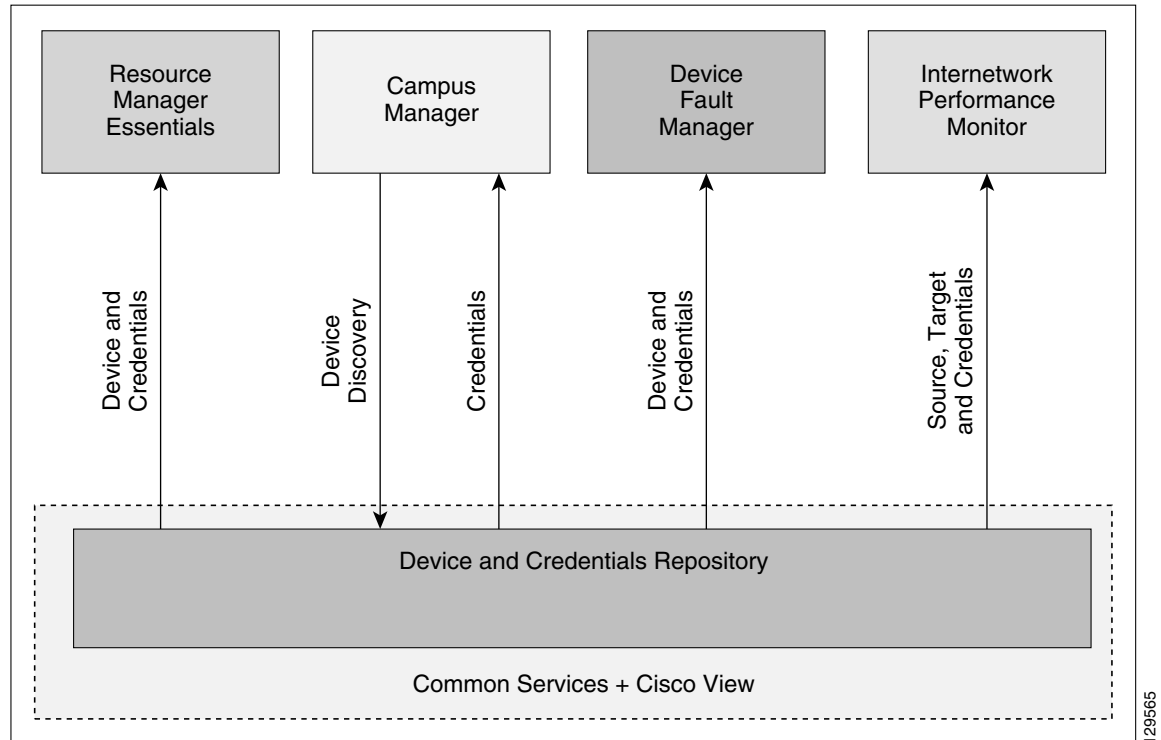
For detailed instructions on upgrading from LMS 2.x to LMS 2.5, please refer to the *LAN Management Solution 2.5 Data Migration Guidelines* document at the URL below:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/lms25/dmgl_rm.htm

LMS 2.5 Architecture

Figure 1-1 shows the architecture diagram of an LMS 2.5 server and how the applications residing on a single LMS server interact to obtain device information.

Figure 1-1 LMS 2.5 Architecture



Common Services and DCR

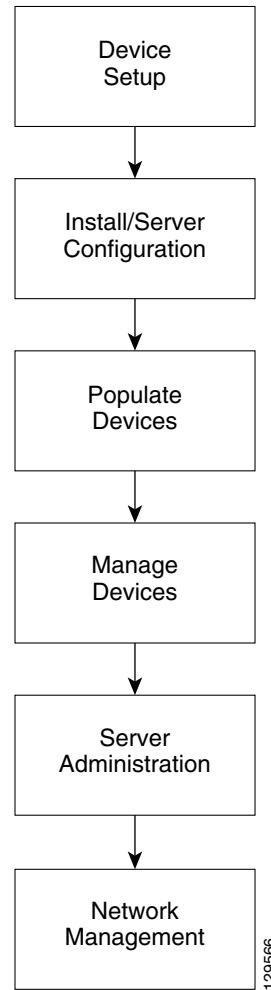
LMS 2.5 applications use Common Services as shown in Figure 1-1. Device and Credentials Repository (DCR) is part of Common Services and acts as a central secure repository for all the device and credential information. All applications within LMS request device credential information from DCR. Since there is a common Device and Credentials Repository, devices populated in DCR can be automatically populated to different applications (by enabling Auto Synchronize mode in an LMS application). For more information on this, see the [“Application Mode Settings in LMS Applications” section on page 4-1](#).

The Device and Credentials Repository also helps in a multi-server setup. This guide only briefly describes some of the basic configuration that can be achieved in a multi-server setup.

Device and LMS Workflow

Figure 1-2 summarizes the device and LMS setup workflow. Subsequent chapters describe the setup and workflow processes in detail.

Figure 1-2 *Device and LMS Setup Workflow*



129566



Setting Up Devices on the Network

LAN Management Solution (LMS) 2.5 helps to manage Cisco devices on the network. But before LMS 2.5 can function correctly, the network devices it interacts with must be set up correctly. The information provided in this chapter is a general description of the means and procedures recommended to ensure that the network devices are set up correctly.



Note

This chapter provides a great deal of information on the device configuration procedures required to manage devices using CiscoWorks LAN Management Solution. But keep in mind that this document is not intended to be a comprehensive configuration guide for LMS 2.5. For additional configuration details, please contact a Cisco certified network engineer if possible and refer to pertinent documents that are posted on *Cisco.com*.



Tip

Prior to LMS deployment, in the case of Cisco IOS and Catalyst OS devices, all configuration changes must be saved to non-volatile memory (NVRAM) using the following commands:

```
write memory OR copy running-config startup-config
```

Please note that these two commands are provided to save *pre-LMS deployment configuration changes*. After LMS is deployed, configuration changes are saved automatically where appropriate and no user intervention is required. Newer versions of Catalyst OS devices have separate running and startup configurations.

Device Setup Elements

This section describes each of the elements in the device setup that needs to be attended to.

System Name

Each Cisco IOS device in the network must have a unique system name (sysName) to discover all devices. The system name is also populated in the Cisco Discovery Protocol (CDP) table. If there are duplicate system names on the network, LMS will discover only one device by that name on the network. On Cisco IOS devices, the domain name also affects the system name.

You can set up the system name by using the following commands:

Cisco IOS Devices

```
hostname <name>
```

Cisco Catalyst OS Devices

```
set system name <name>
```

Domain Name

You can set a domain name on a Cisco IOS or a Catalyst OS device.

Set up the domain name by using the following commands:

Cisco IOS Devices

```
ip domain-name <name>
```

Cisco Catalyst OS Devices

```
set system name <name with domain name>
```

SNMP Settings

LAN Management Solution uses Simple Network Management Protocol (SNMP) community strings to read and write information from and to the devices.



Note

LMS supports SNMP *AuthNoPriv* mode of SNMP v3.

Enabling SNMP v3 on Cisco IOS Devices

To enable SNMP v3 on Cisco IOS devices, follow these steps:

-
- | | |
|---------------|---|
| Step 1 | Create a view. |
| | <pre>snmp view campus 1.3.6.1 included nonvolatile</pre> |
| Step 2 | Set the security model. |
| | <pre>snmp access cmtest security-model v3 authentication read campus write campus nonvolatile</pre> |
| Step 3 | Create a user and specify the authentication protocol to be used. |
| | <pre>snmp user cmtester authentication md5 cisco123</pre> |
| Step 4 | Create a group and associate the user with it. |
| | <pre>snmp group cmtest user cmtester security-model v3 nonvolatile</pre> |
-

Enabling SNMP v3 on Catalyst OS Devices

To enable SNMP v3 on Catalyst OS devices, follow these steps:

-
- | | |
|---------------|--|
| Step 1 | Create a view.

<pre>set snmp view campus 1.3.6.1 included nonvolatile</pre> |
| Step 2 | Set the security model.

<pre>set snmp access cmtest security-model v3 authentication read campus write campus nonvolatile</pre> |
| Step 3 | Create a user and specify the authentication protocol to be used.

<pre>set snmp user cmtester authentication md5 cisco123</pre> |
| Step 4 | Create a group and associate the user with it.

<pre>set snmp group cmtest user cmtester security-model v3 nonvolatile</pre> |
-

Enabling SNMP v1 or v2c on Cisco IOS Devices

To enable SNMP v1 or v2 on Cisco IOS devices, follow these steps:

-
- | | |
|---------------|--|
| Step 1 | <pre>snmp-server community <read-community-string> ro</pre> |
| Step 2 | <pre>snmp-server community <write-community-string> rw</pre> |
-

Enabling SNMP v1 or v2c on Cisco Catalyst OS Devices

To enable SNMP v1 or v2c on Cisco Catalyst OS devices, set as follows:

-
- | | |
|---------------|---|
| Step 1 | <pre>set snmp community read-only <read-community-string></pre> |
| Step 2 | <pre>set snmp community read-write <write-community-string></pre> |
-

The community strings configured on the devices must match the community strings entered in the DCR (Device Credential Repository) component in LMS.

Enabling Traps in Catalyst OS Devices to Be Sent to a Particular Host

To enable traps in Catalyst OS devices to be sent to a particular host, enter this command:

```
set snmp trap 192.168.124.24 public
```

Enabling Traps in IOS Devices to Be Sent to a Particular Host Using SNMP v2c

To enable traps in IOS devices to be sent to a particular host using SNMP v2c, enter this command:

```
snmp-server host 192.168.124.24 traps version 2c public
```

In these examples for enabling traps, the public community string helps selective processing of traps on the trap-receiving side.

System Reload

After a software image distribution operation using Resource Manager Essentials (RME) is completed, RME will reload the device if so specified in the Image Distribution job. RME will be able to reload any device (IOS or Catalyst OS) only if an SNMP manager (in this case, RME) is allowed to reset the agent.

The following command is needed on Cisco IOS devices only:

```
snmp-server system-shutdown
```

Command Line Prompts

To utilize the NetConfig capability to execute batch changes on devices, Cisco device command line prompts must meet the requirements described in this section.

**Note**

Customized prompts should also fulfill these requirements.

Cisco IOS Devices

- The Login prompt should end with an angle bracket (>).
For example: `Cisco>`
- The Enable prompt should end with a pound sign (#).
For example: `Cisco#`

Cisco Catalyst OS Devices

The Enable prompt must end with “(enable).”

For example: `Cisco(enable)`

Telnet/SSH

Telnet is one of the protocols that can be used by RME for configuration management. You can enable Telnet using the following commands.

To enable Telnet on Cisco IOS devices and Catalyst OS devices, enter these commands:

```
line vty 0 4
password <password>
login
exec-timeout 0 0
```

**Note**

More than four VTY lines can be selected for log in.

Different authentication on different VTY lines is not supported.

SSH provides for a secure communication with the device.

Cisco IOS

The following example configures SSH control parameters on a router running Cisco IOS:

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

Catalyst OS

The following examples configure SSH in Catalyst OS:

```
(enable) set crypto key rsa 1024
(enable) set ipNote:
```

**Note**

For greater access control and logging facilities, use TACACS.

SSH configuration requires that the domain name must be configured.

Syslog Messages

Syslog messages can be enabled on Cisco devices to further use the capability of LMS, especially RME.

Cisco IOS Devices

Enable Syslog messages on Cisco IOS devices from global configuration mode:

```
logging on
logging <server-ip-address>
logging trap <logging-level>
```

**Note**

To limit the number of messages sent to the syslog servers, use the logging trap configuration command above.

Catalyst OS Devices

To enable Syslog messages on Catalyst OS devices:

```
set logging server enable
set logging server <server-ip-address>
set logging level all <logging-level> default
```

**Tip**

The <server-ip-address> parameter is the IP address of the LMS server. In case of multiple servers, the server IP address entered here is the address of the RME server. In the case of remote Syslog Analyzer and Collector, this parameter is the IP address of the remote Syslog Analyzer and Collector.

Configuring Protocols

This section describes the basic configuration procedures for the following protocols:

- Cisco Discovery Protocol (CDP)
- Remote Copy Protocol (RCP)
- Secure Copy Protocol (SCP)
- HTTP and HTTPS Protocols
- Multiple Spanning-Tree Protocol (MST)
- Multiple Instance Spanning-Tree Protocol (MIST)
- Per-VLAN Spanning Tree Protocol (PVST+)
- VLAN Trunk Protocol (VTP)

Cisco Discovery Protocol (CDP)

Cisco Campus Manager uses Cisco Discovery Protocol (CDP) to discover Cisco devices on the network. CDP is a Cisco proprietary Layer 2 protocol that is media and protocol independent, and runs on all Cisco-manufactured equipment. A Cisco device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighbors. Since it is a Layer 2 protocol, these packets (frames) are not routed. Campus Manager will use the following protocols in their respective technology: ILMI in LANE/ATM networks and ELMI on Stratacom Frame Relay networks.

Enabling CDP on devices allows Campus Manager to learn information about neighboring devices, and to send SNMP queries to those devices. Campus Manager can discover the network topology only when CDP is enabled on those devices.

Enabling or Disabling CDP on Cisco IOS Devices

CDP is enabled on Cisco IOS devices by default. To enable CDP capability on IOS devices use the following commands.

- To enable CDP globally:
`cdp run`
- To enable CDP on specific interfaces only:
`cdp enable`
- Use the `no` command to disable CDP capability on Cisco IOS devices.

Enabling or Disabling CDP on Cisco Catalyst OS Devices

CDP is enabled on Cisco Catalyst OS devices by default. To enable CDP capability on Catalyst OS devices use the following commands.

- To enable CDP globally:
`set cdp enable`
- To enable CDP on specific ports only:
`set cdp enable [mod/port]`
- To disable CDP on Catalyst OS devices, use the `set cdp disable` command.

**Tip**

Do not run CDP on links that don't need to be discovered by Campus Manager, for example, a connection to the Internet and end-host connection ports on access switches. To protect from CDP DoS attacks, do not enable CDP on links that are connected to non-Cisco devices.

**Note**

Certain non-Cisco devices support CDP. If you enable CDP on the Cisco devices connected to non-Cisco devices, they will appear on the Campus map.

