Monitoring and Troubleshooting With Cisco Prime LAN Management Solution 4.1
CONTENTS

Notices xix
OpenSSL/OpenSSL Project xix
License Issues xix
EMC Project xxi

Preface xxxi
Audience xxxi
Document Conventions xxxii
Product Documentation xxxii
Obtaining Documentation and Submitting a Service Request xxxiv

CHAPTER 1
Overview of Monitoring and Troubleshooting 1-1
What is Monitoring and Troubleshooting? 1-1
What’s New in Monitoring and Troubleshooting in LMS 4.1? 1-2
Key Acronyms, Terms, and Definitions 1-3

CHAPTER 2
Setting Up Monitoring Thresholds 2-1
Managing Fault Thresholds 2-1
Viewing Thresholds 2-2
Previewing Thresholds 2-3
Editing Thresholds 2-5
Restoring Factory Settings for Thresholds 2-7
Threshold Categories for Devices, Interfaces, and Ports 2-8
Threshold Definitions 2-10
Backup Interface Support 2-11
Dial-On-Demand Interface Support 2-11
Environment 2-11
Generic Interface/Port Performance 2-11
Interface/Port Flapping 2-13
Processor and Memory 2-13
Reachability 2-14
Threshold Parameter Values and Events 2-15
Setting Up Performance Thresholds 2-16
Creating a Threshold 2-18
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling Catalyst Devices to Send SNMP Traps to LMS</td>
<td>3-23</td>
</tr>
<tr>
<td>Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs</td>
<td>3-24</td>
</tr>
<tr>
<td>Updating the SNMP Trap Receiving Port</td>
<td>3-24</td>
</tr>
<tr>
<td>Configuring SNMP Trap Forwarding</td>
<td>3-25</td>
</tr>
<tr>
<td>Viewing Fault Device Details</td>
<td>3-25</td>
</tr>
<tr>
<td>Fault Device Details</td>
<td>3-25</td>
</tr>
<tr>
<td>Understanding the Detailed Device View</td>
<td>3-26</td>
</tr>
<tr>
<td>Managing/Unmanaging a Single Device Component</td>
<td>3-27</td>
</tr>
<tr>
<td>Performing Bulk Manage/Unmanage Operations</td>
<td>3-28</td>
</tr>
</tbody>
</table>

**CHAPTER 4**

Performance Management 4-1

Auto Monitoring 4-1

Managing Pollers 4-2

Creating a Poller 4-4

Instance Selector 4-10

Editing a Poller 4-11

Deleting a Poller 4-13

Deactivating a Poller 4-13

Activating a Poller 4-14

Viewing Failures 4-14

Clearing Missed Cycles 4-15

Clearing Failures 4-16

Viewing Poller Configuration Details 4-16

Filtering Poller List 4-17

Selecting Instances 4-17

Polling MIB Objects Exceeding Limit 4-19

Managing Templates 4-19

System-defined Templates 4-19

User-defined Templates 4-23

Creating a Template 4-24

MIB Variable Selector 4-26

Editing a Template 4-26

Deleting a Template 4-27

Copying a Template 4-28

Exporting a Template 4-28

Importing a Template 4-29

Filtering Template List 4-30

Viewing Template Details 4-31
NAM Top N Statistics Portlet  6-34
NAM Attribute Value  6-35
IPSLA Collector Information  6-37
IPSLA Device Categorization  6-38

CHAPTER 7  Using Topology Services  7-1
Understanding Topology Services  7-2
Starting Topology Services  7-2
  Prerequisites to Launch Topology Services  7-3
  Launching Topology Services when the Server is not DNS Resolvable  7-3
  Launching Topology Services from Windows Client  7-4
  Launching Topology Services from Clients Using Internet Explorer 8.0 Browser  7-4
Using Topology Services Legend  7-5
Understanding Topology Services Main Window  7-12
  Understanding Tree View  7-13
Using Topology Services Main Window  7-14
  Navigating in Main Window  7-14
  Understanding the Status Bar  7-16
  Using Find in Main Window  7-17
Understanding Network Topology Views  7-17
  Navigating in Network Topology Views  7-18
  Connecting Securely to Devices From Clients  7-20
    Specifying SSH Client  7-20
    Connecting to the Device  7-21
  Displaying Network Views  7-21
Using Panner to View Topology Maps  7-22
Using Network Views  7-23
  Customizing Network Topology Views  7-25
    Saving Network Topology View Layouts  7-26
    Deleting Devices From Network View  7-26
    Rediscovering Devices from Topology Services  7-26
  Changing Network Topology View Layouts  7-27
Starting Cisco Prime LMS Features and Reports From Topology Views  7-27
  Launching NAM from Topology Services  7-29
  Launching VRF-Lite Topology Map  7-30
  Edge VLAN Configuration at Distribution Layer  7-31
  Edge VLAN Configuration at Access Layer with Trunk  7-31
  Modifying Fault Management Alert Settings  7-32
Contents

Modifying Network View Features  7-33
  Changing Network Topology View Properties for One User Role  7-33
  Changing Network Topology View Properties for All Users  7-34
  Setting Background Images for Topology Views  7-35

Understanding Cluster Switches  7-37
  Displaying Cluster Switches  7-37

Using Topology Filters  7-38
  Link Virtualization Status  7-41
  Enabling RMON to Measure Bandwidth Utilization  7-44
    Modifying the Parameters  7-45
    Enabling RMON on All Ports in Selected Devices  7-46
    Enabling RMON on Selected Ports in Selected Devices  7-47
    Disabling RMON  7-48
  Customizing Bandwidth Utilization Filters  7-48
  Highlighting Filtered Devices  7-49

Using Find in Network Topology Views  7-49

Understanding Summary View  7-50
  Highlighting Devices From Summary View  7-50
  Interpreting Summary Information  7-50
    Interpreting Network View Summary Information  7-51
    Interpreting Unconnected Device View Summary Information  7-51

Upgrading Network Topology Views  7-52
  N-Hop View Portlet  7-52
    Configuring the Portlet  7-54

Using Microsoft Visio With Topology Views  7-55
  Downloading the Cisco Visio Stencil File  7-56
  Exporting Network Topology Views to Visio  7-56

Working With Links  7-57
  Interpreting Link Tooltips  7-57
  Displaying Link Attributes  7-57
    Interpreting Link Attributes  7-58
    Displaying Aggregate Link Attributes  7-58
      Interpreting Aggregate Link Attributes  7-59

Time Domain Reflectometry Reports  7-59
  Understanding Time Domain Reflectometry  7-59
  Using Time Domain Reflectometry Reports  7-60
    Running TDR Test for a Link  7-60
    Running TDR Test For a Port  7-62

Working With Devices  7-63
Performing Data Collection for Devices  7-63
Interpreting Device Tooltips  7-64
Displaying Device Labels  7-64
  Interpreting Device Labels  7-64
  Clearing Device Labels  7-64
Displaying Device Attributes  7-65
Viewing End Host Report  7-65
Viewing Switch Port Report  7-65
  Interpreting Device Attributes  7-65
Displaying Port Attributes  7-66
  Interpreting Port Attributes  7-66
Setting Preferred Management Addresses  7-67
Starting CiscoView  7-68
Starting Telnet  7-69
Starting Device Center  7-70
Working With MLS Devices  7-70
  Displaying MLS Reports  7-71
  Interpreting MLS Reports  7-71
Working With Application Servers  7-72
Displaying Device Service Modules  7-73
Displaying Service Attributes  7-74
  Interpreting Service Attributes  7-75
Displaying Network Topology and Layer-2 Services Reports  7-75
Monitoring Protocol Filter by Port  7-76
  Understanding Protocol Filtering  7-76
  Displaying Protocol Filter Information  7-77
Viewing Data Collection Metrics  7-77
Topology Groups  7-78
  Understanding Topology Groups  7-78
  Interpreting Topology Groups Summary Information  7-79
Hierarchical Maps  7-79
  Understanding Hierarchical Maps  7-79
  Viewing Hierarchical Maps  7-80
Topology Services Menu Reference  7-81
  Topology Services Main Window Menu Reference  7-81
  Network Topology View Menu Reference  7-83
Supported Protocols  7-87
  Inter-Switch Link (ISL) Protocol  7-87
  IEEE 802.1Q  7-88
Support for IPv6 in Topology Services 7-88
Topology Changes 7-88
Viewing IPv6 Addresses Report 7-89
Interpreting IPv6 Addresses Report 7-90

CHAPTER 8
Managing Network Spanning Trees 8-1
Understanding Spanning Tree Protocol 8-1
Per VLAN Spanning Tree Protocol 8-2
Multiple Spanning Tree Protocol 8-2
Multiple Instance Spanning Tree Protocol 8-3
Spanning Tree Recommendation Reports 8-3
Spanning Tree Reports: Optimal Root Recommendation Report 8-4
Interpreting Optimal Root Recommendation 8-5
Spanning Tree Reports: Number of Instances Recommendation Report 8-6
Interpreting Number of Instances Recommendation 8-6
Spanning Tree Reports: Instance Reduction Recommendation Report 8-7
Interpreting Instance Reduction Recommendation 8-8
Spanning Tree Reports: VLAN to Instance Mapping Recommendation Report 8-8
Interpreting VLAN to Instance Mapping Recommendation 8-9
Spanning Tree Reports: STP Visualizer 8-10
Interpreting STP Visualizer 8-12
STP Visualizer Notes 8-12
Generating Reports and Configuring STP on the Network 8-13
Reporting and Configuring PVST Port 8-13
Reporting and Configuring MST Port 8-17
Reporting and Configuring MISTP Port 8-21
Reporting and Configuring PVST Device 8-25
Reporting and Configuring MST Device 8-28
Reporting and Configuring MISTP Device 8-32
Reporting and Configuring MST Instance 8-36
Reporting and Configuring MISTP Instance 8-37
Reporting and Configuring PVST Trunk 8-38
Reporting and Configuring MST Trunk 8-40
Reporting and Configuring MISTP Trunk 8-42
Spanning Tree Filters 8-44
STP Inconsistency 8-44
Viewing STP Loop Inconsistency 8-44
Viewing STP PVID Inconsistency 8-45
Viewing STP Root Inconsistency 8-45
Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.1

Viewing STP Type Inconsistency  8-45
STP Filters in Switch Cloud View  8-45
Spanning Tree  8-46
   Viewing Spanning Tree per IEEE 802.1s Instance  8-46
   Viewing Spanning Tree per Cisco MISTP Instances  8-46
   Viewing VLANs in Switch Clouds  8-47

CHAPTER 9

Fault Monitor  9-1
   Starting Fault Monitor  9-1
   Understanding Fault Monitor  9-2
      Understanding the Layout of Fault Monitor and Events Displays  9-3
         Group Selector  9-3
         Device Fault Summary Tab  9-3
         Faults Tab  9-4
         Window Tools Area  9-4
         Action Button Area on the Device Fault Summary and Fault Tabs  9-5
   Using Fault Monitor  9-5
      Accessing Device and Event Details Windows from within Fault Monitor Tabs  9-5
      Viewing Device Data using Device Fault Summary Tab  9-6
         Owning Faults— Using the Device Fault Summary Tab  9-6
         Clearing Events— Using the Device Fault Summary Tab  9-6
         Annotating Faults— Using the Device Fault Summary Tab  9-7
         Sending E-Mail in Response to an Event— Using the Device Fault Summary Tab  9-8
      Viewing Data Using Faults Tab  9-8
         Acknowledging an Event— Using the Fault Monitor Events Tab  9-8
         Clearing an Event— Using the Fault Monitor Events Tab  9-9
         Annotating an Event— Using the Fault Monitor Events Tab  9-9
         Sending E-Mail in Response to an Event— Using the Fault Monitor Events Tab  9-9
      Filtering Data in Fault Monitor Tabs  9-10
   Event Forensics  9-10
      Using Event Monitor  9-11
         Starting Event Monitor  9-12
         Understanding Event Monitor  9-12
            Understanding the Layout of Event Monitor Displays  9-13
            Accessing Event Details Windows from within Event Monitor Tabs  9-18

CHAPTER 10

Using NetShow Commands  10-1
   Working With NetShow Jobs  10-2
      Viewing the Permission Report  10-2
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CHAPTER 10</strong></td>
</tr>
<tr>
<td><strong>Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.1</strong></td>
</tr>
</tbody>
</table>

**NetShow Job Browser**  
Viewing Job Details  
Masking Credentials  
Creating Jobs  
Editing Jobs  
Copying Jobs  
Stopping Jobs  
Retrying Jobs  
Deleting Jobs  
Archiving NetShow Job Output  
Viewing and Analyzing NetShow Output  
Deleting Output Archive  
Command Sets  
System-Defined Command Sets  
Managing Command Sets  
Viewing Command Set Details  
Creating a New Command Set  
Editing Command Sets  
Deleting Command Sets  
Adding and Deleting Adhoc Commands  
Assigning Command Sets  
Showing Assigned Command Sets  
Assigning Command Sets to Users  
Assigning Custom Command Execution Privilege  
Launching show Commands From Device Center  
Using cwcli netshow Command  

**CHAPTER 11**  
About Troubleshooting Tools  
Troubleshooting Network Devices and Endhosts  
Troubleshooting Steps  
Troubleshooting Details  
Device Troubleshooting  
Device Status Details  
Configuration Status Details  
Reachability Details  
Events and Faults Details  
Port Status Details  
Performance Details  
Link Troubleshooting  

**OL-24371-01**
<table>
<thead>
<tr>
<th>Chapter 12: Embedded Event Manager (EEM)</th>
<th>12-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is EEM?</td>
<td>12-1</td>
</tr>
<tr>
<td>Components of Cisco IOS EEM</td>
<td>12-2</td>
</tr>
<tr>
<td>Types of Actions</td>
<td>12-2</td>
</tr>
<tr>
<td>Support for EEM</td>
<td>12-3</td>
</tr>
<tr>
<td>LMS NetConfig Tasks for EEM</td>
<td>12-3</td>
</tr>
<tr>
<td>EEM Environmental Variables Task</td>
<td>12-3</td>
</tr>
<tr>
<td>Embedded Event Manager Task</td>
<td>12-4</td>
</tr>
<tr>
<td>Configuring EEM Using LMS</td>
<td>12-5</td>
</tr>
<tr>
<td>Configuring Environmental Variables</td>
<td>12-6</td>
</tr>
<tr>
<td>Configuring Embedded Event Manager</td>
<td>12-9</td>
</tr>
<tr>
<td>EEM and LMS Reports</td>
<td>12-12</td>
</tr>
<tr>
<td>EEM and LMS NetShow</td>
<td>12-14</td>
</tr>
<tr>
<td>EEM Show Commands</td>
<td>12-17</td>
</tr>
<tr>
<td>EEM Syslogs</td>
<td>12-17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 13: Generic OnLine Diagnostics (GOLD)</th>
<th>13-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is GOLD?</td>
<td>13-1</td>
</tr>
<tr>
<td>Types of Diagnostics</td>
<td>13-2</td>
</tr>
</tbody>
</table>
### Contents

**Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.1**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot-Up Diagnostics</td>
<td>13-2</td>
</tr>
<tr>
<td>Runtime Monitoring</td>
<td>13-2</td>
</tr>
<tr>
<td>Support for GOLD Tests</td>
<td>13-3</td>
</tr>
<tr>
<td>LM S NetConfig Tasks for GOLD Tests</td>
<td>13-3</td>
</tr>
<tr>
<td>GOLD Boot Level Task</td>
<td>13-4</td>
</tr>
<tr>
<td>GOLD Monitoring Test Task</td>
<td>13-4</td>
</tr>
<tr>
<td>GOLD Health Monitoring Test Task</td>
<td>13-6</td>
</tr>
<tr>
<td>Configuring GOLD Tests using LM S</td>
<td>13-7</td>
</tr>
<tr>
<td>Configuring GOLD Boot Level Tests</td>
<td>13-7</td>
</tr>
<tr>
<td>Configuring GOLD Monitoring Tests</td>
<td>13-12</td>
</tr>
<tr>
<td>Configuring GOLD Health Monitoring Tests</td>
<td>13-16</td>
</tr>
<tr>
<td>GOLD Tests and LM S Reports</td>
<td>13-20</td>
</tr>
<tr>
<td>GOLD Tests and LM S NetShow</td>
<td>13-21</td>
</tr>
<tr>
<td>Report on Configured GOLD Tests on Each Device</td>
<td>13-21</td>
</tr>
<tr>
<td>Detailed Report of All the GOLD Test Results</td>
<td>13-24</td>
</tr>
<tr>
<td>GOLD Show Commands</td>
<td>13-26</td>
</tr>
<tr>
<td>GOLD Syslogs</td>
<td>13-26</td>
</tr>
</tbody>
</table>

**CHAPTER 14**

**Managing IPSLA Devices** 14-1

- Understanding the IPSLA Devices Page 14-2
- Viewing IPSLA Devices 14-2
- Automatically Importing DCR Devices 14-3
- Adding Adhoc Target Devices 14-3
- Licensing Behavior While Adding Devices 14-4
- Editing IPSLA Device Attributes 14-4
- Deleting Devices from IPSLA Monitoring 14-5

**CHAPTER 15**

**Managing Collectors** 15-1

- Understanding Collector Management Page 15-1
- Collector License Information 15-6
- Working with IPSLA Collectors 15-7
- Specifying Source Devices 15-7
- Specifying Target Devices 15-8
- Specifying IPSLA Operations 15-8
- Defining Collectors 15-9
  - Configuring Collectors 15-9
  - Selecting Collectors 15-13
  - Scheduling Collectors 15-14
Chapter 16

Managing Operations 16-1

Overview of IPSLA Operations 16-1
Understanding the List of IPSLA Operations 16-4
Overview of List of Operations Page 16-5
Viewing the List of Defined Operations 16-6
Creating User-Defined Operations 16-9
  General Settings for a User-Defined Operation 16-9
  Specifying Reaction Types 16-12
  Specific Settings for a User-Defined Operation 16-19
  Viewing the Summary of a User-Defined Operation 16-20
Editing User-Defined Operations 16-21
Deleting User-Defined Operations 16-22
Viewing Operation Properties 16-22

Using IPSLA Operations to Measure Network Performance 16-24
  Measuring Network Performance for IP 16-24
    Measuring End-to-End Performance for Echo 16-25
    Defining an Echo Operation 16-26
    Measuring Hop-by-Hop Performance for Path Echo 16-27
    Defining a Path Echo Operation 16-27
  Measuring Network Performance for UDP Echo 16-28
    Defining a UDP Echo Operation 16-30
  Measuring Network Performance for ICMP Jitter 16-31
    Defining an ICMP Jitter Operation 16-32
    Measuring Network Performance for UDP Jitter 16-33
    Defining a UDP Jitter Operation 16-34
### Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.1

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-37</td>
<td>Measuring Network Performance for RTP Defining an RTP Operation</td>
<td>16-37</td>
</tr>
<tr>
<td>16-41</td>
<td>Measuring Network Performance for Gatekeeper Registration Delay Defining a Gatekeeper Registration Delay Operation</td>
<td>16-41</td>
</tr>
<tr>
<td>16-42</td>
<td>Measuring Network Performance for DNS Defining a DNS Operation</td>
<td>16-42</td>
</tr>
<tr>
<td>16-44</td>
<td>Measuring Network Performance for DHCP Defining a DHCP Operation</td>
<td>16-44</td>
</tr>
<tr>
<td>16-45</td>
<td>Measuring Network Performance for HTTP Defining an HTTP Operation</td>
<td>16-45</td>
</tr>
<tr>
<td>16-49</td>
<td>Measuring Network Performance for DLSw Defining a DLSw Operation</td>
<td>16-49</td>
</tr>
<tr>
<td>16-51</td>
<td>Measuring Network Performance for TCP Connect Defining a TCP Connect Operation</td>
<td>16-51</td>
</tr>
<tr>
<td>16-53</td>
<td>Measuring Network Performance for Ethernet Ping Defining an Ethernet Ping Operation</td>
<td>16-53</td>
</tr>
<tr>
<td>16-54</td>
<td>Measuring Network Performance for Ethernet Jitter Defining an Ethernet Jitter Operation</td>
<td>16-54</td>
</tr>
<tr>
<td>16-55</td>
<td>Measuring Network Performance for Ethernet Ping Auto IP SLA Defining an Ethernet Ping Auto IP SLA Operation</td>
<td>16-55</td>
</tr>
<tr>
<td>16-59</td>
<td>Measuring Network Performance for Video Defining a Video Operation</td>
<td>16-59</td>
</tr>
</tbody>
</table>

---

**CHAPTER 17**

**Managing Outage Details**

- Understanding Planned Outage | 17-1
- Creating Planned Outage | 17-2
- Editing Planned Outage | 17-4
- Deleting Planned Outage | 17-4
- Viewing Completed Planned Outages | 17-5

**CHAPTER 18**

**CLI Command Reference**

- Using CLI Command | 18-1
CHAPTER 19
Troubleshooting and FAQs in LMS Monitoring and Troubleshooting 19-1

Frequently Asked Questions 19-1
Performance Management 19-1
NetShow 19-6
Fault Management 19-8
General 19-17
IPSLA Devices 19-21
Operations 19-22
Collectors 19-25
CLI Commands 19-28
IPSLA Monitoring 19-28
Device Management 19-30
VRF-Lite 19-32
## Troubleshooting LMS 19-39

### APPENDIX A

**Notification MIB**
- MIB Definition A-1
- `ciscoEpmHealthNotificationAlarm` Definitions of critical variables A-32

### APPENDIX B

**Processing SNMP Traps**
- Processed SNMP Traps B-1
- Pass-Through SNMP Unidentified Traps B-2
- Unidentified Traps B-6
  - Clearing an Unidentified Trap B-6

### APPENDIX C

**Polling—SNMP and ICMP**
- SNMP and ICMP Polling C-1
  - ICMP Polling C-1
  - SNMP Polling C-2
    - Just-in-Time Polling C-2
    - Consolidating Requests to Optimize Polling C-2
    - Coordinating ICMP and SNMP Polling C-3
    - How LMS Calculates ICMP Polling Intervals C-3

### APPENDIX D

How LMS Troubleshooting Calculates Repeated Restarts and Flapping D-1

### APPENDIX E

Events Processed E-1

### APPENDIX F

MIBs Polled F-1

### INDEX
Notices

The following notices pertain to this software license:

- OpenSSL/OpenSSL Project
- EMC Project

OpenSSL/OpenSSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

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

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

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

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

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).”

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

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

Original SSLeay License:

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

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

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

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

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

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

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

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

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

NOTICES

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

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

EMC Project

EMC Smarts IP Management Suite 7.0 includes software that is subject to the terms and conditions of the following third-party software providers:

Third-Party Software. The EMC SMARTS Software Products include software of third parties from whom EMC Corporation (“EMC”) has received marketing rights and is subject to the following additional terms and conditions:

Advanced Encryption Standard (AES) copyright and license
Smarts software includes AES. Copyright © 2003, Dr. Brian Gladman <brg@gladman.me.uk>, Worcester, UK. All rights reserved.

License Terms:
The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. Distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. Distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. The copyright holder’s name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

Disclaimer: This software is provided ‘as is’ with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose. Issue Date: 26/08/2003

Data Encryption Standard (DES) copyright and license
Smarts software includes an implementation of DES. Copyright Dr. Brian Gladman. All rights reserved.

FLEXnet copyright and license
Smarts software includes the FLEXnet licensing software. Copyright 1994-2004, Macrovision Corporation. All rights reserved. FLEXnet and FLEXlm are registered trademarks of Macrovision Corporation.
GNU inetutils copyright and license
Smarts software includes the GNU inetutils licensed under the terms of the GNU Public License (GPL).

HMAC copyright and license
Smarts software includes HMAC. Copyright 2002, Dr. Brian Gladman, Worcester, UK. All rights reserved.

LICENSE TERMS
The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder’s name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER
This software is provided ’as is’ with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

HP-UX Runtime Environment for the Java™ 2 Platform Copyright and License
Smarts software includes the HP-UX Runtime for the Java™ 2 Platform, distributed pursuant to and governed by Hewlett-Packard Co. (“HP”) software license terms set forth in detail at: http://www.hp.com. Please check the Software to determine the version of Java runtime distributed to you.

J2SSH Copyright and License
Smarts software includes J2SSH 0.2.7 licensed under the terms of the GNU Lesser General Public Licence (LGPL). Copyright (C) 2002-2003 Lee David Painter and Contributors

JacORB copyright and license
Smarts software includes JacORB 2.1 licensed under the terms of the GNU Lesser General Public License (LGPL).

Jakarta Commons HTTP client copyright and license
Smarts software includes Jakarta Commons HTTP client 2.02 licensed under the conditions of the Apache Software License Version 2.0. The original source code is available at http://www.apache.org/. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.
Jakarta Commons Logging copyright and license

Smarts software includes Jakarta Commons Logging 1.02 licensed under the conditions of the Apache Software License version 2.0. The original source code is available at http://www.apache.org/. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Java 2 Platform Standard Edition Runtime Environment 5.0 copyright and license

Smarts software includes the Java 2 JRE 5.0 licensed under the terms of the Sun Microsystems, Inc. Binary Code License Agreement for the JAVA 2 PLATFORM STANDARD EDITION RUNTIME ENVIRONMENT 5.0. Copyright © 2006 Sun Microsystems, All rights reserved.

JavaCC copyright and license

Smarts software includes JavaCC 3.2. Copyright (c) 2003 Sun Microsystems, Inc. All Rights Reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

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

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

Neither the name of Sun Microsystems, Inc. or the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission. This software is provided “AS IS”, without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN Microsystems, Inc. (“SUN”) AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. You acknowledge that this software is not designed, licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility.

JFreeChart copyright and license

Smarts software includes JFreeChart 0.9.3 licensed under the terms of the GNU Lesser General Public Licence (LGPL). Copyright 2000-2002, by Simba Management Limited and Contributors. Please note that JFreeChart is distributed WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Log4j copyright and license

Smarts software includes log4j 1.2.8 licensed under the conditions of the Apache Software License version 1.1. The original source code is available at http://www.apache.org/. Copyright 1999 The Apache Software Foundation. All rights reserved. THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetBSD routines copyright and license
Smarts software includes NetBSD routines for regular expressions. Copyright the University of California at Berkeley, The NetBSD Foundation, Henry Spencer, and Christopher G. Demetriou. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed for the NetBSD Project. See http://www.netbsd.org for information about NetBSD.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

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

Perl copyright and license
Smarts software includes Perl 5.6.1 and Perl 5.8.0 licensed under the terms of the Perl Artistic License. The “Artistic License” Preamble The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications. Definitions: “Package” refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification. “Standard Version” refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.“Copyright Holder” is whoever is named in the copyright or copyrights for the package. “You” is you, if you're thinking about copying or distributing this Package. “Reasonable copying fee” is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)
“Freely Available” means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:
   a. place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.
   b. use the modified Package only within your corporation or organization.
   c. rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.
   d. make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:
   a. distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.
   b. accompany the distribution with the machine-readable source of the Package with your modifications.
   c. give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.
   d. make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own. You may embed this Package’s interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called “undump” or “unexec” methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.
7. C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these subroutines do not change the language in any way that would cause it to fail the regression tests for the language.

8. Aggregation of this Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Package's interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.

9. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Secure Hash Algorithm (SHA)
Smarts software includes SHA-1 and SHA-2. Copyright (c) 2002, Dr. Brian Gladman, Worcester, UK. All rights reserved. LICENSE TERMS The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;

2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;

3. the copyright holder's name is not used to endorse products built using this software without specific written permission. ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER
This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

SUN Microsystems IDL copyright and license
Smarts software includes the IDL Compiler Software licensed under the following terms and conditions:Copyright 1992, 1993, 1994 Sun Microsystems, Inc. Printed in the United States of America. All Rights Reserved. This product is protected by copyright and distributed under the following license restricting its use. The Interface Definition Language Compiler Front End (CFE) is made available for your use provided that you include this license and copyright notice on all media and documentation and the software program in which this product is incorporated in whole or part. You may copy and extend functionality (but may not remove functionality) of the Interface Definition Language CFE without charge, but you are not authorized to license or distribute it to anyone else except as part of a product or program developed by you or with the express written consent of Sun Microsystems, Inc. (“Sun”). The names of Sun Microsystems, Inc. and any of its subsidiaries or affiliates may not be used in advertising or publicity pertaining to distribution of Interface Definition Language CFE as permitted herein. This license is effective until terminated by Sun for failure to comply with this license. Upon termination, you shall destroy or return all code and documentation for the Interface Definition Language CFE. INTERFACE DEFINITION LANGUAGE CFE IS PROVIDED “AS IS” WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. INTERFACE DEFINITION LANGUAGE CFE IS
Provided with no support and without any obligation on the part of Sun or any of its subsidiaries or affiliates to assist in its use, correction, modification or enhancement, Sun or any of its subsidiaries or affiliates shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by interface definition language CFE or any part thereof. In no event will Sun or any of its subsidiaries or affiliates be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages. Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19. Sun, Sun Microsystems and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc.

SunSoft, Inc.
2550 Garcia Avenue
Mountain View, California 94043
SunOS, SunSoft, Sun, Solaris, Sun Microsystems or the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc.

Visual C++ runtime files
Smarts software includes Visual C++ runtime files licensed under the terms of the Visual Studio 2005 license. Copyright 2006 Microsoft Corporation. All rights reserved.

Xerces 2.1.0 copyright and license
Smarts software includes Xerces 2.1.0 licensed under the conditions of the Apache Software version 1.1. Copyright (c) 2000 The Apache Software Foundation. All rights reserved. This software is provided “as is” and any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the Apache Software Foundation or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Apache Software License Version 1.1
Copyright (c) 2000 The Apache Software Foundation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: “This product includes software developed by the Apache Software Foundation (http://www.apache.org/).” Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names “Apache” and “Apache Software Foundation” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called “Apache”, nor may “Apache” appear in their name, without prior written permission of the Apache Software Foundation. THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Apache Software License Version 2.0

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions. “License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. “Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. “Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity, “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License. “Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. “Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. “Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). “Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. “Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.” “Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.
2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
   a. You must give any other recipients of the Work or Derivative Works a copy of this License; and
   b. You must cause any modified files to carry prominent notices stating that You changed the files; and
   c. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
   d. If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT,
MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, workstoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works hereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.
Preface

This guide describes the use of the Monitoring and Troubleshooting tools in Cisco Prime LAN Management Solution 4.1.

This preface provides an outline of the organization of other chapters in this guide, details about related documents that support this application, and demonstrates the styles and conventions used in this guide. This preface contains:

- Audience
- Document Conventions
- Product Documentation
- Obtaining Documentation and Submitting a Service Request

Audience

This guide is for users who are skilled in network administration and management, and for network operators who use this guide to monitor the utilization and availability of a device connected to the network, using LAN Management Solution. The network administrator or operator should be familiar with the following:

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

Table 1 describes the conventions followed in the user guide.

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

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

Product Documentation

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

Table 2 describes the product documentation that is available.

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Title</td>
<td>Available Formats</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Documentation Roadmap for Cisco Prime LAN Management Solution 4.1</td>
<td>• Printed document part of Software kit</td>
</tr>
<tr>
<td>Context-sensitive online help</td>
<td>• In the LMS Home Page, Click <strong>Help</strong> (extreme right corner of your browser window).</td>
</tr>
</tbody>
</table>
Obtaining Documentation and Submitting a Service Request

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


Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
Overview of Monitoring and Troubleshooting

This section provides an overview of Monitoring and Troubleshooting of Cisco Prime LAN Management Solution 4.1.

This contains:
- What is Monitoring and Troubleshooting?
- What’s New in Monitoring and Troubleshooting in LMS 4.1?
- Key Acronyms, Terms, and Definitions

What is Monitoring and Troubleshooting?

Monitoring and Troubleshooting in LMS allows you to monitor the health and performance of network devices, notifies the list of active problems on the network and the changes occurring on the network, and helps you to identify the problems from a single place.

LMS provides you with monitoring dashboards and tools that provide summarized information about the health of the network and allows you to monitor the network.