For related information, please refer to this URL:

- Configuring CDP on Catalyst 6500 Series switches:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00801a5b18.html

Remote Copy Protocol

Remote Copy Protocol (RCP) is one of the protocols that can be used by RME for configuration management and software image management. For LMS to be able to provide configuration and software management using RCP, it must be enabled on the network devices—RCP can be enabled only on devices running Cisco IOS as shown in the following sample commands:

```
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
```

**Note**

The value of `<remote-username>` and `<local-username>` entered in the device should match the `rcp user` value provided in the LMS server. The default value is `cwuser`. This value can be reset by traversing through the following user interface links in the LMS server: **CWHP > Common Services > Server > Admin > System Preferences**.

Secure Copy Protocol (SCP)

The Secure Copy feature was introduced in Cisco IOS 12.2(2)T.

To enable and configure a Cisco router for SCP server-side functionality, perform the following steps:

	Command	Description
Step 1	Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	Router# configure terminal	Enters global configuration mode.
Step 3	Router (config)# aaa new-model	Sets AAA authentication at login.
Step 4	Router (config)# aaa authentication login default group tacacs+	Enables the AAA access control system. Complete syntax: aaa authentication login {default list-name} method1 [method2...]

	Command	Description
Step 5	Router (config)# aaa authorization exec default group tacacs+	Sets parameters that restrict user access to a network. The exec keyword runs authorization to determine if the user is allowed to run an Exec shell; therefore, you must use it when you configure SCP. Syntax: aaa authorization { <i>network</i> <i>exec</i> <i>commands level</i> <i>reverse-access</i> <i>configuration</i> } { <i>default</i> <i>list-name</i> } [<i>method1</i> [<i>method2...</i>]]
Step 6	Router (config)# username superuser privilege 2 password 0 superpassword	Establishes a username-based authentication system. Note You may skip this step if a network-based authentication mechanism—such as TACACS+ or RADIUS—has already been configured. Syntax: username name [<i>privilege level</i>] { <i>password encryption-type encrypted-password</i> }
Step 7	Router (config)# ip scp server enable	Enables SCP server-side functionality.

HTTP and HTTPS Servers

The Cisco IOS HTTP server provides authentication, but not encryption, for client connections. The data that the client and server transmit to each other is not encrypted. This leaves communication between clients and servers vulnerable to interception and attack.

Enabling http Mode

Use the following command to enable http mode:

```
ip http server
```

The Secure HTTP (HTTPS) feature provides the capability to connect to the Cisco IOS HTTPS server securely. It uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.



Note

As of the LMS 2.5 release, HTTPS mode is supported only for Cisco VPN 3000 Series Concentrators.

To enable HTTPS mode in a VPN 3000 concentrator, access the following URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a008015ce28.html#999607

Configuring Multiple Spanning-Tree

Use the following procedure to configure Multiple Spanning-Tree (MST) (802.1s):

Step 1 Enable MST on the Cisco switch.

Use the `set spantree mode mst` command to set the spanning tree mode on the switch to MST.



Note Before you can disable MST, another spanning-tree protocol, such as Per-VLAN Spanning-Tree + (PVST+), must be configured.

Step 2 Define the VLAN-to-instance mappings.

Use the following command to map VLANs to an instance:

```
set spantree MST instance vlan <vlans>
```

For example, to put VLANs 1 to 10 and 20 into instance 10, you would enter this command:

```
set spantree MST 10 vlan 1-10,20
```

By default, all VLANs are mapped to instance 0.



Note Mapping a VLAN to an instance does not take effect until the configuration is committed.

Step 3 Define the MST configuration name and revision number.

Use the following commands to set the configuration and the revision number:

- `set spantree MST configuration name <name>`
- `set spantree MST configuration revision <revision-number>`

Instances 1 to 15 operate only within the MST region.

On the boundary of the MST region, MST copies the port state from the IST, which communicates with the other spanning-tree protocols, such as PVST+, Common Spanning-Tree (CST), and other MST regions to form a loop-free topology.

MST-enabled switches form an MST region only if they have a matching VLAN-to-IST mapping, MST configuration name, and MST revision number. If any of these three fails, the port will be flagged as a boundary port.

Step 4 Commit the MST configuration to apply it on the switch. Use the following command:

```
set spantree MST config commit
```

- If you find that you need to discard all edits made since the last commit, use the `set spantree MST rollback` command.
- If you need to clear changes to the MST configuration made by someone else using another session, use the `set spantree MST rollback force` command.

For related configuration information, refer to the following URL:

<http://www.cisco.com/warp/public/473/123.html>

Configuring Multiple Instance Spanning-Tree

Use the following steps to configure Multiple Instance Spanning-Tree (MISTP).

Step 1 Enable MISTP on the switch.

To set the spanning-tree mode on the switch to MST, use this command:

```
set spantree mode mistp
```

Step 2 Configure the MISTP bridge ID priority.

You can set the *bridge ID priority* for an MISTP instance when the switch is in MISTP or MISTP-PVST+ mode.

The bridge priority value is combined with the system ID extension (that is, the ID of the MISTP instance) to create the bridge ID priority.

You can set 16 possible bridge priority values:

0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

To set the bridge ID priority, use this command:

```
set spantree priority 8192 mistpinstance 1
```

Step 3 Configure the MISTP port cost.

You can configure the *port cost* of switch ports. The ports with lower port costs are more likely to be chosen to forward frames. Assign lower numbers to ports that are attached to faster media (such as full duplex) and higher numbers to ports that are attached to slower media. The default cost differs for different media.

- When using the short method for calculating port cost, the possible cost range is from 1 to 65535.
- When using the long method for calculating port cost, the possible port cost range is from 1 to 200000000.

To set the port cost, use this command:

```
set spantree portcost 2/12 22222222
```

Step 4 Configure the MISTP port priority.

You can configure the *port priority* of switch ports. The port with the lowest priority value forwards frames for all VLANs. The possible port priority values are from 0 to 63; the default is 32. If all ports have the same priority value, the port with the lowest port number forwards frames.

To set the port priority, use the following command:

```
set spantree portpri 2/12 40
```

Configuring Per-VLAN Spanning Tree+

Per VLAN Spanning Tree Plus (PVST+) maintains a spanning tree instance for each VLAN configured in the network and allows a VLAN trunk to be forwarding for some VLANs while blocking for other VLANs. Since PVST+ treats each VLAN as a separate network, it has the ability to load balance traffic (at Layer 2) by forwarding some VLANs on one trunk and other VLANs on another trunk without causing a Spanning Tree loop. It uses 802.1Q trunking technology rather than ISL. PVST+ is an enhancement to the 802.1Q specification and is not supported on non-Cisco devices.

To configure Per-VLAN Spanning Tree+, follow these steps:

Step 1 Enable PVST+ on the switch.

To set the spanning tree mode to pvst+, enter this command:

```
set spantree mode pvst+
```

Step 2 Configure the PVST+ bridge ID priority.

The bridge ID priority is the priority of a VLAN when the switch is in PVST+ mode.

When the switch is in PVST+ mode *without* MAC address reduction enabled, you can enter a bridge priority value between 0 to 65535. The VLAN bridge ID priority is then set to that value.

When the switch is in PVST+ mode with MAC address reduction enabled, you can enter one of 16 bridge priority values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, or 61440.

The bridge priority is combined with the system ID extension (that is, the ID of the VLAN) to create the bridge ID priority for the VLAN.

To set bridge ID priority, enter this command:

```
set spantree priority 30000 1
```

Step 3 Configuring PVST+ port cost

You can configure the port cost of switch ports. The ports with lower port costs are more likely to be chosen to forward frames. Assign lower numbers to ports that are attached to faster media (such as full duplex) and higher numbers to ports that are attached to slower media. The default cost differs for different media.

- When using the short method for calculating port cost, the possible port cost is from 1 to 65535.
- When using the long method for calculating port cost, the possible port cost is from 1 to 200000000.

To set the port cost, use the following command:

```
set spantree portcost 2/3 12
```

Step 4 Configure PVST+ port priority.

You can configure the port priority of switch ports in PVST+ mode. The port with the lowest priority value forwards frames for all VLANs. The possible port priority value is 0 to 63. The default is 32. If all ports have the same priority value, the port with the lowest port number forwards frames.

To set port priority, use this command:

```
set spantree portpri 2/3 16
```

For More Information on the Spanning Tree Protocol

The following links provide more information on Spanning Tree Protocol setup and recommendations.

- Configuring STP and IEEE 802.1s MST:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/spantree.htm
- Spanning Tree Protocol Problems and Related Design Considerations:
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00800951ac.shtml
- Configuring FDDI 802.10 Trunks:
http://www.cisco.com/en/US/products/hw/switches/ps679/products_configuration_guide_chapter09186a008007eeeb.html
- Financial Services Design for High Availability:
http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a008015a8ad.shtml
- Configuring Spanning-Tree Bridging for the Cisco Catalyst Switch:
http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_configuration_guide_chapter09186a00801ee706.html#71577

Default Values for PVST+ Configuration

Table 2-1 shows the default PVST+ configuration values in Cisco Catalyst 6000 devices.

Table 2-1 Default PVST+ Configuration Values for Catalyst 6000 Switches

Feature	Default Values
VLAN 1	All ports assigned to VLAN 1
Enable state	PVST+ enabled for all VLANs
MAC address reduction	Disabled
Bridge priority	32768
Bridge ID priority	32769 (bridge priority plus system ID extension of VLAN 1)
Port priority	32
Port cost	• Gigabit Ethernet: 4 • Fast Ethernet: 191 • FDDI/CDDI: 10 • Ethernet: 1002
Default spantree port cost mode	Short (802.1D)
Port VLAN priority	Same as port priority but configurable on a per-VLAN basis in PVST+
Port VLAN cost	Same as port cost but configurable on a per-VLAN basis in PVST+
Maximum aging time	20 seconds

Table 2-1 Default PVST+ Configuration Values for Catalyst 6000 Switches

Feature	Default Values
Hello time	2 seconds
Forward delay time	15 seconds

Configuring VLAN Trunk Protocol (VTP)

Virtual LAN (VLAN) Trunk Protocol (VTP) reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. VTP is a Cisco-proprietary protocol that is available on most of the Cisco Catalyst Family products.

VTP is used to configure and communicate VLAN settings across multiple switches. VTP must be configured on all switches in order to manage VLANs via Campus Manager. A VTP domain must be established and the VTP mode must be defined on each device.

In addition, at least one switch in each VTP domain must be defined as a VTP server in order for Campus Manager to create VLANs in that domain. Discovering VLANs established on a switch using VTP Transparent mode is supported from Campus Manager 3.1. (The old restriction of requiring at least one server in a VTP domain to identify VLANs has been removed.) Then Campus Manager can be used to view, create, modify, and delete VLANs via the topology services application, instead of the command line.

**Note**

This protocol should be enabled and configured as part of the overall network design. This section is included for reference purposes only.

To set a VTP domain and the mode on a Cisco Catalyst switch, use the following commands. Each switch can be in only one VTP domain:

```
set vtp domain <name>
set vtp mode <client | server | transparent>
set vtp v2 <enable | disable>
```

**Note**

The `set vtp v2` command is required for Token Ring networks. VTP v2 must be used on Token Ring networks. VTP versions 1 and 2 are not compatible, and they cannot both run in the same domain.

The description of the modes is as follows:

- **Server:** Switch will maintain and communicate VLAN settings to all other switches in the VTP domain.
- **Client:** Switch will synchronize VLAN configuration with advertisements received from VTP servers, and forward advertisements to neighbors.
- **Transparent:** Switch will not participate in VLANs advertised by server, but will forward advertisements to neighbors. Any VLANs configured on a transparent switch will be local to that switch only.

Best Practice Recommendations

The campus best practice recommendations emphasize campus stability and predictability (especially for protocols such as STP). General suggestions for enterprises preferring a cautious approach may include making use of VTP Transparent or VTP off (Catalyst OS 7.x) instead of the typical VTP server/client model.

VTP's major benefit of providing uniform VLAN creation across multiple switches may be outweighed by the drawbacks of the same thing it's supposed to simplify, which is the automatic extension of VLANs of all switches in a domain. This does pose the risk of unenforced STP and its issues cross multiple switches. Spanning tree is not a poor protocol—it's the protocol's defaults that are not ideal.

Another major risk of the VTP client/server model is the possibility of new server versioning overriding the existing VTP Server and deleting VLANs unknown to the new master server from all switches within that domain. Though some of these risks can be reduced by VTP Authentication, Trunk Clearing, and VTP Pruning, the added complexity of these is not really worth it.

Enabling Trunking on Catalyst Switch Ports

This protocol should be enabled and configured as part of the overall network design. This section is included for reference purposes only.

Trunking is a method of carrying traffic for multiple VLANs over the same link, between two switches or a switch and a router, thus extending the VLANs across the network. In order to perform trunking, ports on each side of the link must be set to trunk ports, and the Inter-Switch Link (ISL) or IEEE 802.1Q protocol must be enabled.

ISL is a Cisco proprietary protocol used to combine traffic from multiple VLANs over one link. IEEE 802.1Q is the industry-standard protocol for performing the same function.

IEEE 802.1Q must be used on Token Ring networks.

To enable trunking on a Catalyst Switch port, use the following command:

```
set trunk <module/port> on [vlans]
```

This establishes the specified module/port as a trunk port and enables the ISL protocol.

You can use the optional **vlans** parameter to specify a specific range of VLANs to be allowed across the trunk (valid ranges are from 1 to 1005).

For example:

```
set trunk 2/1 on 2-10
```

For more information, go to “Understanding and Configuring VLAN Trunk Protocol (VTP)”:

<http://www.cisco.com/warp/public/473/21.html>



Cisco LAN Management Solution 2.5 Installation Requirements

Cisco LAN Management Solution installation is supported in the U.S. English and Japanese versions of the Windows and Solaris operating systems.

Solaris OS Installation Requirements

This section discusses the LMS requirements to install on the Solaris operation system.

Table 3-1 Minimum Installation Requirements for LMS Solaris Server

Component	Minimum Requirements
Hardware	Sun UltraSPARC IIIi with 1GHz
Software	UltraSPARC IIIi: Solaris 2.8 or 2.9
Available memory	UltraSPARC IIIi: • For an Enterprise license: 2 GB RAM minimum • For a Large Enterprise license: 4 GB RAM minimum
Available disk space	• UltraSPARC IIIi (workstation and server): 80 GB • Unix file system recommended

Recommended Solaris Disk Layout

The following layout for the Solaris disk is recommended:

- /opt/CSCOpX partition
This partition holds application executables, libraries, and database files. The size grows in proportion to number of devices, amount of availability data, and the number of syslog messages.
- /var/adm/CSCOpX partition
This partition holds log files, device configurations, software images, and exported reports. The growth of the partition depends on the number of archived configurations, verbosity of debugs, and the number of software images.