Using the various monitoring tools, you can drill down to specific events and launch context-sensitive troubleshooting tools.

The key features of Monitoring and Troubleshooting are:
- Monitor dashboards — Provides Monitoring, EnergyWise and Identity dashboards to monitor the status and the performance of network.
- Monitoring tools — Provides tools such as Fault Monitor, Event Monitor, MiniRMON and Topology Services to view the information on network faults, events, links and ports in the network and perform remote monitoring functions.
- Diagnostic tools — Provides framework such as Embedded Event Manager (EEM) and Generic Online Diagnostics (GOLD) for diagnostic operations across Cisco platforms running Cisco IOS Software.
- Troubleshooting tools — Provides troubleshooting workflows, Netshow and VRF-lite to troubleshoot the network connectivity, diagnose device problems, identify end host problems, and verify end-to-end connectivity of VRF configured devices.
What's New in Monitoring and Troubleshooting in LMS 4.1?

The following are the new features and enhancements in Monitoring and Troubleshooting:

- IPSLA Video Operation Support
- Smart Interactions in LMS
- Troubleshooting Workflow Changes

Note

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

IPSLA Video Operation Support

The platform-independent IPSLA software feature in Cisco IOS software is incapable of generating the high data rates, 4 to 16 Mbps, which are typical of video applications. To eliminate the protocol overhead and the process scheduling delays that contribute to the limitations of the earlier IPSLAs software to generate video traffic, the Cisco IPSLAs Video Operation feature makes the traffic generation and transmission routines platform dependent.

LMS IPSLA device management now supports new operation called Video and helps in analyzing the video traffic in the IP networks.

See Measuring Network Performance for Video for more details.

Smart Interactions in LMS

Smart Interactions in LMS provides the following services:

- TAC Service Request Tool to create online Cisco Technical Assistance Center (TAC) service requests for support issues covered under the terms of your Cisco support contracts.
- TAC Service Request Query Tool view the history and status of your existing or historical service requests and update the status of your open service requests.
- Access to Cisco Search Community forums that lists the links of the cisco forums and posts related to the key words of the device type.

See Getting Started with Cisco Prime LAN Management Solution 4.1 for more information.

Troubleshooting Workflow Changes

The following changes are made to Troubleshooting workflow in this release:

- Device Diagnostics and Network Connectivity workflows are renamed to Device Center and End Host Center, respectively.
- More quick links of Tasks, Tools, and Reports are added to Troubleshooting workflows and they are displayed in an alphabetical order.
• Launching Topology window is now optional. When you launch the workflow, the device tab is launched first for Device Center and the end host tab is launched first for End Host Center.

• You can now enter all universal format of MAC addresses when you troubleshoot a device using MAC addresses.

See Troubleshooting Network Devices and Endhosts for details of other changes and enhancements in troubleshooting workflow.

Key Acronyms, Terms, and Definitions

Table 1-1 provides a list of key acronyms and definitions used in this document.

<table>
<thead>
<tr>
<th>Acronym/Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active State</td>
<td>Indicates that LMS Monitoring is currently polling for the device.</td>
</tr>
<tr>
<td>Adapter</td>
<td>Program that links a Fault Management domain manager to its environment. Fault Management adapters forward inventory and event information to a domain manager for analysis. These adapters send the results of the analysis to other network management applications or other adapters.</td>
</tr>
<tr>
<td>Adhoc devices</td>
<td>External target devices that are added to manage IPSLA monitoring</td>
</tr>
<tr>
<td>Collector</td>
<td>Entity that encompasses a source router, a target device, an operation, and collector schedule details.</td>
</tr>
<tr>
<td>Collector groups</td>
<td>Allows you to associate a group of collectors. The collector groups are defined based on a set of criteria such as operation name, operation type, source address, target address.</td>
</tr>
<tr>
<td>Device Credentials Repository</td>
<td>Shared store of devices, their attributes and credentials accessible by LMS Device Management functions.</td>
</tr>
<tr>
<td>Embedded Event Manager (EEM)</td>
<td>Embedded Event Manager is an IOS technology that runs on the control plane of the Cisco Catalyst 6500 device. This EEM technology is integrated within Cisco IOS Software and because of this, the Cisco IOS Software EEM is aware of the state of the network from the perspective of view of the device on which it is operating.</td>
</tr>
<tr>
<td>Event</td>
<td>Indicator that is generated in LMS when a fault occurs on a network.</td>
</tr>
<tr>
<td>Generic Online Diagnostics (GOLD)</td>
<td>Device-specific IOS feature with fault detection capabilities. It defines a common framework for diagnostic operations across Cisco platforms running Cisco IOS Software.</td>
</tr>
<tr>
<td>Hierarchical maps</td>
<td>Topology views that display the devices listed under Topology Groups in a hierarchical way. Each map displays the selected group as a cloud of devices. If there are parent and sub-groups, the sub-group is displayed inside the corresponding parent group as a cloud icon.</td>
</tr>
<tr>
<td>hop count</td>
<td>Number of hops till which the network topology is drawn in N-Hop view portlet</td>
</tr>
<tr>
<td>ICMP Jitter</td>
<td>Allows you to generate a stream of ICMP packets between a Cisco IOS device (source) and any other IP device (destination) to gather network performance-related statistics.</td>
</tr>
<tr>
<td>Inactive State</td>
<td>Indicates that LMS Monitoring has stopped polling for the device.</td>
</tr>
</tbody>
</table>
## Key Acronyms, Terms, and Definitions

<table>
<thead>
<tr>
<th>Acronym/Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSLA Responder</td>
<td>Component embedded in a target Cisco device running version 12.1 or later of the Cisco IOS software. It responds to IPSLA request packets from a source device and provides accurate results.</td>
</tr>
<tr>
<td>Jitter</td>
<td>Inter-packet delay between any two consecutive data packets sent between the source and target router.</td>
</tr>
<tr>
<td>latency</td>
<td>Time taken for a packet to travel from the source to target and back. It is also referred to as RTT (Round-Trip Time).</td>
</tr>
<tr>
<td>link ports</td>
<td>Ports connected to Cisco devices (Switch or Router) are link ports.</td>
</tr>
<tr>
<td>NetShow</td>
<td>Commands that represent a set of read-only commands. They can either be run from the Graphical User Interface (GUI) or from the Command Line Interface (CLI).</td>
</tr>
<tr>
<td>non-link trunk ports</td>
<td>Trunk ports connected to End hosts or IP Phones.</td>
</tr>
<tr>
<td>Permanent</td>
<td>Status displayed if the polled MIB variables or instances are not available.</td>
</tr>
<tr>
<td>Poller</td>
<td>Collection of devices and template MIB instances.</td>
</tr>
<tr>
<td>Reachable</td>
<td>Device is available and reachable in the network.</td>
</tr>
<tr>
<td>Round Trip Time (RTT)</td>
<td>Time required for a network packet to travel from the source to the destination and back. RTT includes the time required for the destination to process the message from the source and generate a reply. The latency measurements taken by IPSLA Monitoring and SA Agent are round-trip time latency measurements.</td>
</tr>
<tr>
<td>source device</td>
<td>Devices which support IPSLA and which performs the operations by generating packets at the predefined intervals and storing the measured values.</td>
</tr>
<tr>
<td>source router</td>
<td>Originating router or switch running IOS from which IPSLA Monitoring measures network performance. The source router or switch must be running a version of Cisco IOS software version that supports IPSLA.</td>
</tr>
<tr>
<td>Template</td>
<td>Collection of MIB variables logically grouped by the user or system.</td>
</tr>
<tr>
<td>Threshold</td>
<td>An optimal value for a MIB variable set by the user or the system.</td>
</tr>
<tr>
<td>Traceroute</td>
<td>Device diagnostic tool used to detect routing errors between the management station and the target device</td>
</tr>
<tr>
<td>Transient</td>
<td>Status displayed if either the device is down or the SNMP credentials are incorrect.</td>
</tr>
<tr>
<td>Trap listener</td>
<td>LMS server port that listens to SNMP MAC Notification traps sent from devices.</td>
</tr>
<tr>
<td>TrendWatch</td>
<td>Allows you to continuously monitor MIB variable values over time. You can sample the value at periodic intervals to view the trends</td>
</tr>
<tr>
<td>UDP jitter</td>
<td>User Datagram Protocol jitter. It allows you to measure round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic.</td>
</tr>
<tr>
<td>VRF-Lite</td>
<td>Virtual Routing and Forwarding-Lite is one of the simplest form of implementing virtualization technology in an Enterprise network.</td>
</tr>
</tbody>
</table>
Chapter 2

Setting Up Monitoring Thresholds

Threshold is an optimal value set by you for a device or a group. Cisco Prime LMS compares this threshold rule with the polled data. If the threshold rule is violated consecutively, for the number of times specified, LMS generates an alert.

You can also configure LMS to send alert notifications as an e-mail, a trap or a syslog.

This section explains how to set up the monitoring thresholds and contains:

- Managing Fault Thresholds
- Setting Up Performance Thresholds
- TrendWatch Setup

Managing Fault Thresholds

You can manage thresholds for:

- All devices managed by LMS Monitoring
- LMS System Defined Groups
- Customizable Fault Groups (for devices)
- System Defined Fault groups, for example Access Port Groups, Interface Groups and Trunk Port Groups and their own sub groups.

This section describes how to configure and manage thresholds for device groups and contains the following topics:

- Viewing Thresholds
- Previewing Thresholds
- Editing Thresholds
- Restoring Factory Settings for Thresholds
- Threshold Categories for Devices, Interfaces, and Ports
- Threshold Definitions
- Threshold Parameter Values and Events
# Viewing Thresholds

You can view the thresholds that are associated with device groups, trunk port groups, access port groups, and interface groups.

Since there may be many ports and interfaces, you can use a link in the Threshold Parameter Summary to launch a separate page with all of the ports and interface members of the group. You can also save a comma separated value (CSV) version of the port or interface summary.

## Step 1
Select either one of the following from the menu:

- Monitor > Threshold Settings > Fault > Threshold Settings
- Monitor > Fault Settings > Setup > Threshold Settings

## Step 2
Select any device group from the group selector.

## Step 3
Click the View button.

The Thresholds Summary tabular display opens in a separate window and displays the following:

<table>
<thead>
<tr>
<th>Summary</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>IP address or DNS name of the device (device group summaries only).</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device function (device group summaries only).</td>
</tr>
</tbody>
</table>

## Threshold Parameters

<table>
<thead>
<tr>
<th>Category Name</th>
<th>Threshold category.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Whether threshold analysis is enabled (true) or disabled (false).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Threshold name.</td>
</tr>
<tr>
<td>Metric</td>
<td>Unit of measurement for parameter value:</td>
</tr>
<tr>
<td></td>
<td>• %—percent.</td>
</tr>
<tr>
<td></td>
<td>• count—number of occurrences.</td>
</tr>
<tr>
<td></td>
<td>• sec—number of seconds.</td>
</tr>
<tr>
<td></td>
<td>• C—centigrade.</td>
</tr>
<tr>
<td>Default</td>
<td>Factory setting for the parameter.</td>
</tr>
<tr>
<td>Current</td>
<td>Current value for the parameter.</td>
</tr>
<tr>
<td>Overriding Group</td>
<td>Group from which threshold parameter values are applied. (This is the highest priority group to which the element belongs.)</td>
</tr>
</tbody>
</table>

## Step 4
After viewing the threshold parameters, close the tabular display window.

You can export the data from tabular displays or print the tabular displays. See Reports Management with Cisco Prime LAN Management Solution 4.1 for more details.

For additional information, see the following topic:

- Viewing the Overriding Group—Examples
Previewing Thresholds

When you preview thresholds parameters, you can see the edited threshold parameters before you apply the changes.

**Note**
Preview is only supported for Device Type Groups.

**Step 1** Select either one of the following from the menu:
- Monitor > Threshold Settings > Fault > Threshold Settings
or
- Monitor > Fault Settings > Setup > Threshold Settings

**Step 2** Select any device type group from the group selector.

**Step 3** Click the Preview button.

The Thresholds Summary tabular display opens in a separate window and displays the following:

<table>
<thead>
<tr>
<th><strong>Summary</strong></th>
<th><strong>Explanation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Heading</strong></td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>IP address or DNS name of the device (device group summaries only).</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device function (device group summaries only).</td>
</tr>
<tr>
<td><strong>Threshold Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>Category Name</td>
<td>Threshold category.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether threshold analysis is enabled (true) or disabled (false).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Threshold name.</td>
</tr>
<tr>
<td>Metric</td>
<td>Unit of measurement for parameter value:</td>
</tr>
<tr>
<td></td>
<td>• %—percent.</td>
</tr>
<tr>
<td></td>
<td>• count—number of occurrences.</td>
</tr>
<tr>
<td></td>
<td>• sec—number of seconds.</td>
</tr>
<tr>
<td></td>
<td>• C—centigrade.</td>
</tr>
<tr>
<td>Default</td>
<td>Factory setting for the parameter.</td>
</tr>
<tr>
<td>Current</td>
<td>Current value for the parameter.</td>
</tr>
<tr>
<td>Overriding Group</td>
<td>Group from which threshold parameter values are applied. (This is the highest priority group to which the element belongs.)</td>
</tr>
</tbody>
</table>

**Step 4** After previewing the threshold parameters, close the tabular display window.

The Threshold Parameter Summary report displays the edited parameters for the selected device group. You can see the preview of the edited parameters based on the grouping of the devices in the selected device group.
Preview Threshold Parameter — Examples

The following example helps you to understand the preview of the displayed edited threshold parameters:

Let us consider the devices D1, D2, D3, and D4 belonging to the following four groups:

- Routers: D1 and D2
- Switches and Hubs: D2 and D3
- Customizable Group1: D1 and D3
- Customizable Group 2: D2 and D4

Let the Overriding Group order of the groups be:

- Customizable Group1
- Routers
- Switches and Hubs
- Customizable Group 2

Let the Relative voltage threshold parameter of the Environment Settings category for the groups be:

- Routers: 20
- Switches and Hubs: 30
- Customizable Group1: 40
- Customizable Group 2: 50
To edit the Relative voltage threshold parameter of a device group and to see the preview, do the following:

**Step 1** Select Routers which contains D1 and D2.

**Step 2** Edit the Relative voltage threshold parameter by changing it to 80.

**Step 3** Click the Preview button to see the edited parameters.

The Threshold Parameter Summary report for Routers (D1 and D2) is displayed.

The edited Relative voltage threshold parameter value 80 will be displayed only against the device D2. Although D2 belongs to the groups Routers, Switches and Hubs, and Customizable Group 2, Routers is the overriding group among them. Since D2 belongs to the overriding group Routers, the edited parameter 80 is displayed against D2.

D1 belongs to the groups Routers and Customizable Group1 where Customizable Group1 is the overriding group. So instead of the edited value 80, the value 40, which belongs to Customizable Group1 will be displayed against D1.

For more information on Overriding Groups, see Viewing the Overriding Group—Examples. To change the priority of the Device groups, see Setting Priorities.

Although the thresholds are saved in the database, they are not yet applied to the IP fabric. See Applying Polling and Threshold Changes.

### Editing Thresholds

When you edit thresholds, you edit values that are associated with groups, not with individual devices, ports, or interfaces. For ports and interfaces, you can activate or deactivate an entire group of threshold settings (for example, if you want to disable Reachability Settings for an entire interface group).