- /tftpboot partition

This partition holds configurations and software image images as they are downloaded from or uploaded to devices. This partition must be large enough to handle the biggest SWIM job.

Backup Recommendations

Cisco recommends that you store backups on a separate partition, or preferably, on a separate disk. Backup partitions need to be large enough to store all application databases (for example, RME, ANI, DFM.) as well as device configurations, software images, and user accounts. The backup partition should allow for multiple revisions. Cisco also recommends that you verify all backups that may be needed in the future.

Windows OS Installation Requirements

This section discusses the LMS requirements to install on the Windows operation system.

Table 3-2 Minimum Installation Requirements for LMS Windows Server

Component	Minimum Requirements
Hardware	IBM PC Compatible computer with 2.4 GHz or Pentium III Processor
Software	One of the following: • Windows 2000 Professional with Service Pack 4 • Windows 2000 Server with Service Pack 4 • Windows 2000 Advanced Server with Service Pack 4 • Windows 2003 Standard and Enterprise Editions
Available memory	• For an Enterprise license: 2 GB RAM minimum • For a Large Enterprise license: 4 GB RAM minimum
Available disk space	• 80 GB minimum • Virtual memory: 4 GB • For a Large Enterprise license: 8 GB

Recommended Order for Installing LMS Applications

The recommended order for installing LMS applications is as follows.

1. CiscoWorks Common Services 3.0 (includes CiscoView 6.1)
2. Resource Manager Essentials 4.0
3. Campus Manager 4.0
4. Device Fault Manager 2.0
5. Internetwork Performance Monitor 2.6

**Tip**

The only requirement is to install CiscoWorks Common Services 3.0 *before* installing any other application. There is no need to follow the order recommended above if you are installing just one application in the CiscoWorks machine.

Ports Used by LMS Applications

For a complete list of ports used by LMS applications, please refer to Table 8, “LAN Management Solution Port Usage” at the following URL in the *Quick Start Guide for LAN Management Solution 2.5*:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/lms25/lms25qsg.htm#wp65566

Table 3-3 Port Usage for LMS Applications

Protocol	Port	Service Name	Applications	Direction of Connection
ICMP		Ping	RME, CM, and DFM	Server to device
TCP	22	Secure Shell (SSH)	CiscoWorks Common Services and RME	Server to device
TCP	23	Telnet	Common Services	Server to device
TCP	49	TACACS+ and ACS	Common Services, RME, CM, and DFM	Server to ACS, Device to ACS
TCP	80	HyperText Transfer Protocol (HTTP)	Common Services and CiscoView	Client to server
TCP	514	Remote Copy Protocol (rcp)	Common Services	CiscoWorks Server to device
TCP	514	rsh Daemon	RME	Server to device
TCP	1683	Internet Inter-ORB Protocol (IIOP)	Common Services and CM	Client to server
TCP	1684	IIOP	Common Services and CM	Server to client
TCP	1741	CiscoWorks HTTP Protocol	Common Services, CiscoView, and RME	Client to server
TCP	1742	SSL/HTTP Port	Common Services	Client to server
TCP	1783	IIOP for IPM Gatekeeper	IPM	Client to server
TCP	1784	IIOP for IPM Gatekeeper	IPM	Server to client
TCP	8088	HIOP	Common Services	Server to client and client to server
TCP	9002	DynamID authentication (DFM Broker)	DFM	Client to server
TCP	9088	HIOP port for IPM Gatekeeper	IPM	Server to client and client to server
TCP	42352	ESS HTTP (alternate port is 44352/tcp)	Common Services	Client to server
TCP	44342	IPM Name Server (OSAGENT)	IPM	Client to server

Table 3-3 Port Usage for LMS Applications (continued)

Protocol	Port	Service Name	Applications	Direction of Connection
UDP	69	Trivial File Transfer Protocol (TFTP)	Common Services and RME	Server to device and device to server
UDP	161	SNMP	Common Services, Cisco View, RME, CM, and DFM	Server to device
UDP	162	SNMP Traps (Standard Port)	Common Services and DFM	Device to server
UDP	514	Syslog	Common Services and RME	Device to server
UDP	9000	CSlistener (DFM server if port 162 is occupied)	DFM	Client to server
UDP	16236	UT Host acquisition	CM	Device to server

Licensing Terminology and Process

The section describes the LMS 2.5 software-based product registration and license key activation terminology and technologies.

Table 3-4 Licensing Terminology

Licensing Term	Description
Product Identification Number (PIN)	The PIN is printed on the software claims certificate. The LMS installation program prompts you to enter the PIN during installation. If an authenticated license cannot be obtained during installation, use the PIN to proceed with the installation. If a PIN only is entered, LMS will run normally, but you will be periodically be reminded to complete the license process.
Product Authorization Key (PAK)	The PAK is printed on the software claims certificate. Use the PAK to get a license from <i>Cisco.com</i> . You may obtain and install your license key at any time while you are working on LMS, not necessarily only at the time you install the product.
License File	When you register your LMS purchase on the product licensing area of <i>Cisco.com</i> , you will receive a license file. You need to provide your PAK to receive your license file. If you are a registered user of <i>Cisco.com</i> , get your license file from: • http://www.cisco.com/go/license If you are <i>not</i> a registered user of <i>Cisco.com</i> , use this site to get your license file: • http://www.cisco.com/go/license/public

Licensing Items of Note

- When you first install CiscoWorks Common Services 3.0, you will not be prompted to register your PIN/PAK during the process.

- The first LMS application you install will prompt you to provide the LMS licensing information. The LMS installation program prompts you to enter the license file, or the PIN and PAK. If the licensing information is provided during the installation of the first LMS application, then it need not be provided during the installation of the other applications.
- If you have received LMS as an evaluation copy, you need not register the product during the 90-day evaluation period.



Initial Setup of the LAN Management Solution 2.5 Server

This chapter will guide you through the initial setup of the LAN Management Solution server. This chapter also provides information on the default settings in the applications and how to update the application settings for easier management of devices across the LMS server.

Application Mode Settings in LMS Applications

Application mode settings are available in LMS applications to help control the flow of device and credential information to the applications from the Device Credential and Repository (DCR).



Note

Please note that you must specify the application mode in each of the applications user interfaces.

The two LMS application modes are:

- Manual mode
- Auto Synchronize mode

In *Manual mode*, the LMS applications (Campus Manager, Device Fault Manager, Resource Manager Essentials and Internetwork Performance Monitor) will *not* automatically get device updates (device add, delete, and credential updates) from DCR.

In *Auto Synchronize* mode, the LMS applications will automatically get device updates (device add, delete and credential updates) from DCR. In response to the device updates, the applications may do data collection, performance monitoring, and fault monitoring on the modified devices.

- Campus Manager (CM): CM by default is in Auto Synchronize mode. The application mode in CM cannot be disabled. Hence all devices added in DCR will automatically be managed in CM, unless filters (such as IP address range or VTP domain) have been set up to override the application mode.
- Device Fault Manager (DFM): By default, DFM is also set up in an Auto Synchronize mode. All devices added in DCR will automatically be managed in DFM.

To disable Auto Synchronize mode in DFM:

- a. From the Device Fault Manager, choose **Device Management > Device Selector**.
- b. Deselect the **Synchronize with Device Credential Repository** option.

- Resource Manager Essentials (RME): By default, RME is in Auto Synchronize mode. Devices imported into Device Credential Repository (DCR) will be automatically added in RME.
To disable Auto Synchronize mode in RME:
 - a. From Resource Manager Essentials, choose **Administration > Device Management**.
 - b. Then deselect the **Automatically Manage Devices from Credential Repository** option.
- Internetwork Performance Monitor (IPM): You can set up the IPM source and data collectors after DCR has been populated. For the procedure, refer to the [“Importing Devices Into Internetwork Performance Monitor”](#) section on page 6-13.

**Tip**

For easier management of devices across all LMS applications, it is advisable to leave Auto Synchronize mode enabled.

When multiple CiscoWorks servers are installed and a large number of devices are to be managed between the CiscoWorks servers, Manual mode should be enabled.

If Auto Synchronize mode is enabled for RME to get devices from the DCR, two instances of RME installed in two different servers can be managing the same set of devices. User intervention is required to select dissimilar set of devices to be managed by the two RME servers.

Protocol Setup

RME also uses various protocols for configuration and software management. Network administrators can assign the protocols to be used in RME for Configuration Management and Software Management.

Configuration Management

You can set the protocols and order for Configuration Management applications such as Archive Management, Config Editor, and NetConfig jobs to download configurations and to fetch configurations. The available protocols are:

- Telnet
- TFTP (Trivial File Transport Protocol)
- RCP (Remote Copy Protocol)
- SSH (Secure Shell)
- SCP (Secure Copy Protocol)
- HTTPS (Hyper Text Transfer Protocol Secured)

Set Up Protocol Ordering

Protocol ordering can be set up for these configuration applications: Archive Management, Config Editor, and NetConfig. To set up protocol ordering for Config Management:

-
- Step 1** From Resource Manager Essentials, choose **Administration > Config Management**.
 - Step 2** Select the desired application from the **Application Name** drop-down list.
 - Step 3** Select the protocol order by clicking **Add** or **Remove**, then click **Apply**.
-

**Tip**

For secure communication between the server and a device, use SSH.

To order the Software Management protocol:

-
- Step 1** Click **Software Mgmt**.
 - Step 2** Select **View/Edit Preferences** from the Table of Contents.
 - Step 3** Use the **Add** and **Remove** buttons for selecting the protocol order.
-

Software Image Management

Software Management downloads software images based on the protocol order specified. While downloading the images, Software Management uses the first protocol in the list. If the first protocol in the list fails, these jobs use the second protocol and so on, until Software Management finds a transport protocol for downloading the images.

The supported protocols are: RCP, TFTP, SCP and HTTP.

To define the protocol order that Software Management has to use for software image download:

-
- Step 1** From Resource Manager Essentials, choose **Administration > Software Mgmt > View/Edit Preferences**.
 - Step 2** In the View/Edit Preferences dialog box, define the protocol order.
 - Step 3** Use the **Add** and **Remove** buttons for selecting the protocol order.
-

Setting Up Security

By integrating with the Cisco Secure ACS server, LMS 2.5 provides the following security features:

- Secure the user access to devices.
- Secure browser client communication to the server.

Certificate Setup

Every CiscoWorks server needs to have a System Identity user set up for system processes to use while performing background tasks that are not user initiated. A system identity user is set up by default when the CiscoWorks server is installed.

Setting Up the System Identity User

To view the System Identity User default settings or to change the default settings:

-
- | | |
|---------------|---|
| Step 1 | Navigate to CWHP > Common Services > Server > Security > Multi-Server Trust Management . |
| Step 2 | Select the System Identity Setup link. |
| Step 3 | Edit the necessary details. |
-

Setting Up a Peer Server Account

If a CiscoWorks server has to exchange information (such as device credentials) with other CiscoWorks servers, every CiscoWorks server needs to have a peer server account set up. A peer server account should have the System Identity user information of other CiscoWorks servers.

Peer server accounts can also be used for providing access to a third-party application to access the CiscoWorks server and authenticate and authorize it. Create a peer server account as described here and provide the credential information to the third-party user.

To set up a peer server account:

-
- | | |
|---------------|---|
| Step 1 | Create the System Identity user as described in the previous section. |
| Step 2 | Navigate to CWHP > Common Services > Server > Security > Multi-Server Trust Management . |
| Step 3 | Select the Peer Server Account Setup link. |
| Step 4 | Make sure that the System Identity users of the other CiscoWorks servers are created. |
-

Enabling HTTPS on an LMS Server

You can enable HTTPS on an LMS server to provide secure communication between the server and client.

-
- | | |
|---------------|---|
| Step 1 | SSL can be enabled on the server by going to Common Services > Server > Security > Single-Server Management . |
| Step 2 | Select Browser-Server Security Mode Setup . |
| Step 3 | Select Enable . |
-

Notes

- HTTPS communication will work only after restarting the LMS server.
- Any link and/or application registration will work fine after you change the *CiscoWorks security mode* from **http** to **https**.
- To restart the LMS server.
 - If using a Windows server, enter either the **net stop crmdmgtd** command or the **net start crmdmgtd** command.
 - If using a Solaris server, enter the **/etc/init.d/dmgtd stop** command or the **/etc/init.d/dmgtd start** command.
- To access the LMS server, use *https://server-url:1742*.

Single Sign-On

Single Sign-on is the ability to log in into multiple servers with a single action and the entry of a single password. This is especially useful where, for example, a user on a LAN or WAN requires access to a number of different servers.

In SSO mode, one of the CiscoWorks servers acts as the SSO Authentication server or master and all other CiscoWorks servers act as the slave or SSO regular server. All authentication is done by the master server for any access to slave or master servers.

This task is optional and applicable in a multiple CiscoWorks server setup only.

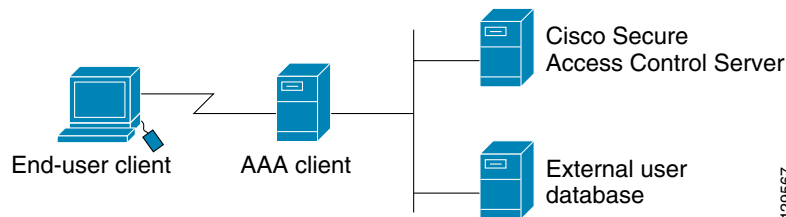
To setup Single Sign-on, follow these steps:

-
- | | |
|---------------|--|
| Step 1 | Complete the “Certificate Setup” section on page 4-4. |
| Step 2 | One of the CiscoWorks servers should be set up as the authentication server. Navigate to CWHP > Common Services > Server > Security > Multi Server Trust Management . |
| Step 3 | Select the Single Sign-on Setup link. |
| Step 4 | Choose the Master (SSO Authentication Server) mode. |
- The same link can be used to set up other CiscoWorks servers as slaves.
-

Setting Up the Cisco Secure Access Control Server

Cisco Secure Access Control Server provides authentication, authorization, and accounting (AAA) services to network devices that function as AAA clients, such as a network access server, PIX Firewall, or router. [Figure 4-1](#) shows the AAA client model.

Figure 4-1 AAA Client Model



LAN Management Solution integrates with the ACS server to leverage the AAA functionality for restricting user access to devices. Common Services provides a way to configure secondary and tertiary ACS servers to support redundancy.