**Step 1** Select either one of the following from the menu:
- Monitor > Threshold Settings > Fault > Threshold Settings
- Monitor > Fault Settings > Setup > Threshold Settings

**Step 2** Select a data source.

The available data sources are:
- Device
- Device Groups
- Port Groups

**Step 3** Select a group for which you can set thresholds.
Step 4  Click Edit.

The Managing Thresholds: Edit page appears, displaying the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>The name of the device group selected. For example, /DeviceTypeGroup/LMS@humde-3250-2/System Defined Groups/Routers</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device function (not applicable to port or interface groups)</td>
</tr>
<tr>
<td>Threshold Category</td>
<td>Only those categories that are applicable to the members in the group are displayed.</td>
</tr>
</tbody>
</table>
| Parameter         | The parameters for the currently selected object and threshold category are displayed, including:  
|                   | • Current value for each threshold  
|                   | • An entry field for a new value.  
|                   | • Default check boxes that allow you to reset factory settings for all thresholds or for selected thresholds. |

Step 5  Edit the thresholds by selecting the threshold category and changing the thresholds appropriately:

- To reset factory settings for all thresholds in the category, select the Default check box in the table heading.
- To set values for individual thresholds for a group, enter data for each threshold.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Value</td>
<td>Enter a new value. This is optional.</td>
</tr>
</tbody>
</table>
| Default     | If you entered a new value, do not select Default check box.  
To reset thresholds to the factory settings, select this check box.  
The Default check box in the table heading can override this setting. |

- To activate or deactivate an entire group of threshold settings for interface and port groups select the Customize Settings button. For example, this can be Interface and Port Flapping settings for interface or port groups, or Reachability settings for device groups.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional Settings</td>
<td>Threshold settings groups that are not currently enabled.</td>
</tr>
<tr>
<td>Active Settings</td>
<td>Threshold settings groups that are currently enabled.</td>
</tr>
</tbody>
</table>

Use the Add or Remove button to select the settings group you want to enable or disable.
- To activate or deactivate all threshold settings, activate or deactivate the Disable All Threshold Settings for this Group check box.
Step 6  Save the thresholds by doing either one of the following:
  • Click Save to save the thresholds and display the Thresholds: Edit page again.
  • Click OK to save the thresholds and close the Thresholds: Edit page.

Step 7  Click Preview to see the edited threshold parameters before applying the changes.

Step 8  Apply the changes so that the changes come into effect. See Applying Polling and Threshold Changes.

The Threshold Parameter Summary report displays the edited parameters for the selected device group. You can see the preview of the edited parameters based on the grouping of the devices in the selected device group. For more information, see the Preview Threshold Parameter — Examples given in the Previewing Thresholds section.

Restoring Factory Settings for Thresholds

You can use this procedure to reset all thresholds for a device group, and you can reset all categories of thresholds to use factory settings.

Before You Begin

To review factory settings for thresholds before you apply them, view the thresholds for the device group. See Viewing Thresholds. Current values are displayed along with the factory settings.

Step 1  Select either one of the following from the menu:
  • Monitor > Threshold Settings > Fault > Threshold Settings
  or
  • Monitor > Fault Settings > Setup > Threshold Settings

Step 2  Select a device group for which you can set thresholds.

Step 3  Click the Factory Setting button. A confirmation dialog box appears.

Step 4  Click Yes.

Note  The settings are stored in the database, but not yet applied to the IP fabric. See Applying Polling and Threshold Changes.

For additional information, see the following topics:
  • Viewing Thresholds
  • Previewing Thresholds
  • Threshold Definitions
  • Threshold Parameter Values and Events
Threshold Categories for Devices, Interfaces, and Ports

Table 2-1 lists the threshold categories for each device group. For the parameters that you can set for each threshold category, see Threshold Definitions, or Threshold Parameter Values and Events.

Table 2-1  System-Defined Groups and Applicable Threshold Groups

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Rule</th>
<th>Threshold Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMS System Defined Groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadband Cable</td>
<td>Controlled by LMS Group</td>
<td>Reachability</td>
</tr>
<tr>
<td>Cisco Interfaces and Modules</td>
<td>Administration</td>
<td>Processor and Memory</td>
</tr>
<tr>
<td>Content Networking</td>
<td></td>
<td>Environment</td>
</tr>
<tr>
<td>DSL &amp;LREs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optical Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Fabric Switches</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switches and Hubs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Universal Gateways and Access Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice and Telephony</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Management</td>
<td></td>
<td>Reachability</td>
</tr>
</tbody>
</table>
### Table 2-1  System-Defined Groups and Applicable Threshold Groups (continued)

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Rule</th>
<th>Threshold Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Defined Fault Groups—Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 GB Ethernet</td>
<td>MaxSpeed = “1000000000” Type contains “ETHER” or “CSMACD”</td>
<td>Generic interface/port performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Backup interface support</td>
</tr>
<tr>
<td>10 GB Ethernet</td>
<td>MaxSpeed = “10000000000” Type contains “ETHER” or “CSMACD”</td>
<td>Dial-On-Demand interface support</td>
</tr>
<tr>
<td>10/100MB Ethernet</td>
<td>Type contains “ETHER” or “CSMACD”</td>
<td>Interface/port flapping</td>
</tr>
<tr>
<td>ATM</td>
<td>Type contains “ATM”</td>
<td></td>
</tr>
<tr>
<td>Token Ring</td>
<td>Type contains “TOKEN”</td>
<td></td>
</tr>
<tr>
<td>ISDN physical interface</td>
<td>InterfaceCode contains “ISDNDPHYSICAL”</td>
<td></td>
</tr>
<tr>
<td>ISDN B channel</td>
<td>InterfaceCode contains “ISDNBCHANNEL”</td>
<td></td>
</tr>
<tr>
<td>ISDN D channel</td>
<td>InterfaceCode contains “ISDNDCONNECT”</td>
<td></td>
</tr>
<tr>
<td>Serial</td>
<td>Type contains “Serial” or “FrameRelay”</td>
<td></td>
</tr>
<tr>
<td>FDDI</td>
<td>Type contains “FDDI”</td>
<td></td>
</tr>
<tr>
<td>Backup¹</td>
<td>Type contains “ISDN”</td>
<td></td>
</tr>
<tr>
<td>Dial-On-Demand¹</td>
<td>Type contains “PPP” or “SLIP”</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
Threshold Definitions

When you manage thresholds, you must select a device group and a threshold category. Threshold categories contain groups of parameters or thresholds that apply to that category. For the threshold parameters that you can set for each category, see Table 2-2.

For more information on Threshold Definitions, see:

- Backup Interface Support
- Dial-On-Demand Interface Support
- Environment
- Generic Interface/Port Performance
- Interface/Port Flapping
- Processor and Memory
- Reachability
Backup Interface Support

The Backup Interface Support threshold configures an interface as a backup. When an interface is identified as a backup:

- The InterfaceOperationallyDown event is not generated if the interface is down.
- The ExceededMaximumUptime event is generated if the interface stays up too long.

Maximum Uptime

The maximum length of time, in seconds, that the interface may be up before the ExceededMaximumUptime event is generated. If the value of this parameter is 0, the ExceededMaximumUptime event is disabled.

Dial-On-Demand Interface Support

The Dial-On-Demand Interface Support threshold identifies an interface as dial-on-demand. In this case:

- The InterfaceOperationallyDown event is not generated if the interface is down.
- The ExceededMaximumUptime event is generated if the interface stays up too long.

Maximum Uptime

The maximum length of time that the interface may be up before the ExceededMaximumUptime event is generated. If the value of this parameter is 0, the ExceededMaximumUptime event is disabled.

Environment

The Environment threshold controls the monitoring of the system environment.

Relative Temperature Threshold

Indicates how close the current temperature value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown temperature is 50°C and the Relative temperature threshold is 10%, the OutofRange event occurs if the temperature exceeds 45°C.

Relative Voltage Threshold

Indicates how close the current voltage value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown value is +30V and the Relative voltage threshold is 10%, the OutofRange event occurs if the voltage exceeds +27V.

Generic Interface/Port Performance

The Generic Interface/Port Performance thresholds configure the monitoring of a non-Ethernet network adapter’s performance characteristics. The categories include basic parameters—such as utilization, errors, broadcast, and packet drops—common to all media types.

Broadcast Threshold

The upper threshold for broadcast traffic, expressed as a percentage of the total bandwidth.
Managing Fault Thresholds

Collision Threshold

The upper threshold for collisions, expressed as a percentage of the total number of output packets. This threshold applies only to Ethernet settings for ports, trunks, and interfaces.

Discard Threshold

The upper threshold for dropped packets, expressed as a percentage of the total number of packets.

Error Threshold

The upper threshold for packet errors, expressed as a percentage of the total number of packets. LMS generates the HighErrorRate event when both the Error threshold and Error traffic threshold are reached or exceeded.

Error Traffic Threshold

The upper threshold for packet rate, expressed as a percentage of the total bandwidth. LMS generates the HighErrorRate event when both the Error threshold and Error traffic threshold are reached or exceeded. The value for Error traffic threshold can include up to two decimal places.

Queue Drop Threshold

The acceptable percentage of packets dropped because of full queues, expressed as a percentage of the total number of packets.

Utilization Threshold

The upper threshold for link utilization, expressed as a percentage of the total bandwidth.

LMS uses the DuplexMode special variable to specify duplexity (UNSPECIFIED, by default), and DuplexSource to track the duplexity setting source (NONE by default).

LMS uses the following algorithm to determine duplexity:

1. LMS checks the portDuplexity MIB attribute in the CISCO-STACK-MIB, and:
   - If the value is set to either half duplex or full duplex, LMS uses that setting for DuplexMode and sets DuplexSource to ENTERPRISE_MIB.
   - If the device is not a Cisco stack switch, the portDuplexity attribute is not present, or the portDuplexity attribute is present but its value is auto/disagree, LMS proceeds to Step 2.

2. LMS checks the dot3StatsDuplexStatus MIB attribute in the ETHERLIKE-MIB, and:
   - If the value is set to either half duplex or full duplex, LMS uses that setting for DuplexMode and sets DuplexSource to ETHERLIKE_MIB.
   - If the dot3StatsDuplexStatus attribute is not present, or it is present but its value is unknown, LMS proceeds to Step 3.
3. LMS checks the cdpCacheDuplex MIB attribute in the CISCO-CDP-MIB, and:
   - If the value is set to either half duplex or full duplex, LMS uses that setting for DuplexMode
     (for both local and remote ports), and sets DuplexSource to NEIGHBOR_MIB.
   - If the value is unknown, LMS proceeds to Step 4.
4. If LMS cannot correctly determine the duplex mode (because it was not set manually nor was it set
   in the MIB), LMS will set DuplexSource to ASSUMED and do the following:
   - If the interface is a 10-MB Ethernet interface, LMS will assume the setting is half duplex. (LMS
     considers an interface to be 10-MB Ethernet when its Type=’’*ETHER*’’ and its
     MaxSpeed=1000000.)
   - For all other interfaces, LMS will assume the setting is full duplex.

### Interface/Port Flapping

The Interface/Port Flapping thresholds control the analysis of network adapters (ports and interfaces)
that are continually going up and down, or flapping.

Flapping analysis monitors SNMP link down traps to identify a flapping network adapter. LMS reports
flapping as a fault condition. For more information, see How LMS Troubleshooting Calculates
Repeated Restarts and Flapping

#### Link Trap Threshold

The number of SNMP link down traps that must be received within the Link trap window for LMS to
consider the interface or port flapping. A value of 0 disables flapping analysis.

#### Link Trap Window

The amount of time used to monitor flapping analysis of a port or interface. If the number of link down
traps meets or exceeds the Link trap threshold during this window of time, the interface or port is
considered to be flapping.

### Processor and Memory

The Processor and Memory thresholds control the performance monitoring of a system's processor and
its associated memory elements.

#### Backplane Utilization Threshold

The upper threshold for a backplane utilization of a switch, expressed as a percentage of the total
backplane bandwidth.

#### Free Memory Threshold

The lower threshold for the acceptable amount of free memory, as measured by the ratio of free memory
to the total memory.

#### Memory Buffer Miss Threshold

The upper threshold for the number of buffer misses, expressed as a percentage of the total number of
buffer requests.
Memory Buffer Utilization Threshold

The upper threshold for the number of buffers used, expressed as a percentage of the total number of buffers.

Memory Fragmentation Threshold

The lower threshold for memory fragmentation. The fragmentation value is the ratio of the largest number of contiguous unallocated bytes to the total amount of free memory. For example, a value of 5 indicates that the largest free buffer must be at least 5% of the free memory.

Processor Utilization Threshold

The upper threshold for processor utilization, expressed as a percentage of the total capacity of the processor.

Reachability

The Reachability thresholds configure the reachability parameters for network adapters (ports and interfaces). They also control the analysis of systems that repeatedly restart, triggering Repeated Restarts and Flapping events. The following parameters are included in the Reachability Settings threshold category.

Restart Trap Threshold

The number of SNMP cold or warm start traps that must be received within the amount of time set by the Restart trap window parameter for LMS to consider a system to be performing excessive restarts. A value of 0 disables restart analysis. For more information, see How LMS Troubleshooting Calculates Repeated Restarts and Flapping

Note

If you want cold and warm start traps to generate events to be displayed immediately in the Alerts and Activities display, set the value of Restart trap threshold to 1.

Restart Trap Window

The amount of time used to monitor repeated restarts of a system. If the number of start traps meets or exceeds the Restart trap threshold during this window of time, the system is considered to be performing excessive restarts.

The minimum value is 30 seconds, and the maximum value is 3600 seconds.
Threshold Parameter Values and Events

Table 2-2 lists threshold categories, the threshold parameters in each category, minimum, maximum, and default values for the threshold parameters, and the events that LMS generates when values pass the threshold.

Most thresholds are upper thresholds, representing the highest acceptable value. Lower thresholds are the exception and are footnoted as such.

Note: The Utilization threshold is 65% for 10MB-100MB Ethernet sub-group of Trunk Port Groups.

<table>
<thead>
<tr>
<th>Threshold Category</th>
<th>Applicable Threshold Parameters (with unit of measure)</th>
<th>Values</th>
<th>Events Generated after Value Passes Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Interface Support</td>
<td>Maximum uptime (seconds)</td>
<td>0 86400 0</td>
<td>ExceededMaximumUptime</td>
</tr>
<tr>
<td>Dial-on-Demand</td>
<td>Maximum uptime (seconds)</td>
<td>0 86400 7200</td>
<td>ExceededMaximumUptime</td>
</tr>
<tr>
<td>Environment</td>
<td>Relative temperature threshold (%)</td>
<td>0 100 10</td>
<td>OutOfRange</td>
</tr>
<tr>
<td></td>
<td>Relative voltage threshold (%)</td>
<td>0 5 0</td>
<td>OutOfRange</td>
</tr>
<tr>
<td>Generic Interface/Port</td>
<td>Broadcast threshold (%)</td>
<td>0 100 15</td>
<td>HighBroadcastRate</td>
</tr>
<tr>
<td>Performance</td>
<td>Collision threshold (%)</td>
<td>0 100 10</td>
<td>HighCollisionRate</td>
</tr>
<tr>
<td></td>
<td>Discard threshold (%)</td>
<td>0 100 5</td>
<td>HighDiscardRate</td>
</tr>
<tr>
<td></td>
<td>Error threshold (%)</td>
<td>0 100 10</td>
<td>HighErrorRate</td>
</tr>
<tr>
<td></td>
<td>Error traffic threshold (%)</td>
<td>0 100 2.0</td>
<td>HighErrorRate</td>
</tr>
<tr>
<td></td>
<td>Queue drop threshold (%)</td>
<td>0 100 1</td>
<td>HighQueueDropRate</td>
</tr>
<tr>
<td></td>
<td>Utilization threshold (%)</td>
<td>0 100 40</td>
<td>HighUtilization</td>
</tr>
<tr>
<td>Interface/Port Flapping</td>
<td>Link trap threshold (count)</td>
<td>0 300 10</td>
<td>RepeatedRestarts</td>
</tr>
<tr>
<td></td>
<td>Link trap window (seconds)</td>
<td>30 3600 3</td>
<td>Flapping</td>
</tr>
<tr>
<td>Processor and Memory</td>
<td>Backplane utilization threshold (%)</td>
<td>0 100 80</td>
<td>InsufficientFreeMemory</td>
</tr>
<tr>
<td></td>
<td>Free memory threshold (%)</td>
<td>0 100 15</td>
<td>HighBackplaneUtilization</td>
</tr>
<tr>
<td></td>
<td>Memory buffer miss threshold (%)</td>
<td>0 100 10</td>
<td>HighBufferMissRate</td>
</tr>
<tr>
<td></td>
<td>Memory buffer utilization threshold (%)</td>
<td>0 100 90</td>
<td>HighBufferUtilization</td>
</tr>
<tr>
<td></td>
<td>Memory fragmentation threshold (%)</td>
<td>0 100 5</td>
<td>ExcessiveFragmentation</td>
</tr>
<tr>
<td>Reachability</td>
<td>Processor utilization threshold (%)</td>
<td>0 100 90</td>
<td>HighUtilization</td>
</tr>
<tr>
<td></td>
<td>Restart trap threshold (count)</td>
<td>0 10 3</td>
<td>RepeatedRestarts</td>
</tr>
<tr>
<td></td>
<td>Restart trap window (seconds)</td>
<td>30 3600 900</td>
<td>Flapping</td>
</tr>
</tbody>
</table>

1. Lower threshold—event is generated when the parameter value is lower than the value you set for it.
Setting Up Performance Thresholds

This section explains how to configure and manage thresholds for a MIB variable. It contains:

- Creating a Threshold
- Editing a Threshold
- Deleting a Threshold
- Filtering Thresholds
- Viewing Threshold Configuration Details

Threshold rule can be set for only one MIB variable at a time and you can set many thresholds for each MIB variable. You can set threshold rules for all the MIB variables on a device selected for polling.

Cisco Prime LMS compares this threshold rule with the polled data. If the threshold rule is violated for a consecutive number of times, LMS generates an alert. This condition is called threshold violation.

Cisco Prime LMS allows you to use user-defined external commands or scripts. These external commands or scripts are run whenever there is a threshold violation. Cisco Prime LMS does not track the results generated from the user-defined external commands or scripts.

You can also configure LMS to send alert notifications as an e-mail, a trap or a syslog.

From the Threshold Setup page, you can create a threshold for a MIB variable, modify the threshold set for a MIB variable and delete the threshold.

To access the Threshold Setup page, select Monitor > Threshold Settings > Performance from the menu. The List of Thresholds dialog box appears.

Table 2-3 describes the fields and buttons in the List of Thresholds dialog box.

<table>
<thead>
<tr>
<th>Field / Button Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold Name</td>
<td>Configured threshold. For example, CPU Threshold. Click on the Name hyperlink to view the details of the threshold created.</td>
</tr>
<tr>
<td>No. of Devices</td>
<td>Number of devices associated with the threshold.</td>
</tr>
<tr>
<td>Variable</td>
<td>MIB variable associated with the threshold. For example, cpmCPU-Tot5min-RV</td>
</tr>
<tr>
<td>Condition</td>
<td>Condition applied for monitoring threshold violation. For example, &gt;=</td>
</tr>
<tr>
<td>Value</td>
<td>Displays the threshold value.</td>
</tr>
<tr>
<td>Violation Count</td>
<td>Configured violation count. An alert is triggered if the specified violation count matches with the actual number of violations.</td>
</tr>
</tbody>
</table>
### Table 2-3 List of Thresholds Fields and Buttons (continued)

<table>
<thead>
<tr>
<th>Field / Button Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Severity level of the threshold violation. For example, Critical, Medium, Low. Severity is a user preference set based on the threshold requirement.</td>
</tr>
<tr>
<td>Script</td>
<td>Displays the user-defined external command or script.</td>
</tr>
<tr>
<td>E-Mail ID</td>
<td>E-mail address to which alert notifications are sent when threshold violation occurs.</td>
</tr>
<tr>
<td>Create (button)</td>
<td>Creates threshold for MIB variable. See Creating a Threshold.</td>
</tr>
<tr>
<td>Edit (button)</td>
<td>Modifies an existing threshold. See Editing a Threshold.</td>
</tr>
<tr>
<td>Delete (button)</td>
<td>Deletes an existing threshold. See Deleting a Threshold.</td>
</tr>
</tbody>
</table>
| Filter              | Select the filter criteria and enter the data. Use one of the following filter criteria and click Show:  
- Threshold Name  
- Variable Name  
- Severity  
- Violation Count  
See Filtering Thresholds. |

You can perform the following tasks from the List of Thresholds dialog box:

- Creating a Threshold
- Editing a Threshold
- Deleting a Threshold
- Filtering Thresholds
- Viewing Threshold Configuration Details
Creating a Threshold

You can set and monitor the optimal value for a MIB variable by defining threshold rules. This is done by selecting a template, choosing an appropriate MIB variable, selecting MIB variable instances and applying a threshold criteria. You can configure the threshold criteria based on your requirement.

To create a threshold:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Monitor &gt; Threshold Settings &gt; Performance from the menu. The List of Thresholds dialog box appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Create. The Threshold Configuration dialog box appears.</td>
</tr>
</tbody>
</table>

Table 2-4 describes the fields in the Threshold Configuration dialog box.

| Table 2-4 Threshold Configuration Fields |
| --- | --- |
| Field / Button | Description |
| Threshold Details | |
| Threshold Name | Enter a descriptive name for the threshold. The name must be unique. The name can contain a mix of alphabets, numerals, and some special characters (such as - _ . # @ $). |
| Template Name | Displays a list of System-defined and User-defined templates as a drop-down list. Select a template name from the drop-down list. For example, CPU Utilization. |
| Variable Name | Displays a list of MIB variables polled using the template as a drop-down list. Select a MIB variable from the drop-down list. For example, cpmCPUTotal5min. For Device Availability and Interface Availability, only the following MIB variables are listed: |
| | • sysUpTime (for Device Availability) |
| | • ifOperStatus (for Interface Availability) |
| Threshold Criteria | |
| Condition | Displays a list of conditions (such as >=, <=, >, <, ==, ! =). Select a condition for applying the threshold. The condition is applied to the value entered in the Value field. To set thresholds for device availability and interface availability, the condition must be specified as equals (==). |
Table 2-4  Threshold Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| Value         | Enter the threshold value. This value acts as a benchmark to monitor the MIB variable. You will be notified if the polled data violates the condition set (such as >=, <=, >, <, ==, !=) for the threshold value. If you have selected Device Availability template or Interface Availability template, then the following values are displayed in the Value drop-down list:  
  - Device Availability  
    - Sys Down  
    - Sys Up  
  - Interface Availability  
    - Down  
    - Up |
Setting Up Performance Thresholds

No. of Violations Enter a value to indicate the number of violations allowed before generating alerts. This can also be a fractional value. Based on the value entered, an alert is triggered if the threshold value is violated for consecutive polling cycles. If the threshold value is not violated during any one polling cycle, the No. of Violations count is reset to zero. The following example shows you what happens when the threshold violation alert is triggered and the value is reset.

Set the following Threshold Criteria to monitor the CPU Utilization:
- Condition: >=
- Value: 70%
- No. of Violations: 3

Case 1:
Assume that these are the CPU Utilization values:
- During first polling cycle — 72%
- During second polling cycle — 75%
- During third polling cycle — 74%

In this case, the threshold value is violated consecutively for three polling cycles. Hence, an alert is triggered when the threshold value is violated on the third polling cycle.

Case 2:
Assume that these are the CPU Utilization values:
- During first polling cycle — 72%
- During second polling cycle — 75%
- During third polling cycle — 68%

In this case, the threshold value is not violated consecutively for three polling cycles. Hence, the No. of Violation count is reset to zero.

Severity Select any of the following applicable severities from the drop-down list:
- Critical
- Medium
- Low

Severity is a user preference set based on the threshold requirement.
Table 2-4  Threshold Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| Execute Script | Select the Execute Script check box.  
Use the Browse button to select a user-defined external command or script. This external command or script is executed when threshold violation occurs.  
You are allowed to select user-defined external command or a script only from the following directory paths:  
- In Windows, $NMSROOT\hum\thresholdscript  
- In Solaris or Soft Appliance, $NMSROOT/hum/thresholdscript  
$NMSROOT is the default LMS installation directory. |

Notification Details

| Send E-Mail to | Enter the e-mail address to which LMS sends alert messages. The e-mail address must be in the format: user@domain.com.  
You can enter multiple e-mail addresses, separated by commas. |
| Send Trap to | Check the check box to send Traps to the Trap Receiver Group when a threshold violation occurs.  
Select the Trap Receiver Group from the drop-down list.  
LMS uses CISCO-EPM-NOTIFICATION-MIB trap message format to generate SNMP traps when an alert occurs. For more information, see Notification MIB.  
This field is optional. |
| Send Syslog to | Check this check box to send Syslog information to Syslog Receiver Group when a threshold violation occurs.  
Select the Syslog Receiver Group from the drop-down list.  
This field is optional. |
| Severity | Select any of the following applicable severities for the Syslog information, from the drop down list:  
- Emergency: Signifies that the system is unusable.  
- Alert: Signifies that an action must be taken immediately.  
- Critical: Signifies that the condition is critical.  
- Error: Signifies an error condition.  
- Warning: Signifies warning conditions.  
- Notice: Signifies that there is a normal but important condition.  
- Informational: Signifies information messages.  
- Debug: Signifies debug-level messages. |

Select Instances or Groups

| Instance Selector | Select one or more instances from the Instances listed in the tree.  
You can do basic and advanced search of instances in the Instance selector. |
| Port Group Selector | Select the desired port groups from the group selector. |
## Setting Up Performance Thresholds

### Step 3
Go to the Threshold Details pane.

### Step 4
Enter a descriptive name for the Threshold. For example, CPU Threshold.

### Step 5
Select a template from the drop-down list.

- The drop-down list shows a list of all the System-defined and User-defined templates.
- If you have selected Port Groups, only the interface-related templates will be displayed.

### Step 6
Select a MIB variable from the drop-down list.

- The drop-down list shows a list of MIB variables polled using the selected template. For example, `cpmCPUTotal5minRev`.
- The selected MIB variable displays all the polled device instances in the Instance Selector pane.

### Step 7
Select one of the following radio buttons:
- Instance Selector
- Port Group Selector
- Device Group Selector

- If you have selected Instance Selector, select the required instances from the instance tree.
- If you have selected Port Group Selector, select the required port groups.
- If you have selected Device Group Selector, select the required device groups.

### Step 8
Go to the Threshold Criteria pane.

### Step 9
Select a condition from the drop-down list.

- The condition is set based on the threshold value entered in the Value field.
- To know the device availability and interface availability, you must select the condition as equals (==).
Step 10 Enter the threshold value in the Value field.
If you have selected the template name as Device Availability or Interface Availability, then the following values are displayed in the Value drop-down list:
- For Device Availability
  - Sys Down
  - Sys Up
- For Interface Availability
  - Down
  - Up

Step 11 Enter a value in the No. of Violations field.
This value indicates the number of violations permitted during consecutive polling cycles. Based on the value entered, an alert is triggered if the threshold value is violated for consecutive polling cycles. If the threshold value is not violated during any one polling cycle, the No. of Violations count is reset to zero.

Step 12 Select a severity from the Severity drop-down list. For example, Critical, Medium or Low.

Step 13 Click Browse.
The Server Side File Browser dialog box appears, prompting you to locate the external command or script from the directory path where LMS is installed.
You are allowed to select an external command or script only from the following directory paths:
- In Windows, $NMSROOT\hum\thresholdscript
- In Solaris or Soft Appliance, $NMSROOT/hum/thresholdscript
$NMSROOT is the default LMS Installation directory. If you try to access any other directory path, an appropriate error message is displayed.
Table 2-5 describes the fields in the Server Side File Browser dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>Displays the directory path to locate the external command or script.</td>
</tr>
<tr>
<td>Directory Content</td>
<td>Displays the files and folders within the directory path.</td>
</tr>
</tbody>
</table>

Step 14 Locate the external command or script and click OK.
The script should be of an extension .bat for Windows and .sh for Solaris or Soft Appliance, and should have proper executable permissions.
LMS executes the script when threshold violation occurs.
The following environmental variables are passed to the script:
- Threshold Name—Name of the threshold set for a MIB variable.
  Environmental variable key passed to the script: ThresholdName.
- Device Name—Name of the device for which the threshold violation occurred.
  Environmental variable key passed to the script: DeviceName.
Chapter 2  Setting Up Monitoring Thresholds

Setting Up Performance Thresholds

- MIB Variable Name—Name of the MIB variable which violated the threshold.
  Environmental variable key passed to the script: MibVarName.
- Instance Name—Name of the device instance for which the threshold violation occurred.
  For example, CPU of Switching Processor. Environmental variable key passed to the script: InstanceName.
- Configured Value—Value set for monitoring threshold violation.
  Environmental variable key passed to the script: ConfiguredValue.
- Breach Value—Actual value of threshold violation.
  Environmental variable key passed to the script: BreachValue.
- Number of Violations—Number of consecutive threshold violations occurred.
  Environmental variable key passed to the script: NoOfOccurrences.
- Severity—Severity of the threshold such as Critical, Medium, Low.
  Environmental variable key passed to the script: Severity.
- Date and Time—Date and time at which the threshold violation occurred.
  Environmental variable key passed to the script: TimeOfOccurance.

LMS does not track the results generated from the user-defined external command or script.

**Step 15**
Select the Notify Me check box and enter the e-mail address in the E-mail ID field to receive E-mail notifications of threshold violation.

The E-mail address must be in the format: user@domain.com.

The E-mail ID field supports multiple e-mail addresses, separated by commas.

**Step 16**
Select the Send Trap check box to send Trap information when any threshold violation has occurred.

**Step 17**
Select the Trap Receiver Group from the drop-down list.

**Step 18**
Select the Send Syslog check box to send Syslog information to Syslog Receiver Group when any threshold violation has occurred.

**Step 19**
Select the Syslog Receiver Group from the drop-down list.

**Step 20**
Click Create to add the threshold.

A message appears, confirming that threshold is added successfully.

**Step 21**
Click OK.

The Threshold Configuration dialog box appears, allowing you to create more thresholds.

Or

Click Cancel to cancel the threshold creation process.

The created threshold is listed in the List of Thresholds dialog box.
## Editing a Threshold

You can modify the threshold criteria of an existing threshold using the Edit button. You can only make changes to the threshold criteria and the selection of instances. You cannot make changes to the threshold details (Threshold Name, Template Name, Variable Name).

You can edit only one threshold at a time. If you select multiple thresholds using the check box, the Edit button is disabled.

To edit a threshold:

**Step 1** Select **Monitor > Threshold Settings > Performance** from the menu.

The List of Thresholds dialog box appears.

**Step 2** Select the threshold by checking the corresponding check box.

If you select multiple thresholds, the Edit button is disabled.

**Step 3** Click **Edit**.

The Threshold Configuration dialog box appears.

See [Creating a Threshold](#) for the description of the fields that appear in the Threshold Configuration dialog box.

You cannot select a different data source while editing thresholds. However, you can modify the same data source.

For example, if you have selected Instance Selector while creating thresholds, you can add or delete instances. You cannot select other data sources from Device Group Selector or Port Group Selector.

**Step 4** Make the necessary changes to the Select Instances and Threshold Criteria panes.

**Step 5** Click **Update**.

A message appears, confirming that the threshold is updated successfully.

The updated threshold is listed in the List of Thresholds dialog box.

## Deleting a Threshold

LMS allows you to delete thresholds using the Delete button. You are allowed to delete only one threshold at a time.

Before a threshold is deleted, you are prompted to confirm the deletion because you cannot restore a threshold that you have deleted from the database.

To delete a threshold:

**Step 1** Select **Monitor > Threshold Settings > Performance** from the menu.

The List of Thresholds dialog box appears.

**Step 2** Select the threshold by checking the corresponding check box.
Step 3 Click **Delete**.
A message appears, prompting you to confirm the deletion.

Step 4 Click **OK** to delete the threshold or **Cancel** to cancel the operation.
If you choose to click **OK**, a message appears that the threshold is deleted successfully.
The List of Thresholds dialog box appears.

**Filtering Thresholds**

This section describes how you can use the filter option to display the threshold information based on a specific criteria.

To filter threshold information:

Step 1 Select **Monitor > Threshold Settings > Performance** from the menu.
The List of Thresholds dialog box appears.

Step 2 Select a criteria for filtering from the drop-down list.

Step 3 Enter the data to be filtered in the text field.

Table 2-10 describes the methods you can follow to filter the data.

Step 4 Click **Show**.
The List of Thresholds dialog box appears, displaying the threshold information based on the filter criteria.
Table 2-10 describes the criteria available to filter.