Integrating LMS Servers with ACS

To integrate LMS servers with ACS, follow these steps:

Set Up the System Identity and Peer Server Account Users in the LMS Server

To ensure that the System Identity User is set up:

-
- Step 1** Navigate to **CWHP > Common Services > Server > Security > Multi-Server Trust Management**.
 - Step 2** Select the **System Identity Setup** link.
 - Step 3** If there are third-party applications integrating with the LMS server, create a peer server account for this purpose because the third-party applications do not need to know the System Identity Setup credentials.
-

Set Up the ACS Server

To set up the Access Control Server, follow these steps:

-
- Step 1** Log in to the ACS Server.
 - Step 2** To add the CiscoWorks LMS server(s) as AAA client(s) of the ACS server, from the Network Configuration menu, choose **Add Entry**.
 - Step 3** Provide the IP address and host name of the CiscoWorks LMS server(s) that you are going to set up.
 - Step 4** Specify a secret Key.
 - Step 5** For the Authentication method, choose **TACACS+**.
 - Step 6** Assign the CiscoWorks LMS server(s) to a new NDG group.

Step 7 To create a new NDG group, from the Network Configuration menu, choose **Add Entry**.

Step 8 Add a System Identity User as a registered user in the ACS Server.

- a. To do this, navigate to **User Setup**.
- b. Enter the username, then click **Add/Edit**.
- c. In the User Setup section, enter the password for the user.



Note Make sure the user is created with the same password as the password specified for the LMS servers.

Step 9 Add the group to **Default Group**, then click **Submit** (located on the lower frame).



Note The same procedure must be done to add any other peer server username (especially the user created for third-party applications) to the ACS server.

Set Up the LMS Server to Communicate with the ACS Server

To set up the LMS server to communicate with the ACS server, follow these steps:

Step 1 Log in to LMS server.

Step 2 Navigate to Common Services Panel in CiscoWorks Home Page.

Step 3 To configure Common Services to be in ACS login mode, choose **Server > Security > AAA Mode Setup > Select ACS Type**.

Step 4 Enter the primary ACS server IP address, ACS Admin User Name and Password, and Shared Secret Key



Note These values for these fields must be the same as the values entered in the ACS server.

Step 5 Restart the LMS server.

- If using a Windows server, enter either the **net stop crmdmgtd** command or the **net start crmdmgtd** command.
- If using a Solaris server, enter the **/etc/init.d/dmgtd stop** command or the **/etc/init.d/dmgtd start** command.

Configure the System Identity User in the ACS Server

In this procedure, you will learn how to assign a *System Administrator* privilege to the User Group on the Device Group to which the LMS server is assigned.



Note The System Identity User is quite unique and not the same as any other user created in the ACS server. The only difference between this setup and the peer server user setup is that the peer server username need not be assigned an Administrator privilege to the NDG group.

To configure the System Identity User in the ACS server, follow these steps:

-
- Step 1** Navigate to **Group Setup**.
 - Step 2** Select the **User Group**.
 - Step 3** Click **Edit Settings**.
 - Step 4** Browse to the applications CiscoWorks, CiscoView, Resource Manager Essentials, Device Fault Manager and CiscoWorks Campus Manager, and provide *System Administrator* privilege for the device group containing the LMS server.
-

Configure the ACS Server to Change Default Permissions and Task to Role Mapping (Optional)

There are five default roles defined by CiscoWorks:

- System Administrator
- Network Administrator
- Network Operator
- Approver
- Help Desk

These roles are by default assigned permissions to various tasks in CiscoWorks. An ACS user can change the task to role mapping as required.

-
- Step 1** Log in to the ACS server.
 - Step 2** To change the task to role mapping, click **Shared Profile Components** (in the navigation bar on the left).
 - Step 3** Choose the application for which you need to set the task to role mapping.
For example, you can click **CiscoWorks Common Services**, click on a user role and change the tasks assigned to that role.
-

Create Network Device Groups, User Groups and Assign Roles to Network Device Groups in the ACS Server

To create Network Device Groups, user groups, and assign roles to those groups, follow these steps:

-
- Step 1** Log in to the ACS server.
 - Step 2** To create Network Device Groups, click **Network Configuration** (in the left navigation bar).
 - Step 3** Add devices to the Network Device Group.
 - Step 4** To add users to User Groups, click **Group Setup**, then click **Users in Group**.
 - Step 5** To assign User Groups permissions (System Administrator, Network Administrator, etc.) on the various Network Device Groups, click **Group Setup**, then click **Edit Settings**.
-

Setting Permissions for Performing Tasks on Devices

If a Security Administrator wants to restrict a user to performing only a selected set of tasks (for example tasks t1, t2, and t3) on a device in the LMS server, then follow these steps.

-
- Step 1** Put the LMS server(s) in ACS security mode
 - Step 2** Set up the Cisco Secure ACS server as described in [“Setting Up the Cisco Secure Access Control Server” section on page 4-6](#).
 - Step 3** Log in to the ACS server.
 - Step 4** Make sure that a role (for example Network Administrator) is available so that it has permissions to perform only the restricted list of tasks.
 - Step 5** Click **Shared Profile Components**, then select an application that has tasks t1, t2 and t3.
 - Step 6** Click **Network Administrator** and enable only the tasks t1, t2, and t3 for this role.
 - Step 7** Click **Group Setup**, then select the user group to which the user is assigned.
 - Step 8** Click **Edit Settings**, go to the application where the tasks t1, t2 and t3 are present, and assign the role **Network Administrator** to the user selected in the previous step.
-



Populating Devices in Cisco LAN Management Solution 2.5

The tasks described in [Chapter 4, “Initial Setup of the LAN Management Solution 2.5 Server”](#) should complete the initial configuration on the LMS server. LMS is now ready to start importing devices for management.

Devices can be populated in the LMS server through one of the three tasks listed below:

- [Campus Manager Device Discovery, page 5-1](#)
- [Bulk Device Import to Device and Credentials Repository, page 5-2](#)
- [Device Credentials Update, page 5-3](#)

Campus Manager Device Discovery

Campus Manager has the ability to discover Cisco devices present in the network using Cisco Discovery Protocol (CDP). Hence to have the ability to discover devices using Campus Manager, CDP should be enabled on the network. If CDP is enabled on your network, you can enter a single or multiple *Seed Devices* in Campus Manager.



Note

A *seed device* should generally be core device. A core switch (or switches) should be the seed device because this device will have a lot of CDP neighbors and this hastens the discovery process.

In LMS 2.5, Campus Manager processing has been partitioned into two separate processes: one of the processes is called *Device Discovery*, while the other is called *Campus Data Collection*.

Device Discovery within Campus Manager uses seed devices to discover the network using CDP. In the device discovery process, Campus Manager populates the Device and Credentials Repository (DCR) with the list of discovered devices in the network. Information about the devices is fetched by Campus Manager only during the data collection process.

To gather the list of devices, you must first initiate the Device Discovery process.

Defining a Seed Device in Campus Manager

To define a seed device in Campus Manager, follow these steps:

Step 1 Choose **Administration**.

Step 2 Then select the **SNMP Settings** link.



Note Only the read community string needs to be entered in the SNMP Settings page. **Add** or **Edit** the read community strings depending on the number of community strings configured in the network. By default only the *SNMPv2* read string is populated.

Step 3 To populate SNMPv3, select the **SNMPV3** radio button.

Step 4 After editing the SNMP strings, click **Apply** on the SNMP Settings screen.

Step 5 To enter a seed device, click the **Discovery Settings** link (under TOC).

Step 6 Configure the seed devices, then click **Apply**.

This action triggers an immediate Device Discovery process.

Address filters are available to either to discover or not discover devices in a particular network.

Step 7 To configure the address filters, click **IP Address Range**.



Note If the device discovery is scheduled, devices in LMS would be populated only after Campus Manager Device Discovery has taken place.

Step 8 To verify the device discovery status, click the **Go to Campus Administration** link.

Step 9 Refresh the page to update the device discovery status and verify the number of devices discovered when in *Idle* state.

All the devices discovered by Campus Manager should now be populated in the DCR.

Bulk Device Import to Device and Credentials Repository

LMS also supports bulk import into the Device and Credentials Repository.

To do bulk device import, navigate through **CWHP > Common Services > Device Management > Bulk Import**.

Bulk import into DCR can be done by one of the three formats listed below.

- **File Import**

Select the **File** option to import devices from a CSV or XML file.

The input file should have the format as specified in the online help. In this case, all device credentials can be provided along with the device name and IP address.

If the imported device does not have a device type associated with it, then it will be a member of the group */CS@server-name/ System Defined Groups/Unknown Device Type*.

You can then assign a device type to the device by selecting the device in Device Management screen and clicking **Edit**.

- **Local NMS**

To import devices from either HP OpenView Network Node Manager 6.x or IBM Tivoli NetView 7.x installed in the same machine as the CiscoWorks server, select the **Local NMS** option. You will have to provide the installation location of HP OpenView NNM 6.x or IBM Tivoli NetView 7.x.

- **Remote NMS**

To import devices from either HP OpenView Network Node Manager 6.x or IBM Tivoli NetView 7.x installed in a different machine from the CiscoWorks server, select the **Remote NMS** option.



Note

In LMS 2.5, the importing devices is allowed only from a remote Unix NMS server or a remote Windows NMS server that supports the RSH protocol.

Editing the Credentials for the Imported Devices

Once the devices have been imported through the **Local NMS** or **Remote NMS** options, you can edit the credentials for these devices by selecting the groups to which the devices belong, then in the Device Management screen, click **Edit**.



Tip

If you have CDP enabled on your network, populating the Cisco devices through Campus Manager Device Discovery is recommended.

Device Credentials Update

To utilize the complete functionality of LMS, device credentials other than the SNMP read credentials need to be entered in the Device and Credentials Repository.

To perform credential update in DCR:

- Step 1** Navigate to **CWHP > Common Services > Device and Credentials > Device Management**.
- Step 2** Select all the devices under the CS group by checking the **CS@server-name** group, then click **Edit**.



Tip

Don't select any device in the screen that follows.

- Step 3** Click **Next**, which will by default select all the devices.
- Step 4** Enter the device credentials, then click **Finish**.
- Step 5** If you need to enter *User Fields* for devices, click **Next** and enter up to four user-defined fields.
If all the devices have the same credentials, use the above step to Edit their credentials. You can add additional user-defined fields.
- Step 6** However, if the devices have different credentials, create groups of devices having the same credentials by going to **CWHP > Common Services > Groups**.
- Step 7** Create groups underneath the *CS@server-name/User Defined Groups* group.

Device Management

Device discovery just populates devices in LMS. Additional information about the devices such as configuration files and software images on the network needs to be added. All applications within LMS should be populated with the imported devices.

Adding Devices to RME From DCR

If RME has not been set up in Auto Synchronize mode, devices can be added into RME from the Device and Credentials Repository using either of following procedures:

- If all the devices added in DCR are also to be managed by RME, the Auto Synchronize option in RME should be enabled.

You can enable Auto Synchronization by:

- a. Going to the CiscoWorks Home Page and navigating to **RME > Administration > Device Management > Device Management Settings**.
 - b. Check **Automatically Manage Devices from Credential Repository**.
- If only a subset of devices available in DCR are to be managed in RME, the Auto Synchronize option can be left turned off.

If the devices have been populated through Campus Manager Device Discovery or a third party NMS and if the Auto Synchronize option on RME was enabled, the initial configuration collection of devices would fail since the credentials (SNMP write, Telnet/SSH) needed for configuration collection were not available in LMS.

Viewing Configuration Collection Status in RME

You can view configuration collection status in RME by:

1. Going to **CWHP > Resource Manager Essentials > Config Management > Archive Management**.
2. To see the list of devices that failed the archive operation, click the **Number of Failed Devices** link.

Since the credentials have been updated in LMS, you would need to run the synchronize operation to collect the configuration files for the managed devices.

Collecting Devices' Startup and Running Config

To collect the startup and running configuration of devices:

-
- | | |
|---------------|--|
| Step 1 | Go to TOC > Sync Archive . |
| Step 2 | You must schedule a Sync Archive job. To do so, select the devices under RME@server-name group. |
| Step 3 | Check Fetch Startup Config . |

This can be done only for the devices that failed the initial synchronize archive operation.

Taking these steps should populate the managed devices in the server. To ensure that the applications are working properly, step through the verification process described in the following section.

Verification of Device Import Status in LMS Applications

This section describes the verification of device import procedures in Resource Manager Essentials, Campus Manager, and Device Fault Manager.

Resource Manager Essentials

The following RME device verification tasks are described in this section:

Confirm Configuration File Collection

To confirm if the configuration files have been collected:

1. To verify job status, go to **Config Management**, then select the **Archive Management** link.
 2. To view the archive collection status or view the job details, refresh the screen.
-

Check Device Credentials

To check the device credentials:

1. Check device credentials by going to **Resource Manager Essentials > Devices > Device Management > Device Credential Verification**.
 2. To verify the type of device credentials to be checked, click **Check Device Credential**.
 3. To view the report and see if the device credentials are correct, click **View Credential Verification Report**.
 4. If you need to change the credentials on devices, click **Edit Device Credentials**.
-

Campus Manager

To get the current status of devices in Campus Manager:

Navigate to **CWHP > Campus Manager > Administration**.

- You can find the discovery status of devices under *Device Discovery*.
- You can view the data collection status of a device under *Data Collection*.

Device Fault Manager

To get the current status of devices in DFM:

Navigate to **CWHP > Device Fault Manager > Device Management > Discovery Status**.

- Devices should be in status *Known*.
- DFM Processing should be *Active*.



Server Administration in Cisco LAN Management Solution 2.5

This chapter deals with server administration and configuration settings to optimally utilize the resources of the server while also maintaining a current status of the network topology.

Common Services

Common Services provides an operating foundation that allows CiscoWorks applications to share data and system resources. It also provides a common desktop for launching CiscoWorks applications and centralizes login, user role definitions, and access privileges. Periodic updates to CiscoWorks Common Services 3.0 are made available for download.

For installation and user guide documentation, please refer to the following documents:

- *Installation and Setup Guide for CiscoWorks Common Services 3.0* (includes CiscoView) on Solaris:
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_installation_guide_book09186a00801e8b87.html
- *Installation and Setup Guide for CiscoWorks Common Services 3.0* (includes CiscoView) on Windows:
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_installation_guide_book09186a00801e8b8a.html
- *User Guide for CiscoWorks Common Services 3.0*
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_book09186a00801e8b82.html

Creating User Defined Groups

Grouping devices in Common Services is used to create user-defined groups based on the *User Defined* field defined by DCR for the devices. These groups can then be used by Resource Manager Essentials, Campus Manager, Device Fault Manager, or Internetwork Performance Monitor to launch tools pertinent to that application. (Similarly, each application in LMS 2.5 provides the ability to create user-defined groups.)

To create user defined groups, follow these steps:

-
- Step 1** Navigate to **CWHP > Common Services > Groups**.
 - Step 2** Select the **Group Admin** link.
 - Step 3** In the Group Administration window, select **/CS@server-name/User Defined Groups** from the group selector, then click **Create**.
 - Step 4** Enter a group name and click **Next**.
 - Step 5** Select the **Variable** drop-down box.
The *Variable* field offers four possible values: *user_defined_field_0*, *user_defined_field_1*, *user_defined_field_2*, and *user_defined_field_3*.
 - Step 6** Select an operator and value that matches the device value in DCR, then click **Add Rule Expression** and click **Next**.
All the devices that match the criteria are shown in the right panel.
 - Step 7** Click **Next**.
 - Step 8** To create the new group under */CS@server-name/User Defined Groups*, click **Finish**.
This newly created group can be accessed from any application screen in LMS.
-

Backing Up LMS Data

Cisco recommends that the backup data should *not* be stored in the directory where LMS is installed (by default, under the NMSROOT directory in Windows or Solaris). Please note that the DCR Master/Slave mode is also backed up.

To backup LMS data:

-
- Step 1** Navigate to **CWHP > Common Services > Admin**.
 - Step 2** Select the **Backup** link.
 - Step 3** You can provide a backup directory name.
The backup job can either be run immediately or be scheduled.
-

Restoring LMS Data

Restoring LMS data can be done only via the command line interface. For a complete description of the procedures for backing up and restoring LMS data, refer to the *LAN Management Solution Data Migration Guidelines* document at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/lms25/dmgl_rm.htm

-
- | | |
|---------------|---|
| Step 1 | Log in to the LMS server. |
| Step 2 | Shutdown the daemon manager: <ul style="list-style-type: none">• For a Windows server: Execute the net stop crmdmgtd command.• For a Solaris server: Execute the /etc/init.d/dmgtd stop command. |
| Step 3 | Change directory to <i>NMSROOT/bin</i> . |
| Step 4 | Execute the script restorebackup.pl . |
-

Campus Manager

In Campus Manager 4.0, the discovery mechanism can be categorized into the following three areas:

- Device Discovery
- Data Collection
- User Tracking Major Acquisition

Campus Manager Device Discovery

Device Discovery can be run on a predetermined schedule or initiated by an operator.

**Note**

Discovering a device is not equivalent to managing the device in Campus Manager.

The following are some key facts about Device Discovery:

- Device Discovery performs Network Discovery using the Cisco Discovery Protocol as the discovery mechanism.
- Device Discovery determines the management IP address of the device.
- Devices in DCR and user-configured seed devices from Campus Manager are used by the device discovery process. It populates the Device and Credentials Repository with the following discovered information:
 - Host name
 - Domain name
 - Management IP address
 - Display name

- sysObjectID
- SNMP credentials

Optimizing Network Discovery

To optimize the discovery of the network, the following tasks can be performed.

Setting Up IP Filters

You can set IP filters if only certain subnets need to be discovered. IP address filters help to define the IP address ranges inside of the devices that need to be discovered. These IP address ranges typically fall inside the same subnet.

To set up IP filters:

1. Navigate to **Campus Manager Administration > Admin > Device Discovery > Discovery Settings**.
 2. Under *IP Address Range*, click **Configure**.
-

Disabling DNS Lookup

DNS lookup could be one potential area for device discovery to slow down, so DNS lookup can be disabled.

To disable DNS lookup:

1. Navigate to **Campus Manager Administration > Admin > Device Discovery > Discovery Settings**.
 2. Uncheck the **DNS Lookup** checkbox.
-

Troubleshooting Device Discovery

To troubleshoot device discovery:

1. Navigate to the Campus Manager Panel from **CWHP > Campus Manager Administration > Reports > Discovery Reports**.
 2. Check to see if the SNMP settings are correct for the devices to be discovered correctly.
 3. If the log file shows any SNMP timeout exceptions, you can increase **SNMP Timeout** and **Retry** values.
-

Campus Manager Data Collection

You can run Data Collection on a predetermined schedule or through operator action.

The following are some key facts about Campus Manager Data Collection:

A list of devices and corresponding credentials in Device and Credentials Repository are used for data collection.

Only devices in DCR are managed. If a device is not in DCR, it cannot be managed by Campus Manager. You can apply a filtering mechanism to manage a subset of devices found in the Device and Credentials Repository. The filtering is based on either IP addresses or the VTP domain.

Optimizing Data Collection

To optimize the data collection for devices in the network, complete the following tasks:

Setting IP Address or VTP Domain Filters

You can set IP address or VTP domain filters:

Navigate to **Campus Manager Administration > Admin > Campus Data Collection > Data Collection Filters**.

Optimizing According to the Number of Devices

- When data collection is done for more than 5,000 devices, the ANIServer process (Java based) reaches a threshold of 1,024 MB.
- If data collection is done for a device count close to 5,000, Cisco recommends you increase the heap size for the ANIServer from `-Xmx1024m` to `-Xmx1280m`.

Modifying the heap size. To modify the heap size in the ANIServer, edit the file `NMSROOT/objects/dmgt/dmgt.d.conf` file.

In this file, there is an entry for starting the ANIServer process. This entry has a string `-Xmx1024m`. Change this string to `-Xmx1280m`.



Note

Any edits to `dmgt.d.conf` file can be done only after the LMS server is shutdown. You must restart the LMS server the edit to the `dmgt.d.conf` file is complete.

User Tracking Module

In addition to the Campus Manager data collection feature, the User Tracking module in Campus Manager can acquire data on end hosts, IP phones, and subnets. There are two major types of acquisition in User Tracking:

- *Major Acquisition:* Collects data on end hosts, Cisco IP phones, and subnets in the network.
- *Minor Acquisition:* Polls the end hosts and IP phones to keep the User Tracking data current.

Initiating a UT Major Discovery

1. Navigate to **CWHP > Campus Manager > User Tracking > Admin > Acquisition**.
2. Initiate a **UT Major Discovery**.

The following is the list of some important options that can be selected for a major acquisition:

- *Enable User Tracking for DHCP environment:* This is an option for tracking the end hosts in case the IP address changes.
- *Use DNS to resolve host names:* This is an option for resolving the host names.
- *IP phone acquisition on dot1q trunks for IOS switches:* This is an option for fetching end hosts that are connected to a switch in Voice VLAN Setup.

Setting a Schedule for a Major Acquisition

To set a schedule for running a major acquisition:

1. Navigate to **Campus Manager > User Tracking > Admin > Acquisition**.
2. Then select the **Schedule Acquisition** link.

Ping Sweep on IP Addresses in a Subnet

You can enable a ping sweep on all IP addresses in a subnet before starting a major acquisition. There is an option to exclude certain subnets from the ping sweep.

Purge Policies

You can delete end hosts and IP phones from User Tracking either on demand or on a specified interval after major acquisition:

Navigate to **CWHP > Campus Manager > User Tracking > Admin > Acquisition > Delete Interval**.

Archives or jobs older than a particular date can also be purged:

Navigate to **CWHP > Campus Manager > User Tracking > Admin > Reports > User Tracking Purge Policy**.

Hierarchical Groups in Campus Manager

Hierarchical groups help users to visualize the topology implemented for user-defined groups. Hierarchical groups are created on top of Topology groups.

-
- Step 1** Navigate to **CWHP > Campus Manager**.
 - Step 2** Select the **Topology Services** link.
 - Step 3** In the window that opens up, select **Topology Groups**, then right-click **/Campus@server-name/System Defined Groups**.
 - Step 4** Select the **Display View** option.

The three immediate subgroups are shown as maps. You can click on the maps and choose to show aggregate links between two maps. This view shows the aggregate links between all devices contained inside those two maps.

Resource Manager Essentials

This section describes the LMS server administration tasks for Resource Manager Essentials.

Inventory Collection and Polling

When RME is installed, system jobs are created for both inventory collection and polling, with their own default schedules. A periodic inventory collection job collects inventory data from all devices in the All Devices group and updates the inventory database. The periodic polling polls all devices to check for changes in inventory and collects and updates the inventory database only if there is a change.

The default periodicity of the inventory collector job is once a week and the default periodicity of the poller job is once a day.



Tip

The poller detects most changes in all devices with much less impact on your network and on the LMS server.

Changing the Job Schedule Default Settings

To change the default settings:

-
- Step 1** Navigate to **Resource Manager Essentials > Administration > Inventory > System Job Schedule**.
The System Job Schedule dialog box displays the current collection or polling schedule.
- Step 2** Change the values as needed and click **Apply**.
-

Configuration File Collection and Polling

The configuration archive can be updated with configuration changes by periodic configuration archival (with and without configuration polling).

To enable periodic configuration archival:

Choose **Resource Manager Essentials > Administration > Config Mgmt > Archive Mgmt > Collection Settings**.



Note

A scheduled collection and polling are disabled by default since the customer's network may have sporadic bursts of traffic and network management operations should not take up the existing bandwidth. It is best for the customer to select the periodic collection and polling.

Specifying When and How Config Collection and Polling Occurs

You can modify how and when the configuration archive retrieves configuration files by selecting one or both of the following options:

- **Periodic Polling**

Configuration archive performs a SNMP query on the device, if there are no configuration changes detected in the devices, no configuration is fetched.

- **Periodic Collection**

Configuration is fetched without checking for any changes in the configuration.

To specify Periodic polling, Periodic collection, or both:

1. Choose **Resource Manager Essentials > Administration > Config Mgmt > Archive Mgmt > Collection Settings**.
2. Select one or both of these options.

Default Protocols Used for Configuration Fetch and Deploy

Many protocols are used for performing a configuration fetch and deploy operation. The system provides a default order of protocols that will be used to fetch or deploy the configuration files on the device. The order of protocols that are used can be rearranged, or some protocols can be removed from the list if it is not relevant to your network.

To access the default order of protocols used and change the order:

-
- | | |
|---------------|--|
| Step 1 | Navigate to Resource Manager Essentials > Administration . |
| Step 2 | Select the Config Mgmt link. |
-

RME Purge Policies

This section describes the RME purge policies for configuration management, Syslog messages, and Change Audit data.

Specifying When to Purge Configuration Files

You can specify when to purge archived configurations. This frees disk space and keeps your archive at a manageable size. (By default, the purging jobs are disabled.) You can purge configuration files based on two criteria:

- Age. Configurations older than the number of days you specify are purged.
- Maximum number of versions of each configuration to keep.

The oldest configuration file is purged when the maximum number is reached. For example, if you set the maximum versions to keep to 10, when the eleventh version of a configuration is archived, the first is purged to keep the total number of archived versions at 10.

Step 1 Choose **Resource Manager Essentials > Administration > Config Mgmt > Archive Mgmt > Purge Settings**.

The Archive Purge Setup dialog box appears.

Step 2 Select **Enable**.

Step 3 To schedule a purge job, click **Change**.

Step 4 To specify when to purge configuration files from the archive, select one or both of the following options:

- **Maximum Versions:** Enter the number of configuration files to retain.
- **Purge Versions Older Than:** Enter a number and select days, weeks, or months.
- **Purge Labeled Files:** To delete the labeled configuration files.

The labeled files will be deleted only if values have been entered for both *Maximum versions to retain* and *Purge versions older than*.



Tip

Cisco recommends that you specify values for both purge options: a number of maximum versions permitted and the maximum age permitted (in days, weeks, or months) for configuration files.

Step 5 Click **Apply**.

Periodic Purging of Syslog Messages

A default policy can be specified for the periodic purging of Syslog messages.

To specify the default purge policy for Syslog messages:

Step 1 Select **Resource Manager Essentials > Administration > Syslog > Set Purge Policy**.

Step 2 Specify the number of days in the *Purge records older than* field.

Only the records older than the number of days that you specify here will be purged. The default value is 7 days.

Purging Change Audit Data

A periodic purge or a forced purge of Change Audit data can be scheduled. This frees disk space and maintains the Change Audit data at a manageable size.

Step 1 Select **Resource Manager Essentials > Administration > ChangeAudit > Set Purge Policy**.

Step 2 Enter the values for each field.

Step 3 To save the purge policy that you have specified, click **Save**.

Defining Syslog Message Filters

You can exclude messages from Syslog Analyzer by creating filters. To do so:

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Message Filters**.

A list of all message filters is displayed in a dialog box, along with the names, and the status of each filter—**Enabled** or **Disabled**.

Step 2 Specify whether the filters are for dropping the Syslog messages or for keeping them by selecting either **Drop** or **Keep**.



Note

The **Drop or Keep** option applies to all message filters and is not on a per-filter basis.

- If you select the **Drop** option, the Common Syslog Collector drops the syslogs that match any of the Drop filters from further processing.
- If you select the **Keep** option, Syslog Collector allows only the syslogs that match any of the Keep filters, for further processing.

Change Audit

This section discusses two aspects of RME's Change Audit feature—setting up inventory filters and defining exception periods.

Setting Up Inventory Filters

Certain inventory attributes can change often and these changes can get logged whenever there is a collection. This may cause a lot of change audit messages to accumulate fairly quickly. To prevent this, you can enable inventory change filters to *not* track change audits for these attributes.

To set up inventory filters:

Navigate to **Resource Manager Essentials > Administration > Inventory > Inventory Change Filter**.

Defining Exception Periods

An *Exception Period* is a time you specify when no network changes should occur.

To set an Exception Period:

Step 1 Navigate to **Resource Manager Essentials > Tools > Change Audit > Exception Period Definition**.

Step 2 From the Day drop-down list, select **Days of the week**.

Step 3 From the Start Time and the End Time drop-down lists, specify the start time and the end time.

Step 4 Click **Add**.

SWIM Baseline Collection

The RME Software Image Manager (SWIM) tool is very useful for software management and upgrades for most Cisco devices.

We recommend that you first import a baseline of all software images running on your network.

The baseline imports a copy of each unique software image running on the network (the same image running on multiple devices is imported into the software library only once). The images act as a backup if any of your devices become corrupted and need a new software image or if an error occurs during an upgrade. If some devices are running software images that are not in the software repository, then you can generate a synchronization report for these devices.

Synchronizing the Software Repository

To synchronize the RME software repository, follow these steps:

-
- Step 1** Choose **Resource Manager Essentials > Software Mgmt > Software Repository**.
 - Step 2** Select **Software Repository Synchronization**.
 - Step 3** Click **Schedule**.
 - Step 4** Enter the scheduling information, then click **Submit**.
 - Step 5** Import a baseline of all software images.