<table>
<thead>
<tr>
<th>Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold Name</td>
<td>Select <strong>Threshold Name</strong> and enter the data. You can use any of the following methods to filter by entering:</td>
</tr>
<tr>
<td></td>
<td>• Complete threshold name</td>
</tr>
<tr>
<td></td>
<td>• Any three consecutive characters of the threshold name</td>
</tr>
<tr>
<td></td>
<td>• Any wildcard characters of the threshold name (such as <em>a, a</em>, <em>a</em>)</td>
</tr>
<tr>
<td>Variable Name</td>
<td>Select <strong>Variable Name</strong> and enter the data. You can use any of the following methods to filter by entering:</td>
</tr>
<tr>
<td></td>
<td>• Complete MIB variable name</td>
</tr>
<tr>
<td></td>
<td>• Any three consecutive characters of the MIB variable name</td>
</tr>
<tr>
<td>Severity</td>
<td>Select <strong>Severity</strong> and enter the severity as Critical, Medium, or Low.</td>
</tr>
<tr>
<td>Violation Count</td>
<td>Select <strong>Violation Count</strong> and enter the violation count numeric value.</td>
</tr>
</tbody>
</table>
Viewing Threshold Configuration Details

You can view the threshold configuration details listed for each device, in a tabular format.

To view a threshold configuration:

**Step 1**
Select **Monitor > Threshold Settings > Performance** from the menu.
The List of Thresholds dialog box appears.

**Step 2**
Click on the threshold name link.
The Threshold View page appears, displaying the threshold configuration details.

Table 2-7 describes the fields in the Threshold View page.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instances</td>
<td>Displays the list of instances selected for the device.</td>
</tr>
<tr>
<td>Go to Device</td>
<td>Select a device name from the drop-down list. The threshold configuration</td>
</tr>
<tr>
<td></td>
<td>details for the selected device is displayed.</td>
</tr>
<tr>
<td>Export</td>
<td>Click the Export icon to export threshold configuration details to a file of</td>
</tr>
<tr>
<td></td>
<td>CSV or PDF format.</td>
</tr>
<tr>
<td>Print</td>
<td>View the threshold configuration details in a printer-friendly format.</td>
</tr>
</tbody>
</table>

TrendWatch Setup

This section explains how to configure and manage a TrendWatch for a MIB variable.

This section also explains:

- Creating a TrendWatch
- Editing a TrendWatch
- Deleting a TrendWatch
- Deactivating a TrendWatch
- Activating a TrendWatch
- Copying a TrendWatch
- Filtering TrendWatch

The TrendWatch feature ensures that the capacity, performance, and utilization of critical resource remains within the defined service level.

You can configure TrendWatch through LMS, by setting up rules for each MIB-variable or thresholds for a specific time period. TrendWatch will be scheduled (Immediate, Once, Daily, Weekly, and Monthly) as a job. You can configure it to send alert notifications through e-mail, trap or Syslog.
TrendWatch allows you to continuously monitor a value over time, sampling the value at periodic intervals to view the trends. You can watch variable trends in days, weeks, months and years. You can identify trends that develop over time and take appropriate actions.

TrendWatch does not monitor real-time data. It is calculated on past or historical data.

You can create TrendWatch reports either for thresholds that are changed or for devices from the Report Management page. For Threshold-based TrendWatches, all the instances selected in the threshold, apply to a particular TrendWatch.

The TrendWatch rule can be set for only one MIB variable at a time and you can set many TrendWatches for each MIB variable. You can set TrendWatch rules for all MIB variables on a device that is selected for polling.

LMS compares the TrendWatch rule with the polled data. If the TrendWatch rule is violated, LMS generates an alert. This condition is called TrendWatch violation.

You can create a TrendWatch for a MIB variable, based on a template or on a threshold. The TrendWatch Setup page allows you to create, modify, or delete a TrendWatch.

To access the TrendWatch Setup page, select Monitor > Threshold Settings > TrendWatch. The List of TrendWatches page appears.
Table 2-8 describes the fields and buttons in the List of TrendWatches page.

### Table 2-8  List of TrendWatch Fields and Buttons

<table>
<thead>
<tr>
<th>Field / Button Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrendWatch Name</td>
<td>Displays the TrendWatch name. For example, CPU TrendWatch. Click on the Name hyperlink to view the details of the TrendWatch created.</td>
</tr>
<tr>
<td>No. of Devices</td>
<td>Number of devices associated with the TrendWatch.</td>
</tr>
</tbody>
</table>
| Status              | Status of a TrendWatch. The following TrendWatch status is displayed:  
  • Active—LMS is currently querying for device instances.  
  • Inactive—LMS has stopped querying for device instances. |
| Variable            | MIB variable associated with the TrendWatch. For example, `cpmCPUMTotal5minRev` |
| Severity            | Severity level of the TrendWatch violation. For example, Critical, Medium, Low  
  Severity is a user preference set based on the TrendWatch requirement. |
| E-Mail ID           | E-mail address to which alert notifications are sent when TrendWatch violation occurs. |
| Create (button)     | Creates a TrendWatch. See Creating a TrendWatch. |
| Edit (button)       | Modifies an existing TrendWatch. See Editing a TrendWatch. |
| Delete (button)     | Deletes an existing TrendWatch. See Deleting a TrendWatch. |
| Activate (button)   | Activates an inactive TrendWatch to monitor device instances. See Activating a TrendWatch. |
| De-activate (button)| Stops a TrendWatch from monitoring device instances. See Deactivating a TrendWatch. |
| Copy (button)       | Creates a TrendWatch from an existing TrendWatch. See Copying a TrendWatch. |
| Filter              | Select the filter criteria and enter the data.  
  Use one of the following filter criteria and click Show:  
  • TrendWatch Name  
  • Variable Name  
  • Severity  
  See Filtering TrendWatch. |
| Show (button)       | Shows the Trend Watches based on filter criteria |
You can perform the following tasks from the List of TrendWatches page:

- Creating a TrendWatch
- Editing a TrendWatch
- Deleting a TrendWatch
- Deactivating a TrendWatch
- Activating a TrendWatch
- Copying a TrendWatch
- Filtering TrendWatch

Creating a TrendWatch

You can configure a TrendWatch for a MIB variable by defining rules, so that you can monitor the trend for a given period of time and keep the values within the defined service level.

You can configure the TrendWatch criteria based on your requirement. You can create TrendWatches based on:

- Templates
- Thresholds

This section contains:

- Creating a TrendWatch Based on Templates
- Creating a TrendWatch Based on Threshold

Creating a TrendWatch Based on Templates

You can create TrendWatch rules on a MIB variable to monitor the devices for TrendWatches. Some examples of TrendWatch rules are:

- When the average weekly CPU or interface utilization goes up or down relative to previous week by \( n \)%.
- When the device or interface availability over a period is less than \( n \)%.
- When the average utilization of the interface is above \( n \)%.
- When the availability was down for \( N \) minutes, more than \( X \) times in a week/month/quarter
- When the minimum value is less than \( N \) for \( X \) times over a period of \( Y \) weeks
- When \( n \) percentage of times the utilization is greater than \( x \) percentage.
To create a TrendWatch based on template:

**Step 1** Select **Monitor > Threshold Settings > TrendWatch** from the menu.

The List of TrendWatches page appears.

**Step 2** Click **Create**.

The TrendWatch Configuration dialog box appears.

Table 2-9 describes the fields in the TrendWatch Configuration dialog box.

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TrendWatch Details</strong></td>
<td></td>
</tr>
</tbody>
</table>
| TrendWatch Name      | Enter a descriptive name for the TrendWatch. The name must be unique. It should not be the same as any existing report name. The name can contain a mix of alphabets, numerals, and some special characters (such as - _ .).
| Based on             | Select either **Template** or **Threshold** to configure TrendWatch depending on your requirement. Based on your selection either a list of templates or thresholds configured is listed. The Template Name, Variable Name, and TrendWatch Conditions will be disabled if you select the Threshold-based TrendWatch. The condition, value and instances will be obtained from the threshold definition. |
| Template Name        | Displays a list of System-defined and User-defined templates that are being polled by the historic pollers, as a drop-down list. Select a template name from the drop-down list. For example, CPU Utilization. This field is disabled if you have selected **Threshold** to configure Threshold based TrendWatch. If you have selected Port Group selector, the interface related templates will be listed. |
| Variable Name        | Displays a list of MIB variables being polled using the template, as a drop-down list. Select a MIB variable from the drop-down list. For example, \textit{cpmCPUTotal5min}. For Device Availability and Interface Availability, only the following MIB variables are listed: \begin{itemize} \item sysUpTime (for Device Availability) \item ifOperStatus (for Interface Availability) \end{itemize} This field is disabled if you have selected **Threshold** to configure Threshold based TrendWatch. |
### TrendWatch Setup

#### Select Severity
Select any of the following applicable severities from the drop-down list:
- Critical
- Medium
- Low

Severity is set based on your TrendWatch requirement.

If you have selected **Threshold** to configure Threshold based TrendWatch, then the Threshold severity will be listed in the drop-down list.

### Select Instances or Groups

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Selector</td>
<td>Select one or more instances from the Instances listed in the tree. You can do basic and advanced search of devices in the Instance selector.</td>
</tr>
<tr>
<td>Port Group Selector</td>
<td>Select the desired port groups from the group selector.</td>
</tr>
<tr>
<td>Device Group Selector</td>
<td>Select the desired device groups from the group selector.</td>
</tr>
</tbody>
</table>

#### Instance Selector

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Input</td>
<td>Enter your search expression in this field. You can enter only instance name and not device name for the search input.</td>
</tr>
<tr>
<td>All</td>
<td>Click All to view all the device instances for the selected MIB variable. Check the check boxes to select the instances.</td>
</tr>
<tr>
<td>Search Results</td>
<td>Displays all your Simple or Advanced search results. You can select all instances, clear all instances, or select a few instances from this list. Advanced search is applicable only if you select to create TrendWatch based on templates.</td>
</tr>
<tr>
<td>Selection</td>
<td>Lists all the instances that you have selected in the All or Search Results tab or a combination of both. You can also use the instance tree to deselect the instances you have already selected. The Select Instance tree will list only the devices being polled for the MIB variable selected in the Variable Name drop-down list. This field is disabled if you have selected <strong>Threshold</strong> to configure Threshold based TrendWatch.</td>
</tr>
<tr>
<td>Condition</td>
<td>Displays a list of conditions (such as &gt;=, &lt;=, &gt;, &lt;, ==, !=, Relatively Up, Relatively Down). Select a condition for applying the TrendWatch. The default is None. The condition is applied to the value entered in the Value field. This field is disabled if you have selected <strong>Threshold</strong> to configure Threshold based TrendWatch.</td>
</tr>
</tbody>
</table>

### Table 2-9 TrendWatch Configuration Fields (continued)
### TrendWatch Setup

**Value**

Enter the TrendWatch value. This value acts as a benchmark to monitor the MIB variable. You will be notified if the polled data violates the condition set (such as >=, <=, >, <, ==, !=, Relatively Up, Relatively Down) for the TrendWatch value.

This field is disabled if you have selected **Threshold** to configure Threshold based TrendWatch.

### TrendWatch Conditions

**Group By**

Displays a list of Group By types (such as Hourly, Daily, Weekly, Monthly and Quarterly) to perform TrendWatch.

Select any one of the following Group By types

- None—Displayed by default.
- Hourly—Monitors the MIB variable based on the condition on an hourly basis.
- Daily—Monitors the MIB variable based on the condition on a daily basis.
- Weekly—Monitors the MIB variable based on the condition on a weekly basis.
- Monthly—Monitors the MIB variable based on the condition on a monthly basis.
- Quarterly—Monitors the MIB variable based on the condition on a quarterly basis.
- Yearly—Monitors the MIB variable based on the condition on a yearly basis.

This field is disabled if you have selected **Threshold** to configure Threshold based TrendWatch.

---

**Table 2-9  TrendWatch Configuration Fields (continued)**

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Enter the TrendWatch value. This value acts as a benchmark to monitor the MIB variable. You will be notified if the polled data violates the condition set (such as &gt;=, &lt;=, &gt;, &lt;, ==, !=, Relatively Up, Relatively Down) for the TrendWatch value. This field is disabled if you have selected <strong>Threshold</strong> to configure Threshold based TrendWatch.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group By</th>
<th>Displays a list of Group By types (such as Hourly, Daily, Weekly, Monthly and Quarterly) to perform TrendWatch. Select any one of the following Group By types</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Displayed by default.</td>
</tr>
<tr>
<td>Hourly</td>
<td>Monitors the MIB variable based on the condition on an hourly basis.</td>
</tr>
<tr>
<td>Daily</td>
<td>Monitors the MIB variable based on the condition on a daily basis.</td>
</tr>
<tr>
<td>Weekly</td>
<td>Monitors the MIB variable based on the condition on a weekly basis.</td>
</tr>
<tr>
<td>Monthly</td>
<td>Monitors the MIB variable based on the condition on a monthly basis.</td>
</tr>
<tr>
<td>Quarterly</td>
<td>Monitors the MIB variable based on the condition on a quarterly basis.</td>
</tr>
<tr>
<td>Yearly</td>
<td>Monitors the MIB variable based on the condition on a yearly basis.</td>
</tr>
</tbody>
</table>

This field is disabled if you have selected **Threshold** to configure Threshold based TrendWatch.
### TrendWatch Setup

**Aggregate**
- Displays a list of values (such as Min, Max, Avg, Std Deviation). Select a value to evaluate the variable for a condition.
- Select any one of the following Aggregate types
  - None—Displayed by default.
  - Average—Average of polled value. For example, average value per hour.
  - Minimum—Minimum of polled value. For example, minimum value per hour.
  - Maximum—Maximum of polled value. For example, maximum value per hour.
  - Std Deviation—Standard deviation of polled value. For example, standard deviation of the values per hour.

If you have selected Device Availability template or Interface Availability template, then only Average will be listed in the drop down list and it will be selected by default.

This field is disabled if you have selected **Threshold** to configure Threshold based TrendWatch.

**Trend**

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Occurred</td>
<td>Specify how many times the TrendWatch violation has occurred. Enter a value in the text field, select either <strong>At least</strong>, <strong>Exactly</strong>, or <strong>Almost</strong> from the drop-down list, and select a time frame of your trend watch. Select the time frame as <strong>Times</strong> or <strong>Percentage of Times</strong> from the drop-down list.</td>
</tr>
<tr>
<td>Last</td>
<td>Click the Last radio button to monitor whether the trend has occurred in the last n days or weeks, or months, or years. Enter a value in the text field and select a time frame for the TrendWatch.</td>
</tr>
</tbody>
</table>
  - Days—Specify the trend occurrence date interval
  - Weeks—Specify the trend occurrence Week interval
  - Months—Specify the trend occurrence Month interval
  - Years—Specify the trend occurrence Years interval
  For example, 5 Days, 2 Weeks, 3 Months, 1Year
  This field is disabled if you have selected the **From** radio button.
| From           | Click the From radio button to generate whether the trend has occurred in the specified date and time. Specify the start date and time that the TrendWatch condition has occurred. Select the date by clicking it in the Calendar icon; select the time from the drop-down list. The From date must be earlier than the current date. |
**TrendWatch Configuration Fields (continued)**

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To</strong></td>
<td>Specify the end date and time that the TrendWatch condition has occurred. Select the date by clicking it in the Calendar icon; select the time from the drop-down list. The To date must be later than the From date and earlier than the current date.</td>
</tr>
<tr>
<td><strong>Show Rule</strong></td>
<td>Click <strong>Show Rule</strong> to view the created TrendWatch rule. The created TrendWatch rule is displayed in the message box.</td>
</tr>
<tr>
<td><strong>Notify Details</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Send Email to</strong></td>
<td>Check this check box for notification through e-mail. The e-mail will contain all the TrendWatch job details. In case of any violations, violation details will be added to the TrendWatch details. Enter the e-mail address to which LMS sends alert messages. The e-mail address must be in the format: <em><a href="mailto:user@domain.com">user@domain.com</a></em>. You can enter multiple e-mail addresses, separated by commas. This field is optional.</td>
</tr>
<tr>
<td><strong>Attach Report</strong></td>
<td>Check this check box to attach a CSV report to the e-mail. By default, a CSV file is sent as an attachment to the e-mail ID specified. If you check Add Full Report check box, instead of CSV, a PDF format of the report will be sent as an attachment to the specified e-mail id. You need to enable the E-mail Attachment check box and specify the Maximum Attachment size in the System Preferences dialog box (<em>Admin &gt; System &gt; System Preferences</em>) to send the report as an E-mail. If the file size exceeds the Maximum Attachment size, the URL link of the report is sent as an e-mail. You can click the URL link to view the report.</td>
</tr>
<tr>
<td><strong>Send Trap to</strong></td>
<td>Check this check box to send Traps to the Trap Receiver Group when any TrendWatch violation has occurred. Select the Trap Receiver Group from the drop-down list. LMS uses CISCO-EPM-NOTIFICATION-MIB trap message format to generate SNMP traps when an alert occurs. For more information, see Notification MIB. This field is optional.</td>
</tr>
<tr>
<td><strong>Send Syslog to</strong></td>
<td>Check this check box to send Syslog information to Syslog Receiver Group when any TrendWatch violation has occurred. Select the Syslog Receiver Group from the drop-down list. This field is optional.</td>
</tr>
</tbody>
</table>
### TrendWatch Setup

#### TrendWatch Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| Severity       | Select any of the following applicable severities for the Syslog information, from the drop down list:  
   - Emergency: Signifies that the system is unusable.  
   - Alert: Signifies that an action must be taken immediately.  
   - Critical: Signifies that the condition is critical.  
   - Error: Signifies an error condition.  
   - Warning: Signifies warning conditions.  
   - Notice: Signifies that there is a normal but important condition.  
   - Informational: Signifies information messages.  
   - Debug: Signifies debug-level messages. |

#### Schedule Details

| Schedule Type | You can choose the Run status by selecting schedule type. Based on the selection the report will run periodically or immediately. Select one of the following Schedule Types from the drop-down list:  
   - Immediate—TrendWatch is run immediately.  
   - Once—TrendWatch is run only once for the set date and time.  
   - Daily—TrendWatch is run daily at the scheduled time.  
   - Weekly—TrendWatch is run weekly for the set date and time.  
   - Monthly—TrendWatch is run monthly for the set date and time.  
Start At | Specify the date and time that the TrendWatch is scheduled for. The time should be later than the current time. This field is disabled if you have selected **Immediate** as the Schedule Type. |

#### Report Information

| Report Publish Path | Browse and select the path to publish your report. |
Chapter 2  Setting Up Monitoring Thresholds

TrendWatch Setup

Table 2-9  TrendWatch Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Full Report</td>
<td>Use the Add Full Report check box to create a PDF format of the report for all devices. If you check this check box along with Attach Report check box, a PDF format of the report will be sent as an attachment to the specified e-mail ID. If the file size exceeds the Maximum Attachment size, then a CSV file will only be sent as an attachment along with the URL link of the HTML report. You can download the PDF format of the report using the export option provided in the HTML report. The PDF format of the report takes longer time to generate as it includes the report for all the polled devices. Inventory &gt; Device Administration &gt; Add as Managed Devices. Scheduling PDF reports with large number of data on a daily basis results high CPU and memory usage. We recommend you to schedule PDF reports with less number of data at optimal time intervals.</td>
</tr>
<tr>
<td>Create (button)</td>
<td>Creates the TrendWatch and resets the fields in the TrendWatch Configuration dialog box to add a new TrendWatch.</td>
</tr>
<tr>
<td>Cancel (button)</td>
<td>Cancels the creation of TrendWatch.</td>
</tr>
</tbody>
</table>

Step 3  Go to the TrendWatch Details pane and enter a descriptive name for the TrendWatch. For example, CPU Threshold.

Step 4  Select Template from the Based On radio button to configure TrendWatch based on the template.

Step 5  Select a template from the Template Name drop-down list. The drop-down list shows all the System-defined and User-defined templates.

Step 6  Select a MIB variable from the Variable Name drop-down list. The drop-down list shows all the MIB variables associated with that template. For example, `cpmCPUTotal5minRev`. Based on the selected MIB variable, all the polled device instances are listed in the Select Instances pane.

Step 7  Select a severity from the Severity drop-down list. For example, Critical, Medium or Low.

Step 8  Select one of the following radio buttons:
- Instance Selector
- Port Group Selector
- Device Group Selector
If you have selected Instance Selector, select the required instances from the instance tree.
If you have selected Port Group Selector, select the required port groups.
If you have selected Device Group Selector, select the required device groups.
Step 9  Go to the TrendWatch Conditions pane.  
Here you can define the TrendWatch condition.  
For example you can find out whether the TrendWatch violation occurrence for the CPU Utilization, has a daily average that is greater than 50% and it occurs at least 10% of times. This means, if the device is polled for 100 times and there are 10 violation, it is 10% of times.

Step 10  Select Group By Value from the Group By drop-down list.  
For example Hourly, Daily, Monthly, Quarterly, and Yearly.  
The condition is set based on the TrendWatch value entered in the Value field.

Step 11  Select the Aggregate value from the Aggregate drop-down list.  
If you have selected the template name as Device Availability or Interface Availability, then only Average will be listed in the drop down list and it will be selected by default.

Step 12  Select a condition from the Condition drop-down list.  
The condition is set based on the TrendWatch value entered in the Value field.  
For example, the hourly average of CPU Utilization is relatively up by 50%. This means that if the value for the current hourly average is 75% and the value for the last hourly average was 50%, then the hourly average of CPU Utilization has gone relatively up by 50%.

Step 13  Enter the TrendWatch value in the Value field.

Step 14  Go to the Trend pane and select At least, Exactly, or Atmost from the drop-down list.

Step 15  Enter the value in the text box and select the number of times or the percentage of times that the trend has occurred, from the drop-down list.

Step 16  Select Times or Percentage of Times from the drop-down list.  
For example assume that you have configured a TrendWatch rule for last one day on an hourly basis. If the difference between two hours is greater than or equal to the set value then the trendwatch violation has occurred.

Step 17  Either:  
a. Select the Last radio button and enter the number in the text box,  
b. Select Days, Weeks, Months or Years from the drop-down list.  
Or  
a. Select the From radio button and enter the date from the calendar  
b. Select the time from the drop-down list.  
c. Enter the To date from the calendar  
d. Select the time from the drop-down list.  
For example, assume that you have configured a TrendWatch rule for an instance with the trend that occurs for at least five times in the past two weeks. If these criteria is not met, a TrendWatch violation has occurred and is stored in the database.

Step 18  Click Show Rule to view the created TrendWatch rule.
Step 19  Go to the Notification Details pane.
- Check the check box to send notification through e-mail. Enter the e-mail address to which LMS sends alert messages. The e-mail address must be in the format: user@domain.com. You can enter multiple e-mail addresses, separated by commas.
- Check the Attach report check box to attach the report as a CSV file. This CSV file is sent to the e-mail address specified in the e-mail field.
- Check the check box to send Traps to the Trap Receiver Group when any TrendWatch violation has occurred. Select the Trap Receiver Group from the drop-down list.
- Check the check box to send Syslog information to Syslog Receiver Group when any TrendWatch violation has occurred. Select the Syslog Receiver Group from the drop-down list.

Step 20  Go to the Schedule Details pane and select the Schedule type from the drop-down list.

Step 21  Specify the date and time the job is scheduled at. This field is disabled if you have selected **Immediate** as the Schedule Type.

Step 22  Go to Report Information pane and specify the path to publish the reports,

Step 23  Check the Add Full Report check box to create a PDF format of the report for all devices.

Step 24  Click **Create** to add the TrendWatch.
A message appears, confirming that TrendWatch is added successfully.

Step 25  Click **OK**.
The TrendWatch Configuration dialog box appears, allowing you to create more TrendWatches.
Or
Click **Cancel** to cancel the TrendWatch creation process.
The created TrendWatch is listed in the List of TrendWatches page.

Step 26  Click on the Name hyperlink to view the details of the TrendWatch created.

---

**Creating a TrendWatch Based on Threshold**

You can create TrendWatch rules on a threshold to monitor the devices for TrendWatches. An example of TrendWatch rules in this scenario is:

If the absolute value for CPU utilization is greater than $n\%$, for $x$ times in a week/month/year.

To create a TrendWatch based on threshold:

**Step 1**  Select **Monitor > Threshold Settings > TrendWatch** from the menu.
The List of TrendWatches page appears.

**Step 2**  Click **Create**.
The TrendWatch Configuration dialog box appears.
Table 2-9 describes the fields in the TrendWatch Configuration dialog box.

**Step 3**  Go to the TrendWatch Details pane and enter a descriptive name for the TrendWatch.
For example, CPU threshold.

**Step 4**  Select **Threshold** from the Based on Radio button to configure TrendWatch based on threshold.
Step 5 Go to the Select Thresholds pane and select the required threshold from the instance tree.

Step 6 Go to the Trend pane and select **At least, Exactly** or **Atmost** from the drop-down list.

Step 7 Enter a value in the text box.

Step 8 Select Times from the drop-down list.

This will be the only option available because you have selected **Threshold** to configure Threshold based TrendWatch.

Step 9 Either:
   a. Select the **Last** radio button and enter the number in the text box,
   b. Select **Days, Weeks, Months** or **Years** from the drop-down list.

Or
   a. Select the **From** radio button and enter the date from the calendar.
   b. Select the time from the drop-down list.
   c. Enter the **To** date from the calendar.
   d. Select the time from the drop-down list.

For example, assume that you have configured a TrendWatch rule for an instance with the trend that occurs for at least two times in the past one day. If this criteria is not met, a TrendWatch violation has occurred and is stored in the database.

Step 10 Click **Show Rule** to view the created TrendWatch rule.

Step 11 Go to the Notification Details pane.

- Check the check box to send alert notification through e-mail. Enter the e-mail address to which LMS sends alert messages. The e-mail address must be in the format: user@domain.com. You can enter multiple e-mail addresses, separated by commas.
- Check the Attach report check box to attach the report as a CSV file. This CSV file is sent to the e-mail address specified in the e-mail field.
- Check the check box to send Traps to the Trap Receiver Group when any TrendWatch violation has occurred. Select the Trap Receiver Group from the drop-down list.
- Check the check box to send Syslog information to Syslog Receiver Group when any TrendWatch violation has occurred. Select the Syslog Receiver Group from the drop-down list. Select the severity for the Syslog information from the Severity drop-down list.

Step 12 Go to the Schedule Details pane and select the Schedule type from the drop-down list.

Step 13 Specify the date and time the job is scheduled at.

Step 14 Go to Report Information pane and specify the path to publish the reports.

Step 15 Check the Add Full Report check box to create a PDF format of the report for all devices.

Step 16 Click **Create** to add the TrendWatch.

A message appears, confirming that TrendWatch is added successfully.
Step 17  Click **OK**.
The TrendWatch Configuration dialog box appears, allowing you to create more TrendWatches.  
Or  
Click **Cancel** to cancel the TrendWatch creation process.  
The created TrendWatch is listed in the List of TrendWatches page.

Step 18  Click on any TrendWatch name link.  
The TrendWatch view appears, displaying the TrendWatch rule details.

**Editing a TrendWatch**

You can modify the TrendWatch criteria of an existing TrendWatch using the Edit button. You can only make changes to the Notification details, Schedule details and the selection of Thresholds for threshold based TrendWatch.

You cannot make changes to the TrendWatch details (TrendWatch Name, Template Name, Variable Name).

You can edit only one TrendWatch at a time. If you select multiple TrendWatches using the check box, the Edit button is disabled.

To edit a TrendWatch:

**Step 1**  Select **Monitor > Threshold Settings > TrendWatch** from the menu.  
The List of Trend Watches page appears.

**Step 2**  Select the TrendWatch by checking the corresponding check box.  
If you select multiple TrendWatches the Edit button is disabled.

**Step 3**  Click **Edit**.  
The TrendWatch Configuration dialog box appears.  
See Table 2-9 for the description of the fields that appear in the Template-based TrendWatch dialog box.  
You cannot select a different data source while editing trendwatch. However, you can modify the same data source.  
For example, if you have selected Instance Selector while creating trendwatches, you can add or delete instances. You cannot select other data sources from Device Group Selector or Port Group Selector.

**Step 4**  Make the necessary changes to the Select Instances, Notification details and Schedule Details panes.  

**Note**  In the Schedule details pane, the Daily, Weekly and Monthly options are available for periodic reports.

**Step 5**  Click **Update**.  
A message appears, confirming that the TrendWatch is updated successfully.  
The updated TrendWatch is listed in the List of TrendWatches page.
Deleting a TrendWatch

LMS allows you to delete TrendWatches using the Delete button. Before a TrendWatch is deleted, you are prompted to confirm the deletion because you cannot restore a TrendWatch that you have deleted from the database.

Deleting a TrendWatch will delete the associated report and all its instances.

You can select multiple TrendWatches and delete them together.

To delete a TrendWatch:

**Step 1** Select Monitor > Threshold Settings > TrendWatch from the menu.

The List of TrendWatches page appears.

**Step 2** Select the TrendWatch by checking the corresponding check box.

**Step 3** Click Delete.

A message appears, prompting you to confirm the deletion.

**Step 4** Click OK to delete the TrendWatch or Cancel to cancel the operation.

If you choose to click OK, a message appears stating that the TrendWatch is deleted successfully.

Deactivating a TrendWatch

If you do not want the TrendWatch to monitor a (the polled) MIB variable, you can deactivate it using the De-activate button on the List of TrendWatches page.

For example, if there is an outage, you may not want notification e-mails for a particular period of time. In such instances you may choose to de-activate TrendWatches.

You can select multiple TrendWatches and deactivate them together.

To deactivate a TrendWatch:

**Step 1** Select Monitor > Threshold Settings > TrendWatch from the menu.

The List of TrendWatches page appears.

**Step 2** Select the TrendWatch to be deactivated by checking the check box.

**Step 3** Click De-activate.

A message appears, prompting you to confirm the deactivation.

**Step 4** Click OK to deactivate the TrendWatch.

Or

Click Cancel to cancel the operation.

If you click OK, a message appears that the TrendWatch is changed to an inactive state.

The List of TrendWatches page appears, displaying the status of the TrendWatch as Inactive.
Activating a TrendWatch

If you want an inactive TrendWatch to start monitoring a device for MIB variables, you can activate it using the Activate button on the List of TrendWatches page. You can select multiple TrendWatches and activate them together.

To activate a TrendWatch:

**Step 1** Select **Monitor > Threshold Settings > TrendWatch** from the menu.

The List of TrendWatches page appears.

**Step 2** Select the TrendWatch to be activated by checking the appropriate check box.

**Step 3** Click **Activate**.

A message appears, prompting you to confirm the activation.

**Step 4** Click **OK** to activate the TrendWatch.

Or

Click **Cancel** to cancel the operation.

If you click **OK**, a message appears that the TrendWatch is changed to an active state. The List of TrendWatches page appears, displaying the status of the TrendWatch as **Active**.

If you activate a TrendWatch, the monitoring starts based on the schedule.

---

**Copying a TrendWatch**

You can create a copy of an existing TrendWatch by selecting a TrendWatch name and clicking the Copy option.

For example, if you want to copy the same set of conditions for different set of devices or instances, you may choose to copy a TrendWatch.
To copy a TrendWatch:

**Step 1**  Select Monitor > Threshold Settings > TrendWatch from the menu.
The List of TrendWatches page appears.

**Step 2**  Check the check box corresponding to the TrendWatch name in the list.

**Step 3**  Click Copy.
The TrendWatch configuration dialog box appears, displaying the settings in the existing TrendWatch.
*Table 2-9* describes the fields in the TrendWatch Configuration dialog box.

**Step 4**  Go to the TrendWatch Details pane and enter a descriptive name for the TrendWatch.
For example, CPU Threshold.
The Template Name, Variable Name, Severity and TrendWatch conditions will be disabled when you configure a TrendWatch based on the threshold.

**Step 5**  Select a MIB variable from the Variable Name drop-down list.
The drop-down list shows a list of MIB variables polled using the selected template. For example, `cpmCPUTotal5minRev`.
The selected MIB variable displays all the polled device instances in the Select Instances pane.