Once the Software Repository Synchronization job completes successfully, you can create a job to import all software images on your network by following these steps:

- Step 6** Select **Resource Manager Essentials > Software Mgmt > Software Repository**.
- Step 7** Click **Add**.
- Step 8** Select **Network**.
- Step 9** Select **Use Generated Out-of-Sync Report**, then click **Next**.



Note If you do not select the *Use Generated Out-of-Sync Report* option, it will take longer to show the software image selection dialog box.

All running images that are not in the software repository will be displayed.

- Step 10** Click **Next**, then enter the Job Control Information.
 - Step 11** Click **Next**, then click **Finish**.
-

Managing RME Jobs

Jobs need to be created for performing archive management, editing configuration files, downloading configurations, and managing device IOS/Catalyst OS images. There is a central location where you can view all jobs created for various purposes in RME.

To view all jobs created in RME:

1. Navigate to **CWHP > Resource Manager Essentials > Job Mgmt**.

2. Then select the **RME Jobs** link.

You can search all jobs on criteria such as status of the jobs and types of job.

RME allows you to approve jobs before they are executed.

To configure job approval:

Step 1 Navigate to **CWHP > Resource Manager Essentials > Administration > Approval**.

Step 2 Select the **Approver Details** link.



Note

The user created here should have Approver role in the system (such as local security mode or ACS security mode).

Creating a List of Job Approvers

You must create a list of approvers. The list has to be named and assigned approvers.

Step 3 Navigate to **CWHP > Resource Manager Essentials > Administration > Approval**.

Step 4 Select **Create/Edit Approver Lists**.

Step 5 Provide an Approver name in the top left text field, then click **Add**.

Step 6 Select users from the list of *Available Users* field, then click **Add** (in the middle).

Step 7 Save the configuration of the approval lists.

Specify Which Applications Will Require Job Approval

Step 8 Assign approval lists with the various functions such as NetConfig, Config Editor, Archive Management, and Software Management.

Step 9 Enable Approval policies on the various functions such as NetConfig, Config Editor, Archive Management and Software Management.

Now all jobs created for NetConfig, Config Editor, Archive Management, and Software Management will require approval before they can be executed.

Viewing Jobs Pending Approval

Step 10 You can view all jobs that are pending approval by navigating to **CWHP > Resource Manager Essentials > Job Mgmt**.

Step 11 Select the **Job Approval** link.

The approver can either accept or reject the job. If a job is rejected, the status of the job is updated for the user who created the job.

Importing Devices Into Internetwork Performance Monitor

Once the devices are added into the Device and Credentials Repository, you can import devices from DCR into Internetwork Performance Monitor. IPM interacts with this repository to get the device list, device attributes, and device credentials.

**Note**

Before you import devices from Device and Credential Repository, ensure that there are devices in the repository. Also, there is no mechanism to import only selected devices from DCR into IPM. All the devices in DCR will be imported into IPM. Those devices in DCR that cannot be an IPM source will be not added and in the import log file there will be an error message for that device.

You can import devices as:

- *Sources*

When you import devices as *Sources*, IPM contacts the device and adds them only if they are running IOS image with IP SLA feature and if the Read and Write community strings are provided.

- *Target IP SLA responders*

When devices are imported as *Target IP SLA Responders*, if the device has a read community string, IPM verifies whether the IP SLA responder is enabled or not on the target. If there is not a read community string, the target's IP SLA responder status is not verified.

- *Target IP devices*

When you import devices as *Target IP Devices*, IPM adds the device without either contacting the device or making any verification.

When you import devices from the Device and Credentials Repository, if the devices already exist in IPM, they are updated.

Import status log file. IPM creates a separate log file for the Device and Credentials Repository Import status. You can view the log file in: *IPMROOT/etc/source* or *IPMROOT/etc/target*.

View the results of importing devices. You can view the results of importing devices from the CiscoWorks home page by clicking **View Import Source Log** or **View Import Target Log**.

Device Fault Manager

Administration of the Device Fault Manager server can be categorized into the following topics:

- Daily purging schedule
- Forwarding SNMP traps
- Receiving SNMP traps
- Default SMTP server
- Rediscovery
- Group administration
- Polling and threshold management
- View management

Daily Purging Schedule

A daily purging schedule needs to be set up for fault history information in Device Fault Manager. To set up a purge schedule:

Navigate to the Device Fault Manager panel and choose **Configuration > Other Configuration > Daily Purging Schedule**.

Forwarding SNMP Traps

This configuration can be made to blindly forward traps that come into DFM's trap receiver. These are traps that are received from the devices in the network. To set up trap forwarding:

Navigate to the Device Fault Manager panel and choose **Configuration > Other Configuration > SNMP Trap Forwarding**.



Note

It is not NB trap generation for applications such as HP Open View

Receiving SNMP Traps

This configuration is made for setting the global port for receiving traps in DFM. To set the port used for trap receiving:

Navigate to the Device Fault Manager panel and choose **Configuration > Other Configuration > SNMP Trap Receiving**.

Default SMTP Server

Device Fault Manager has an email notification service that can send emails when alerts or events are generated. This Email notification service needs SMTP Server information for forwarding emails.

To set the SMTP Server information for sending emails:

Navigate to the Device Fault Manager panel and choose **Configuration > Other Configuration > SMTP Default Server**.

Rediscovery

Rediscovery is limited to the list of devices that are known to Device Fault Manager. You can schedule multiple rediscoveries.

To schedule a rediscovery:

Choose **Configuration > Other Configuration**, then select the **Rediscovery Schedule** link.



Note

Rediscovery does *not* add devices into DCR as it does in Campus Manager.

Group Administration

Group administration's function is to create, edit, or delete groups internal to Device Fault Manager. These groups can be shared with other applications.

To create Device Fault Manager groups:

Navigate to **Configuration > Other Configuration**, then select the **Group Administration** link.

Setting Polling and Threshold Parameters

For the faults and events to show up in Device Fault Manager, you must set polling and threshold parameters.

- *Polling parameters* make the Device Fault Manager server poll the devices in the various groups at specified intervals.
- *Threshold parameters* determine the thresholds for various devices. When these thresholds are crossed for the various types of devices, alerts are raised in Device Fault Manager server.

To set the polling and threshold parameters:

Navigate to **CWHP > Device Fault Manager > Configuration**, then select the **Polling and Threshold** link.

Creating Views

View management allows the operator to see alerts and activities on a group of devices. You can create a view on a list of groups and this view will be visible in the Alerts and Activities window under Device Fault Manager.

To create views:

Navigate to **Configuration > Other Configuration**, then select the **Alerts and Activities Defaults** link.

CiscoView

CiscoView is a web-based device management application that provides dynamic status, monitoring, and configuration information for the broad range of Cisco internetworking products. CiscoView displays a physical view of a device chassis, with color-coding of modules and ports for at-a-glance status. Monitoring capabilities display performance and other statistics. Configuration capabilities allow comprehensive changes to devices, given requisite security privileges are granted.

CiscoView now provides a light-weight HTML-based client. It also incorporates IPv6 functionality with the manageability over IPv4 addresses.

To launch CiscoView, navigate to **CWHP > CiscoView > Chassis View**.

Device Center

Device Center is a portal within the LMS solution that provides the ability to gather and debug information about a particular device. The *Summary* in Device Center provides the following information:

- Device IP address
- Device type
- 24-hour change audit summary
- Last inventory and configuration collection times
- Syslog summary
- Fault-related alerts for the device and the neighboring devices

Device Center also provides a set of functions that help facilitate debugging, run reports on the device, and any management tasks, such as changing credentials.

Device Center is installed as part of the Common Services installation. To launch Device Center:

Navigate to **CWHP > Device Troubleshooting > Device Center**.



Note

The information populated in the Device Center depends on which applications are installed on the LMS server.

Launching Debugging Utilities

To launch debugging utilities on a particular device, follow these steps:

-
- Step 1** Browse through the group hierarchies to select a device or search for a particular device by typing in the name in the search utility provided above the group selector.
- Step 2** Click the link on the device name after you have selected it.
- This launches the summary and tools page for the device.
- You can look at the 24-hour reports on the device in the top half of the right frame and launch tools in the bottom half of the right frame.
-

A suggested list of tools can be launched in the order specified as follows. This list is not complete, but helps to understand some of the tools available in Device Center.

- *Ping*: Ping the device to see if it is reachable from the LMS server.
- *Credential Verification Report*: Launch the Credential Verification Report to check for any missing credentials.
- If the credentials are missing, launch the Edit Device Credentials tool to edit the credentials.
- *Edit Device Credentials tool*: Launch the Detailed Device Report on the device to view memory, flash, image, and IP address information.
- *Fault History Report*: Launch the Fault History Report to view any faults that occurred in the last 24 hours or 31 days.

- *CiscoView tool*: If some faults are found, go to the CiscoView tool to view the chassis and make the necessary changes on the interfaces or ports.
- *Switch Port Usage report*: If the device is a switch, you can launch the Switch Port Usage report for a summary of the ports that are recently up, down, or unused.
- *Archive and image management*: You can synchronize the archive or download a previous archive of the configurations or do a software image upgrade.



Network Management in Cisco LAN Management Solution 2.5

This chapter provides more information on the network management tasks in LMS across the various applications: Device Fault Manager, Resource Manager Essentials, Campus Manager, Internetwork Performance Monitor, and Common Services.



Note

This chapter includes a subset of possible network management examples for the suite of LMS applications. Please note that this chapter does not provide a comprehensive reference for LMS network management.

Fault Monitoring

The Device Fault Manager (DFM) gives you the option of monitoring faults in three distinct ways:

- You can look at historic fault data using fault history.
- You can choose to be notified by email, trap messages, or Syslog messages.
- You can look at the current faults in real-time in an alerts and activities window.

Set Up Tasks

The following tasks must be completed before fault monitoring can be enabled in Device Fault Manager:

Add List of Devices From the DCR

A list of devices must be added from the Device and Credentials Repository into the Device Fault Manager.

Navigate to **CWHP > Device Fault Manager > Device Management > Device Selector** tool.

Check Status of Devices

The status of all devices should be in the *Known* state:

Choose **Device Fault Manager > Device Management > Device Summary**.

Polling and Threshold Configuration

Faults and events show up automatically for all devices because default polling settings are used for polling the devices.

To set the Polling and Threshold parameters:

1. Navigate to **CWHP > Device Fault Manager > Configuration**.
2. Then select the **Polling and Threshold** link.

This **Polling and Threshold** link provides an option to either change the default polling and threshold setting or to set a new polling and threshold setting for the user-defined device interface and port groups.

Polling parameters are used to make the Device Fault Manager server poll the devices in the various groups at specified intervals.

Threshold parameters determine the thresholds for various devices. When these thresholds are crossed, alerts are raised in the Device Fault Manager server.

Fault and Alerts Notification Services

Various notification services are available in Device Fault Manager to notify you of a fault or alert that occurred in the device.

-
- Step 1** Navigate to **CWHP > Device Fault Manager**.
 - Step 2** Select the **Notification Services** link.
 - Step 3** Create a Notification Group by clicking the **Notification Groups** link.
 - Step 4** Select a group from the group selector, then choose one of the following:
 - Alert severity
 - Event severity
 - Alert status
 - Event status for the devices in the group to send notification
 - Step 5** Click **Next**.
 - Step 6** Provide the notification group name and click **Next**.
 - Step 7** Click **Finish** to create the notification group.
 - Step 8** To send traps to NB applications like HP Open View Network Node Manager when a notification needs to be raised per notification group, click the **SNMP Trap Notification** link.
 - Step 9** To send email notification to a user when a notification needs to be raised per notification group, click the **E-Mail Notification** link.
 - Step 10** To send syslog messages to other machines when a notification needs to be raised on a notification group, click the **Syslog Notification** link.
-

Fault History

No configuration is needed in Fault History. All faults in the devices are automatically accumulated and can be viewed:

Navigate to **Device Fault Manager**, then select the **Fault History** link.

You can view the faults by searching for a single device, a group of devices, a fault ID, or an event ID.

Alerts and Activities

The Alerts and Activities window shows the real-time display of faults on devices or views.

To launch the Alerts and Activities window:

Navigate to **CWHP > Device Fault Manager**, then click the **Alerts and Activities** link.

For related information, see the [“Creating Views” section on page 6-15](#).

Baseline Configuration

All enterprises need to enforce some standard policy across all the devices in the network. Enterprise networks need to audit the policy periodically and enforce the policy if any devices are found in violation of it.

With the RME Baseline template and compliance check you can execute this functionality:

First identify a set of standardized policy-based commands that you want to have on a set of devices. Then create Baseline templates with those set of commands identified. After creating the baseline templates, you can accomplish following tasks.

- Compare device configurations and generate a report that lists all the devices that are non-compliant to the baseline template.
- Deploy the baseline template to the same category of devices in the network.
- Schedule a compliance check job and deploy the baseline template on to the devices.

Data Extraction from LMS Applications

This section describes the Campus Data Extraction Engine and the RME Data Extraction Engine.

Campus Data Extraction Engine

Campus Manager provides a data extraction engine to extract data about the following:

- User tracking data
- Layer 2 topology
- Discrepancies in the network configuration

Data Extraction can be done either through the command-line interface or Servlet access.

The cmexport Utility

You can access the command-line interface utility **cmexport** by going to the *NMSROOT/campus/bin* directory.

The top-level Help provides the following information.

```
cmexport <-h | -v | commands> <arguments>
```

Core Commands

The core data extraction commands are described in [Table 7-1](#).

You must invoke the **cmexport** command with one of the core commands specified in [Table 7-1](#). If no core command is specified, **cmexport** can execute the **-v** or **-h** options only.

Table 7-1 Core Commands: Campus Manager Data Extraction

Core Command	Description
ut	Generates User Tracking data in XML format.
l2topology	Generates Layer 2 topology data in XML format.
discrepancy	Generates discrepancy data in XML format.
-f	Specify the filename and the directory for storing the Data Extraction Engine output.
-h	(Null option) Lists the usage Help information for this utility.
-v	Displays the version of the cmexport utility.

Archival Locations

Data generated through the **cmexport** command-line interface is archived at the following locations by default.

- For User Tracking:
PX_DATADIR/cmexport/ut/timestamput.xml
- For Layer 2 Topology:
PX_DATADIR/cmexport/L2Topology/timestampL2Topology.xml
- For Discrepancy:
PX_DATADIR/cmexport/Discrepancy/timestampDiscrepancy.xml

Directory Locations

- The *PX_DATADIR* directory is at these locations:
 - Windows: *%NMSROOT%\files* folder
 - Solaris: */var/adm/CSCOpX/files*
- NMSROOT* is the directory where you installed Campus Manager.
- timestamp* is the time at which the log was written in this format:
YearMonthDateHourOfDayMinuteSecond format.

This utility does not inherently delete the files created in the archive. You should delete these files when necessary. However, using the same filename and directory twice would cause the previous file to be overwritten.

Possible Combinations of cmexport Commands

User Tracking

Table 7-2 User Tracking cmexport Parameters

Parameter	Description
-layout	User tracking host data is exported in XML format for the layout given in <i>layoutname</i> . The layout is a custom layout defined by the user in User Tracking. This parameter is applicable only when -host is chosen
-layoutPhone	User tracking phone data is exported in XML format for the layout given in layoutPhone . This parameter is applicable only when -phone is chosen.
-query	User tracking host data is exported in XML format for the query given in <i>queryname</i> . This parameter is applicable only when -host is chosen.
-queryPhone	User tracking phone data is exported in XML format for the query given in <i>phonequeryname</i> . This parameter is applicable only when -phone is chosen.
-view	Specifies the format in which the user tracking XML data is presented. It currently supports two options: <i>switch</i>: User tracking data is displayed based on the switch. <i>subnet</i>: User tracking data is displayed based on the subnet in which they are present.

Example Commands

```
cmexport ut -u admin -p admin -host
cmexport ut -u admin -p admin -phone
cmexport ut -u admin -p admin -host -query dupMAC -layout all
cmexport ut -u admin -p admin -host -query dupMAC -layout <name>
cmexport ut -u admin -p admin -phone -queryPhone <name> -layoutPhone <name>
cmexport ut -u admin -p admin -host -f ut.xml
cmexport ut -u admin -view switch -host
```

Layer 2 Topology or Discrepancy Commands

```
cmexport L2Topology|Discrepancy -u admin -p admin
cmexport L2Topology|Discrepancy -u admin -p admin -f 013104L2.xml
```

Servlet Access to the Data Extraction Engine

The Servlet access to Campus Manager Data Extraction Engine is described below.

The Servlet accepts users request and authenticates the requesting user's identity using Common Services authentication mechanism. The command to export user tracking, topology, and discrepancy can be sent as HTTP or HTTPS requests.

The Servlet requires a payload file that contains details about the user's credentials, the command you want to execute, and optional details, such as log and debug options as inputs in XML format. The Servlet then parses the payload file encoded in XML, performs the operations, and returns the results in XML format. Typically, Servlet access is used to extract data from a client system. While generating data through the Servlet, the output will be displayed at the client terminal.

The input XML file contains various tags for username, password, core command, and optional tags.

Extracting the Export File From the Servlet

The steps to extract the export file from the Servlet are as follows:

-
- Step 1** Generate the necessary payload XML file with the required data.
 - Step 2** Use a script to perform a POST operation to the Servlet with the payload file. The Servlet is:
http://Campus-Server:1741/CSCOnm/campus/servlet/CMExportServlet
 The HTTP response of the Servlet contains the XML file generated by executing the **cmexport** command on the server with the parameters provided in the payload file.
 - Step 3** Extract the XML file from the content of the HTTP response and save it to a local file.
-

Sample Payload

```
<payload>
<!--The following element specifies the username (valid CiscoWorks or ACS user ID) of the
person initiating this DEE call -->
  <username>username</username>
<!-- The following element specifies the valid password of the user ID -->
  <password>password</password>
<!--The following element specifies the DEE command used for extracting User Tracking host,
phone, discrepancy and L2 topology information -->
  <command>ut_host</command>
<!--The following element specifies the logfile where all logs need to be output -->
  <logfile>filename</logfile>
<!--The following element specifies the debug level at which the log is output. -->
  <debug>1</debug>
<!--The following element specifies the custom report name created in the User Tracking
user interface by navigating to CWHP > Campus Manager > User Tracking > Reports > Custom
Reports.>
  <view></view>
</payload>
```

Sample Perl Script to Access the Servlet



Note

Sample scripts are available in the Campus Manager Data Extraction Engine online Help.

```
#!/opt/CSCOpX/bin/perl
use LWP::UserAgent;
$| = 1;
$temp = $ARGV[0] ;
$fname = $ARGV[1] ;
if ( -f $fname ) {
open (FILE,$fname) || die "File open Failed $!";
while ( <FILE> )
{
    $str .= $_ ;
}
close(FILE);
}
url_call($temp);
#-- Activate a CGI:
sub url_call {
    my ($url) = @_;
    my $ua = new LWP::UserAgent;
    $ua->timeout(5000);
    my $hdr = new HTTP::Headers 'Content-Type' => 'text/html';
    my $req = new HTTP::Request ('GET', $url, $hdr);
    $req->content($str);
    my $res = $ua->request($req);
    my $result;
    if ($res->is_error)
    {
        print "ERROR : ", $res->code, " : ", $res->message, "\n";
        $result = '';
    }
    else
    {
        $result = $res->content;
        if($result =~ /Authorization error/)
        {
            print "Authorization error\n";
        }
        else
        {
            print $result ;
        }
    }
}
```

The Perl script listed above will invoke the servlet with the use of *payload.xml* file. The command will look similar to these commands for HTTP and HTTPS modes:

- In HTTP mode
`./perl script.pl http://server:1741/campus/servlet/CMExportServlet payload.xml`

- In HTTPS mode:

```
./perl script.pl https://server/campus/servlet/CMExportServlet payload.xml
```

Any user using the Data Extraction Engine is authenticated and authorized. The username and password are either provided as part of the command-line interface and Servlet call or the password is put in a password file for retrieval by the Data Extraction Engine. The access permissions to the file can be set to prevent any unauthorized access. When using this option, the CMEXPORTFILE environment variable should be set so it points to the file containing the credentials. The command should be entered in the following format:

```
cmexport ut -u admin -host
```

This syntax enables **cmexport** to find the relevant password associated with the username (in the example here, for the username *admin*).

Resource Manager Essentials Data Extraction Engine

Resource Manager Essentials provides a data extraction engine to extract data about the following:

- Inventory
- Change audit
- A device's configuration details

Data extraction can be done by either through the command-line interface or Servlet access.

The command-line interface utility **cwcli** can be accessed by going to *NMSROOT/bin* directory.

The top-level Help command **cwcli -help** provides the following information:

General syntax to run a command with arguments is:

```
cwcli <application/command> <arguments>
```

For detailed help on a command and its arguments, run:

```
cwcli <application/command> -help
```

You must invoke the **cwcli** command with one of the core commands specified in [Table 7-3](#). If no core command is specified, **cwcli** can execute the **-v** or **-help** options only.

Table 7-3 Core Commands: Resource Manager Essentials Data Extraction

Core Command	Description
config	Provides a set of commands that are used to download and fetch configurations, compare two different configurations, delete the archived configuration files, and reload the device.
export	Exports inventory/configuration/change audit data in XML.
inventory	A command-line interface tool to create, delete, and cancel an inventory collection job. It also helps in importing or exporting the data in inventory as XML files.
invreport	List all custom reports and generates CSV formatted inventory report(s) for given template(s).
netconfig	A command-line interface tool to create, delete, and cancel a NetConfig job. It also helps in importing or exporting the User Defined Template XML files

Table 7-3 Core Commands: Resource Manager Essentials Data Extraction (continued)

Core Command	Description
-v	Displays the version of the cwcli utility.
-help	(Null option) Lists the usage information for this utility.

Command-Line Syntax

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, configuration, and change audit 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 options are not important. However, you must enter the core command immediately after **cwcli export**.

On UNIX, you can view the cwcli export man pages by setting the MANPATH to:

```
/opt/CSCOpX/man/man1
```

The man pages to launch the **cwcli export** command are **man cwcli-export** to launch the **cwcli export** command.

- To launch the cwcli export changeaudit command: **man export-changeaudit**
- To launch the cwcli export config command: **man export-config**
- To launch the cwcli export inventory command: **man export-inventory**

Data Archiving Location

Data generated through the **cwcli export** command-line interface is archived at the following locations by default:

- Change Audit
 - On Solaris: `/var/adm/CSCOpX/files/rme/archive/YYYY-MM-DD-HH-MM-SS-changeaudit.xml`
 - On Windows: `NMSROOT\files\rme\archive\ YYYY-MM-DD-HH-MM-SS-changeaudit.xml`
- Config
 - On Solaris: `/var/adm/CSCOpX/files/rme/cwconfig/YYYY-MM-DD-HH-MM-SS-MSMSMS-Device_Display_Name.xml`
 - On Windows: `NMSROOT\files\rme\cwconfig\ YYYY-MM-DD-HH-MM-SS-MSMSMS-Device_Display_Name.xml`
- Inventory
 - On Solaris: `/var/adm/CSCOpX/files/rme/archive/YYYY-MM-DD-HH-MM-SS-inventory.xml`
 - On Windows: `NMSROOT\files\rme\archive\ YYYY-MM-DD-HH-MM-SS- inventory.xml`

RME Servlet

The details of Servlet access to RME Data Extraction Engine is given below.

The name of the Servlet is `/rme/cwcli`. The following is the Servlet to be invoked to execute any command:

For a post request

`http://<rme-server>:<rme-port>/rme/cwcli <payload XML file>`

For a get request

`http://<rme-server>:<rme-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 are 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 execute the import command payload.xml is as follows:

```
<payload>
<command>
cwcli config import -u admin -p <Base64Encoded pwd> -device 10.77.240.106
<arg>
-f
</arg>
<arg-val>
banner motd "Welcome, Sir"
</arg-val>
</command>
</payload>
```

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 executed as

```
cwcli config import -u admin -p <Base64Encoded pwd> -device 10.77.240.106 -f tempfile
```

Here the tempfile contains the line banner motd “Welcome, Sir.”

For example:

`Perl samplescript.pl http(s)://<rme-server>:<rme-port>/rme/cwcli <payload XML file>`



Note

For the secure mode (HTTPS), the port number is 443. The default port for CiscoWorks server in HTTP mode is 1741.

Sample Script to Invoke the Servlet

```
#!/opt/CSCOpX/bin/perl
use LWP::UserAgent;
$temp = $ARGV[0] ;
$fname = $ARGV[1] ;
open (FILE,$fname) || die "File open Failed $!";
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 ('POST', $url, $hdr);
    $req->content($str);
    my $res = $ua->request ($req);
    my $result;
    if ($res->is_error)
    {
        print "ERROR : ", $res->code, " : ", $res->message, "\n";
        $result = '';
    }

    else {
        $result = $res->content;
        if($result =~ /Authorization error/)
        {
            print "Authorization error\n";
        }
        else {
            print $result ;
        }
    }
}
```

Internetwork Performance Monitor Export

There has been no change in the way the data can be exported in Internetwork Performance Monitor from the previous version of the product. The `ipm export` command line interface is the command to do IPM export.

The IPM Export Command

The following example shows the command syntax and help that is displayed when you use the `ipm export` Help command:

You must be logged in as the root user (in Solaris) or administrator (in Windows) to use export IPM data using the `ipm export` command.

```
ipm export
[-q] [[-k <letter>] | -w] [-h]
[ ( -c | -s | -t | -o | -cs) [<CollectorName>] ]
| [ (-dh | -dd | -dw | -dm) <StartTime> <EndTime> [ <CollectorName> ] ]
| [ (-jh | -jd | -jw | -jm) <StartTime> <EndTime> [ <CollectorName> ] ]
| [ (-ph | -pd | -pw | -pm) <StartTime> <EndTime> [ <CollectorName> ] ]
| [ -r [<WhichDay>] ]
| [ -all [<StartDate>] [<EndDate>]]
```

General Options

[ipmRoot] Root location of IPM, such as `/opt/CSCOipm`.

- q** Quiet output- Display no column headings. Only applicable in plain text output format.
- k** Delimiter- set the field delimiter to <letter>. By default, this is set to a comma ','. Only applicable in plain text output format.
- w** HTML output - A web page will be generated from the output of this command.
- h** Help - output this usage help

Format:

Time: <StartTime> and <EndTime> need to be input as:

MM/DD/YYYY-hh:mm:ss

Date: <WhichDay> needs to be input as:

MM/DD/YYYY

<StartDate> and <EndDate> need to be input as:

MM/DD/YYYY

The DCR Command Line Interface

Using the command line interface, you can add, delete, modify devices and change Device and Credentials Repository modes. You can also view the list of DCR attributes that can be stored in DCR, and view the current DCR mode.

The main command to launch is at:

```
NMSROOT/bin/dcrcli
```

The steps are as follows:

-
- Step 1** Enter `NMSROOT/bin/dcrcli -u username`
 - Step 2** Enter the password corresponding to the username.
 - Step 3** Select one of the various top-level commands:
 - **add:** Adds a device.

- **del**: Deletes a device.
 - **details**: View device details.
 - **exp**: Export to a file.
 - **impFile, impNms, impRNms, impACS**: Imports a device list from File, Local NMS, Remote NMS and ACS (AAA server).
 - **lsattr**: Lists the attributes stored in DCR.
 - **lsmode**: Lists the DCR mode as Master, Slave or Standalone.
 - **mod**: Modifies a device.
 - **setmaster, setstand, setslave**: Sets the DCR to Master, Standalone or Slave mode.
-

User Tracking Reports

You can generate User Tracking (UT) Reports by navigating to **CWHP > Campus Manager > User Tracking**. Then select the **Reports** link.

You can generate the following reports:

- Provides the ability to quickly view reports on end hosts and IP phones. A simple query can be input to view a subset of the end hosts or IP phones present in User Tracking.
- Run reports on switch port usage statistics of the switches. You can run the switch port usage reports for recently down, unused down, and unused up ports.
- List the jobs that are run periodically to generate reports. These jobs are for generating reports on end hosts, IP phones, duplicate device entries, and switch port usage.

You can find the report job listing by navigating to **User Tracking > Reports > Report Jobs** link.

- Generate Custom reports for end hosts and IP phones by selecting a group, then evaluating a query on the group to subset the number of end hosts and IP phones.

You can generate Custom reports by navigating to **User Tracking > Reports > Custom Reports**. You can save the custom reports.

You can use the custom reports while generating detailed reports on end hosts or IP phones by going to **User Tracking > Reports > Report Generator**.

Configuring Syslog on Devices

LMS has the ability to collect and analyze syslog messages received from devices in the network. The ability to collect syslog messages helps manage the network more effectively. Enabling syslog messages provides a number of advantages:

- LMS will collect and update any configuration and inventory changes on the network.
- Received syslog messages can be analyzed and can also be used for further triggering automated actions.

Enabling Syslogs Through NetConfig

Syslogs can be enabled on devices using NetConfig. A template for enabling Syslogs is built in NetConfig.

You can access the template under **Resource Manager Essentials > Config Mgmt > NetConfig**.

Create a NetConfig Job

Create a NetConfig job by going to the TOC menu, and clicking **NetConfig Jobs**.

Once the device configurations are being managed by RME, you can enable syslogs through NetConfig. RME 4.0 provides the ability to schedule a single job for devices using Cisco IOS and Catalyst OS.

VLAN Recommendations

Campus Manager provides the ability to view VLANs and to get recommendations on spanning trees. The different types of spanning trees that are supported for recommendations are PVST, MIST and 802.1s.

Since most of the switched traffic is directed through the *root bridge*, it is essential to have the proper switch designated as the root bridge. Campus Manager provides the ability to select the root bridge based on the following criteria:

1. Least depth

The least depth method would help the user select a root for the particular VLAN that would provide the least from each node in the network to the root. The spanning tree formed in this selection would have the minimum depth.

2. Least cost

Least cost recommendation will provide a recommendation on a root that would be the least cost from all the nodes in the switch cloud.

3. Traffic data

Campus Manager can also recommend the root bridge based on the traffic in the network. Campus Manager accepts traffic information from two sources: Cisco Network Analysis Module (NAM) and the NetFlow collector.

Viewing the Least Depth Spanning Tree Recommendation

To see the least depth spanning tree recommendation:

-
- Step 1** Navigate to **Topology Services > Network Views > LAN Edge View**.
 - Step 2** Select the desired switch cloud.
 - Step 3** Click **Display View**.
 - Step 4** In the Switch Cloud view, select **Reports**.
 - Step 5** To run optimal root and instance reduction and instance recommendation reports, select one of these options:
 - **Per VLAN STP Recommendations**

- Cisco MISTP Recommendations
 - IEEE 802.1s Recommendations
-

Ether Channel and Trunk Deployment

Campus Manager Topology Services Layer 2 view also provides the ability to configure Ether channels and trunks.

Ether Channel Configuration

To configure an Ether channel:

-
- Step 1** Select a link on the Layer 2 view.
 - Step 2** Right-click and select **Configure Ether Channel**.
The Ether Channel Configuration window appears.
 - Step 3** Specify **PagP** for the *Ether Channel protocol*.
 - Step 4** Set the channel mode to **Desirable**.
 - Step 5** The *distribution protocol* can be set to **ip**, **mac**, or **port**.
 - Step 6** You can set the *distribution address type* to **source**, **destination**, or **both**.
The Ether Channel Configuration window also displays all the links between the two devices where the Ether channel is being set up.
 - Step 7** You can select the links that should be part of the Ether channel.
The configuration window also provides the ability to copy the running configuration to startup configuration.
-

Trunk Configuration

To configure a trunk:

-
- Step 1** Right-click a particular link and select **Create Trunk**.
 - Step 2** Select the type of encapsulation:
 - 802.1Q
 - ISL
 - Negotiate
 - Step 3** Enter the *Allowed* and *Disallowed* VLANs on that trunk.
-

Configuration File Change Management

This section discusses the applications that handle configuration file change management.

RME Config Editor

You can use the RME Config Editor function to edit a device configuration stored in the configuration archive and download it to the device. The Config Editor tool allows you to make changes to any version of a configuration file, review changes, and then download the changes to the device.

The Config Editor now allows multiple users to edit configuration files simultaneously. You can save these configuration files to a private work area.

NetConfig Templates

The NetConfig function provides a set of command templates that can be used to update the device configuration on multiple devices all at once. The NetConfig tool provides wizard-based templates to simplify and reduce the time it takes to roll out global changes to network devices.

You can use these templates to execute one or more configuration commands on multiple devices at the same time. For example, to change SNMP community strings on a regular basis (to increase security on devices), use the appropriate SNMP template to update community strings on all devices using the same job. A copy of all updated configurations will be automatically stored in the configuration archive.

NetConfig comes with several predefined templates containing all the necessary commands. You simply supply the parameters for the command and NetConfig takes care of the actual command syntax. These predefined templates include corresponding rollback commands; therefore, if a job fails on a device, the configuration will be returned to its original state.

Change Audit Reports

All changes made on the network through LMS are recorded as part of a change audit. If syslogs are enabled on devices, any out-of-band changes made on the devices are also recorded as part of change audit.

To view Change Audit reports:

Step 1 Navigate to **Resource Manager Essentials > Reports > Report Generator**.

Step 2 Select **Change Audit** as the application.

Select the report type:

- 24-hour report
 - Standard report
 - Exception Period report
-

These reports help manage the changes on the network. Resource Manager Essentials also provides the capability to have an *Audit Trail*. An Audit Trail provides a trail of all the changes that are made on the server, for example, addition or deletion of devices, or a credential change.



A

Access Control Server

- ACS login mode for Common Services [4-7](#)
- client model [4-6](#)
- integrating with LMS [4-6](#)
- network device groups [4-8](#)
- role mapping [4-8](#)
- setting up [4-6](#)
- System Identity User, configuring [4-8](#)

alerts and activities window [7-3](#)

ANIServer

- heap size [6-5](#)
- application modes
 - Auto Synchronize mode [4-1](#)
 - manual mode [4-1](#)

B

backing up LMS data [6-2](#)

backup recommendations [3-2](#)

baseline template [7-3](#)

bridge ID priority [2-10](#)

bulk device import [5-2](#)

- editing imported device credentials [5-3](#)
- file import [5-2](#)
- Local NMS import [5-3](#)
- Remote NMS option [5-3](#)

C

Campus Manager [1-2](#)

- auto synchronization enabled [4-1](#)
- and CDP [2-6, 5-1](#)
- current device status [5-5](#)
- data collection [6-4](#)
- data extraction engine [7-3](#)
- device discovery [6-3](#)
- hierarchical groups [6-6](#)
- seed device, defining [5-2](#)
- User Tracking [6-5](#)
- User Tracking reports [7-13](#)
- VLAN recommendations [7-14](#)

CDP [2-6](#)

- configuring on Catalyst 6500 switches [2-7](#)
- enabling and disabling [2-6](#)

change audit [6-9](#)

- reports, viewing [7-16](#)

CiscoView [1-1, 6-15](#)

cmexport utility [7-4](#)

collectors [1-2](#)

command line prompt requirements [2-4](#)

Common Services [1-1, 6-1](#)

- ACS login mode [4-7](#)
- Device Center [6-16](#)
- device grouping [6-2](#)
- user defined groups, creating [6-2](#)

community strings

- SNMP [2-2](#)

Config Editor [7-16](#)

configuration files
 purging archived files [6-8](#)
 configuration management [4-2, 7-16](#)

D

data collection
 ANIServer heap size [6-5](#)
 Campus Manager [6-4](#)
 IP address filters, setting [6-5](#)
 VTP filters, setting [6-5](#)
 data extraction engine [7-3](#)
 cmexport utility [7-4](#)
 extracting the export file [7-6](#)
 servlet access to [7-6](#)
 debugging utilities, launching [6-16](#)
 default roles in CiscoWorks [4-8](#)
 Device and Credentials Repository (DCR) [1-3](#)
 bulk device import into [5-2](#)
 and Campus Manager [6-5](#)
 command-line interface [7-12](#)
 update procedure [5-3](#)
 Device Center [6-16](#)
 debugging utilities, launching [6-16](#)
 Device Fault Manager [1-2](#)
 alerts and activities window [7-3](#)
 Auto Synchronize mode, disabling [4-1](#)
 check status of devices [7-1](#)
 CiscoView [6-15](#)
 current device status [5-5](#)
 daily purging schedule [6-14](#)
 default SMTP server [6-14](#)
 fault history [7-3](#)
 group administration [6-15](#)
 notification services [7-2](#)
 polling and threshold parameters [6-15, 7-2](#)
 rediscovery [6-14](#)
 set up tasks [7-1](#)
 SNMP traps

Device Fault Manager (continued)
 forwarding [6-14](#)
 receiving [6-14](#)
 views, creating [6-15](#)
 device grouping [6-2](#)
 dmgttd.conf file, changes to [6-5](#)
 DNS lookup, disabling [6-4](#)
 domain name [2-2](#)
 and SSH configuration [2-5](#)

E

enable prompt [2-4](#)
 enabling traps [2-3](#)
 Ether channel configuration [7-15](#)
 exception period [6-10](#)

F

fault history [7-3](#)
 file import [5-2](#)
 filters
 IP address or VTP domain filters, setting [6-5](#)

H

hierarchical groups [6-6](#)
 HTTP server
 http mode [2-8](#)
 HTTPS server [2-8](#)

I

installation
 order of LMS applications [3-2](#)
 Solaris server requirements [3-1](#)
 Windows server requirements [3-2](#)
 Integration Utility [1-1](#)

Internetwork Performance Monitor

- collectors [1-2](#)
- exporting data [7-11](#)
- importing devices into [6-13](#)
- source device [6-13](#)
- target IP devices [6-13](#)
- target IP SLA responders [6-13](#)
- inventory filters [6-10](#)
- IP filters, setting up [6-4](#)

L

- License file [3-4](#)
- licensing [3-4](#)
- LMS
 - and Access Control Server [4-6](#)
 - application modes [4-1](#)
 - backing up data [6-2](#)
 - communicate with ACS server [4-7](#)
 - Device Center [6-16](#)
 - dmgttd.conf file, changes to [6-5](#)
 - HTTPS, enabling [4-5](#)
 - integrating with ACS [4-6](#)
 - licensing [3-4](#)
 - migrating from LMS 2.x to 2.5 [1-2](#)
 - order of installation [3-2](#)
 - port assignments [3-3](#)
 - restarting the server [4-5, 4-7](#)
 - restoring data [6-3](#)
 - security setup [4-4](#)
 - server-ip-address parameter [2-5](#)
 - SSL enabled [4-5](#)
 - syslog messages from devices [7-13](#)
 - URL for accessing server [4-5](#)
 - versions available [1-2](#)
- local NMS import [5-3](#)
- login prompt [2-4](#)

M

- MAC address reduction [2-11](#)
- message filters [6-10](#)
- migrating from LMS 2.x to LMS 2.5 [1-2](#)
- Multiple Instance Spanning-Tree
 - configuring [2-10](#)
- Multiple Spanning-Tree
 - configuring [2-9](#)
- multi-server setup [1-3](#)

N

- NetConfig [2-4](#)
 - create a job [7-14](#)
 - job management utility [7-8](#)
 - template for enabling syslog messages [7-14](#)
 - templates for configuration management [7-16](#)
- network device groups [4-8](#)

P

- peer server account [4-4](#)
- ping sweep [6-6](#)
- port cost, configuring [2-10](#)
- port priority, configuring [2-10](#)
- product authorization key (PAK) [3-4](#)
- product identification number (PIN) [3-4](#)
- protocols
 - protocol ordering [4-3](#)
- PVST+ [2-11](#)
 - default configuration values [2-12](#)
 - MAC address reduction [2-11](#)

R

- RCP
- Remote Copy Protocol. See RCP

Remote NMS option [5-3](#)

Resource Manager Essentials. See RME

restoring LMS data [6-3](#)

RME [1-1](#)

adding devices from DCR [5-4](#)

Auto Synchronize mode, disabling [4-2](#)

baseline template [7-3](#)

change audit [6-10](#)

change audit data, purging [6-9](#)

change audit reports [7-16](#)

Config Editor [7-16](#)

configuration collection status, viewing [5-4](#)

configuration file collection and polling [6-7](#)

configuration files, purging [6-8](#)

confirm config file collection [5-5](#)

data archiving location [7-9](#)

data extraction engine [7-8](#)

device credentials, checking [5-5](#)

exception period, setting [6-10](#)

exclude Syslog messages [6-10](#)

inventory collection [6-7](#)

inventory filters [6-10](#)

jobs

approval [6-12](#)

viewing [6-11](#)

message filters [6-10](#)

polling [6-7](#)

protocols, default order of [6-8](#)

RCP

server-ip-address parameter [2-5](#)

servlet [7-10](#)

Software Image Manager [6-11](#)

software repository synchronization [6-11](#)

syslog messages [2-5](#)

syslog messages, purging [6-9](#)

system reload operation [2-4](#)

Telnet [2-4](#)

role mapping [4-8](#)

root bridge, designating [7-14](#)

S

SCP

exec keyword [2-8](#)

Secure Copy Protocol. See SCP

security [4-4](#)

peer server account [4-4](#)

system-identity user [4-4](#)

seed device [5-1](#)

servlet [7-6](#)

extracting the export file [7-6](#)

Perl script to access servlet [7-7](#)

single sign-on [4-5](#)

SMTP

default server [6-14](#)

SNMP v3

AuthNoPriv mode [2-2](#)

Catalyst OS devices, enabling on [2-3](#)

community strings [2-2](#)

IOS devices, enabling on [2-2](#)

Software Image Manager

baseline of images, importing [6-11](#)

software repository synchronization [6-11](#)

software repository synchronization [6-11](#)

Solaris

disk partitions [3-1](#)

installation requirements [3-1](#)

spanning trees

least depth recommendation [7-14](#)

root bridge, designating [7-14](#)

supported [7-14](#)

SSH [2-4](#)

synthetic traffic generation technology [1-2](#)

Syslog

exclude messages from Analyzer [6-10](#)

purging messages [6-9](#)

syslog messages [2-5](#)

and NetConfig [7-14](#)

server-ip-address parameter [2-5](#)

System Identity User [4-4](#)
 adding in ACS server [4-7](#)
 configuring in ACS [4-8](#)
 system name [2-1](#)
 system reload [2-4](#)

T

target IP devices [6-13](#)
 target IP SLA responders [6-13](#)
 Telnet [2-4](#)
 traps
 enabling [2-3](#)
 trunk configuration [7-15](#)
 trunking, enabling on Catalyst switches [2-14](#)

U

upgrading from LMS 2.x to LMS 2.5 [1-2](#)
 user defined groups, creating [6-2](#)
 User Tracking [6-5](#)
 cmexport parameters [7-5](#)
 custom reports [7-13](#)
 enable for DHCP environment [6-5](#)
 major acquisition [6-5](#)
 minor acquisition [6-5](#)
 ping sweep [6-6](#)
 purge policies [6-6](#)
 report job listing [7-13](#)
 reports [7-13](#)

V

VLAN recommendations [7-14](#)
 VLAN-to-instance mapping [2-9](#)
 VPN 3000 concentrator
 enabling HTTPS mode [2-8](#)

VTP [2-13](#)
 modes [2-13](#)

W

Windows server
 installation requirements [3-2](#)