**Step 6**  Modify the data source, if required.

**Note**  You cannot select a different data source while copying Trendwatch. However, you can modify the same data source. For example, if you have selected Instance Selector while creating Trendwatches, you can add or delete instances. You cannot select other data sources from Device Group Selector or Port Group Selector.

**Step 7**  Select a severity from the Severity drop-down list.
For example, Critical, Medium or Low.

**Step 8**  Go to the TrendWatch Conditions pane and select the Group By value from the Group By drop-down list.
For example Hourly, Daily, Monthly, Quarterly, and Yearly.
The condition is set, based on the TrendWatch value entered in the Value field.

**Step 9**  Select the Aggregate value from the Aggregate drop-down list.

**Step 10**  Select a condition from the Condition drop-down list.
The condition is set based on the TrendWatch value that you have entered in the Value field.

**Step 11**  Enter the TrendWatch value in the Value field.

**Step 12**  Go to the Trend pane, and enter the time period in the text field.

**Step 13**  Select **Times** or **Percentage of Times** from the drop-down list.
For example, assume that you have configured a TrendWatch rule for last one day on hourly basis. If the difference between two hours is greater than or equal to the set value then the TrendWatch rule is violated and will be stored in the database.

**Step 14**  Click **Show Rule** to view the created TrendWatch rule.
Step 15 Go to the Notification Details pane.
   - Check the check box for alert notification through e-mail. Enter the e-mail address to which LMS sends alert messages.
   - Check the Add Report check box to attach a PDF report with the e-mail notification.
   - Check the check box to send Traps to the Trap Receiver Group when any TrendWatch violation has occurred. Select the Trap Receiver Group from the drop-down list.
   - Check the check box to send Syslog information to Syslog Receiver Group when any TrendWatch violation has occurred. Select the Syslog Receiver Group from the drop-down list.

Step 16 Go to the Schedule Details pane and select the Schedule type from the drop-down list.

Step 17 Specify the date and time the job is scheduled at.

Step 18 Go to Report Information pane and specify the path to publish the reports.

Step 19 Check the Add Full Report check box to create a PDF format of the report for all devices.

Step 20 Click Create to add the TrendWatch.

A message appears, confirming that TrendWatch is added successfully.

Step 21 Click OK.

The TrendWatch Configuration dialog box appears, allowing you to create more TrendWatches.

Or

Click Cancel to cancel the TrendWatch creation process.

The created TrendWatch is listed in the List of TrendWatches page.

Filtering TrendWatch

This section describes how you can use the Filter option to display the TrendWatch information based on a specific criteria.

To filter TrendWatch information:

Step 1 Select Monitor > Threshold Settings > TrendWatch from the menu.

The List of TrendWatches page appears.

Step 2 Select a criteria for filtering from the drop-down list.

Step 3 Enter the data to be filtered in the text field.

Table 2-10 describes the methods you can follow to filter the data.

Step 4 Click Show.

The List of TrendWatches page appears, displaying the TrendWatch information based on the filter criteria.

Table 2-10 describes the criteria available to filter.
### TrendWatch Filter Fields

<table>
<thead>
<tr>
<th>Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
</table>
| TrendWatch Name  | Select **TrendWatch Name** and enter the data. You can use any of the following filter methods by entering:  
  - Complete TrendWatch name  
  - Any three consecutive characters of the TrendWatch name  
  - Any wildcard characters of the TrendWatch name (such as *a, a*, *a*) |
| Variable Name    | Select **Variable Name** and enter the data. You can use any of the following methods to filter by entering:  
  - Complete MIB variable name  
  - Any three consecutive characters of the MIB variable name  
  - Any wildcard characters of the MIB variable name (such as *a, a*, *a*) |
| Severity         | Select **Severity** and choose the severity as Critical, Medium, or Low. |
| Violation Count  | Select **Violation Count** and enter the violation count in numeric value. |
Fault Management

This chapter describes the following topics:

- Overview of Polling and Thresholds
- Updating Polling Parameters and Thresholds
- Setting Priorities
- Threshold Configuration
- Managing Polling Parameters
- Applying Polling and Threshold Changes
- Configuring SNMP Trap Receiving and Forwarding

These topics explain the process for configuring polling settings and threshold values for LMS.

Overview of Polling and Thresholds

The centralized Grouping Services Administration organizes devices, device interfaces, and device ports into different groups. The LMS system-defined groups include groups such as Broadband Cable, Routers, Switches and Hubs, and so on.

These groups have specific polling and threshold settings, while the Broadband Cable device type has different polling and threshold settings. Since a device can belong to multiple groups, the devices use the polling and threshold settings of the overriding group.

This section contains the following topics:

- Which Settings Are Applied to Devices, Ports, and Interfaces?
- Customizable Groups
- Selecting Groups

The Polling and Threshold function creates its own corresponding groups based on LMS Device groups and Fault groups:

- Polling groups that determine how often group members are polled for data.
- Threshold groups that determine acceptable levels of performance and utilization for group members.

When group objects are polled and the data of an object shows that threshold values have been exceeded, or values have fallen below acceptable levels, LMS generates the appropriate events.
LMS is configured with factory settings (or defaults) for polling parameters and threshold values. You can use the factory settings, modify them, and restore them to factory settings at any time.

In many cases, it may be acceptable to use the factory settings for polling parameters. However, depending on how important a device group is, you can increase or decrease the polling interval to:

- Minimize the impact on the polled devices
- Enhance the resolution of the collected data

You can also enhance the performance and utilization of devices by adjusting thresholds. You need to consider:

- Location of the devices in the IP fabric
- Resource constraints

### Which Settings Are Applied to Devices, Ports, and Interfaces?

Every device, device port, and device interface belongs to at least one system-defined group. When a device belongs to several groups, LMS uses the settings of the overriding group.

The overriding group is the highest priority device group to which the device belongs. These topics provide more information on priorities:

- Prioritizing Groups for Polling and Thresholds, lists default group priorities.
- Setting Priorities for Polling and Threshold Groups, explains how to change group priorities.

For information on the groups to which you can apply polling or threshold settings, see these topics:

- Which Polling Settings Are Applied?
- Which Threshold Settings Are Applied?

### Which Polling Settings Are Applied?

You can set and apply polling parameters to device groups. You cannot do this for individual devices. When a device is polled, its ports and interfaces are also polled; therefore port and interface polling is controlled at the group level.

Every device belongs to at least one system-defined device group. See Administration of Cisco Prime LAN Management Solution 4.1 for information about how devices are assigned to system-defined groups. If a device belongs to more than one group, LMS uses the polling settings of the overriding group (with the highest priority, as described in Setting Priorities for Polling and Threshold Groups).

### Which Threshold Settings Are Applied?

You can set and apply threshold parameters to device, interface, and port groups. When a device is polled, LMS compares the new data against the threshold settings. If a threshold value has been exceeded, or a value has fallen below acceptable levels, LMS generates the appropriate event.

If a device, port, or interface belongs to more than one group, LMS uses the threshold settings of the overriding group (the group you determine to have the highest priority, as described in Viewing the Overriding Group—Examples).
Customizable Groups

Customizable groups are the only user-defined groups for which you can set polling and threshold parameters. They are provided so you can create groups that fit your needs. LMS provides 28 customizable groups, which are divided into four categories:

- Access Port Groups
- Trunk Port Groups
- Interface Groups
- Device Groups

Table 3-1 lists the seven customizable groups that appear in each of the four categories.

<table>
<thead>
<tr>
<th>Customizable Groups</th>
<th>Intended Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Consider reserving customizable groups A, B, and C to troubleshoot</td>
</tr>
<tr>
<td>B</td>
<td>Add one device to any of these groups when you need to test. For example, to test a changed threshold or interval value for a polling setting.</td>
</tr>
<tr>
<td>C</td>
<td>Consider using customizable groups 1, 2, 3, and 4 when you want to override polling settings and thresholds for more than one device.</td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

You configure a customizable group to have the highest priority. To do so, see Setting Priorities for Polling and Threshold Groups. You must add devices to the customizable groups before you can set polling parameters or threshold values for them. To do so, see Administration of Cisco Prime LAN Management Solution 4.1.

Selecting Groups

When you use polling and threshold options, you must first select a group. If you want to view parameters, you can select any group. If you want to edit parameters or restore them to factory settings, you must select a group for which parameters exist.

Table 3-5 lists groups in the order in which they are displayed in the group selector and notes whether applicable parameters exist for the group. The group selector you see may not display all of the device groups listed in this table.

- System-defined groups are displayed in the polling and thresholds user interface when they have members.
- Customizable groups are displayed in the polling and thresholds user interface when a rule has been applied to them (using Group Administration).
### Table 3-2  Device Groups as Displayed in the Device Selector

<table>
<thead>
<tr>
<th>Device Groups in Display Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CS@server</strong></td>
<td>None</td>
</tr>
<tr>
<td>System Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Broadband Cable</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Cisco Interfaces and Modules</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Content Networking</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>DSL and Long Reach Ethernet (LRE)</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Network Management</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Optical Networking</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Routers</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Security and VPN</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Server Fabric Switches</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Storage Networking</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Switches and Hubs</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Server Fabric Switches</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Universal Gateways and Access Servers</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Voice and Telephony</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Wireless</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td><strong>DFM@server</strong></td>
<td>None</td>
</tr>
<tr>
<td>System Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Access Port Groups</td>
<td>None</td>
</tr>
<tr>
<td>1GB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>10GB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>10MB-100MB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>ATM</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Others</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Interface Groups</td>
<td>None</td>
</tr>
<tr>
<td>1GB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>10GB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>10MB-100MB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>ATM</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Backup</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Dial-on-Demand</td>
<td>Thresholds</td>
</tr>
<tr>
<td>FDDI</td>
<td>Thresholds</td>
</tr>
<tr>
<td>ISDN B Channel</td>
<td>Thresholds</td>
</tr>
<tr>
<td>ISDN D Channel</td>
<td>Thresholds</td>
</tr>
<tr>
<td>ISDN Physical Interface</td>
<td>Thresholds</td>
</tr>
</tbody>
</table>
Table 3-2  Device Groups as Displayed in the Device Selector (continued)

<table>
<thead>
<tr>
<th>Device Groups in Display Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Others</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Serial</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Token Ring</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Trunk Port Groups</td>
<td>None</td>
</tr>
<tr>
<td>1GB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>10GB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>10MB-100MB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>ATM</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Others</td>
<td>Thresholds</td>
</tr>
<tr>
<td>User Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Access Port Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group C</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 1</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group C</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group 1</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Interface Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group C</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 1</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Trunk Port Groups</td>
<td>None</td>
</tr>
</tbody>
</table>
Table 3-2  

<table>
<thead>
<tr>
<th>Device Groups in Display Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizable Group A</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group C</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 1</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td>Thresholds</td>
</tr>
</tbody>
</table>

For additional information, see the following topics:

- Viewing Polling Parameters
- Previewing Polling Parameters
- Editing Polling Parameters
- Viewing Thresholds
- Previewing Thresholds
- Editing Thresholds
Updating Polling Parameters and Thresholds

This topic explains how to update polling parameters and thresholds, and provides links to the related procedures.

LMS is preconfigured with factory settings for polling parameters and thresholds for each system-defined group of devices. You can make the following changes:

- Update the polling parameters and thresholds for system-defined groups.
- Restore polling parameters and thresholds to factory settings.
- Add devices to one or more of seven predefined customizable groups and edit their polling parameters and thresholds.

The following table describes the basic process for updating polling parameters and thresholds.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedures</th>
</tr>
</thead>
</table>
| **Step 1** If you are working with a customizable group, you may need to attend to the following tasks first:  
  a. Add devices to the customizable group. By default, no devices belong to customizable groups.  
  b. (Optional) Set the priority of the customizable group.  
     By default, customizable groups have a lower priority than system-defined groups. However, you may want to change the priority. | - Editing and Creating Groups. See the Administration of Cisco Prime LAN Management Solution 4.1 document for details.  
  - Setting Priorities for Polling and Threshold Groups |
| **Step 2** Change polling parameters for a device group  
This device group can be either a LMS system-defined group or a customizable device group. | - Editing Polling Parameters  
  - Restoring Factory Setting Polling Parameters |
| **Step 3** Change threshold parameters for any device, interface, or port group. | - Managing Fault Thresholds  
  - Restoring Factory Settings for Thresholds |
| **Step 4** After completing all changes, select a time of low activity on the network to update the IP fabric with these changes. The new values will not be used until you apply your changes. | - Applying Polling and Threshold Changes |

Setting Priorities

This section explains the following topics:

- Prioritizing Groups for Polling and Thresholds
- Viewing the Overriding Group—Examples
- Setting Priorities for Polling and Threshold Groups
- Setting Parameters for a Device, Interface, or Ports
### Prioritizing Groups for Polling and Thresholds

Devices, ports, and interfaces can belong to multiple groups. Owing to this, LMS uses the highest priority group to which the device belongs to determine which polling and threshold parameters to use.

LMS prioritizes groups as shown in the following tables, with groups in descending order of priority.

See the following tables for these details:

- Access and Trunk Port Group Priorities for Thresholds
- Interface Groups Priorities for Thresholds
- Device Groups Priorities for Polling and Thresholds

To find the overriding group for a device, you can select any device group to which the device belongs and view a Polling Parameter Summary or a Threshold Parameter Summary for the group.

A 10 GB Ethernet interface device, during an upgrade, behaves in the following ways:

- If the 10MB - 100MB group has been set to high priority when compared to 1 GB Ethernet group, then the 10GB device falls under the 10MB - 100MB group. In order to make it fall under 10 GB Ethernet Group, you must set the priority of the group to high.

- If the 10MB - 100MB group has been set to low priority when compared to 1 GB Ethernet group, then the 10GB device falls under 10 GB group.

For more information, see Setting Priorities.

<table>
<thead>
<tr>
<th>Access and Trunk Port Groups in Priority Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>1 GB Ethernet</td>
<td>Threshold</td>
</tr>
<tr>
<td>10MB - 100MB Ethernet</td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td></td>
</tr>
<tr>
<td>User Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Threshold</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td></td>
</tr>
<tr>
<td>Customizable Group C</td>
<td></td>
</tr>
<tr>
<td>Customizable Group 1</td>
<td>Thresholds</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td></td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td></td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3-4  Interface Groups Priorities for Thresholds

<table>
<thead>
<tr>
<th>Interface Groups in Priority Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>1GB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>10MB-100MB Ethernet</td>
<td>Thresholds</td>
</tr>
<tr>
<td>10 GB Ethernet</td>
<td>Threshold</td>
</tr>
<tr>
<td>ATM</td>
<td>Threshold</td>
</tr>
<tr>
<td>Token Ring</td>
<td>Threshold</td>
</tr>
<tr>
<td>ISDN Physical Interface</td>
<td>Threshold</td>
</tr>
<tr>
<td>ISDN B Channel</td>
<td>Threshold</td>
</tr>
<tr>
<td>ISDN D Channel</td>
<td>Threshold</td>
</tr>
<tr>
<td>Serial</td>
<td>Threshold</td>
</tr>
<tr>
<td>FDDI</td>
<td>Threshold</td>
</tr>
<tr>
<td>Backup</td>
<td>Threshold</td>
</tr>
<tr>
<td>Dial-on-Demand</td>
<td>Threshold</td>
</tr>
<tr>
<td>Others</td>
<td>Threshold</td>
</tr>
<tr>
<td>User Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Threshold</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td></td>
</tr>
<tr>
<td>Customizable Group C</td>
<td></td>
</tr>
<tr>
<td>Customizable Group 1</td>
<td>Threshold</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td></td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td></td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td></td>
</tr>
</tbody>
</table>

### Table 3-5  Device Groups Priorities for Polling and Thresholds

<table>
<thead>
<tr>
<th>Device Groups in Priority Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Security and VPN</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Content Networking</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Voice and Telephony</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Wireless</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Universal Gateways and Access Servers</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Broadband Cable</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Routers</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Storage Networking</td>
<td>Polling and thresholds</td>
</tr>
</tbody>
</table>
Setting Priorities

For additional information, see the following topics:

- Selecting Groups
- Viewing Polling Parameters
- Previewing Polling Parameters
- Viewing Thresholds
- Previewing Thresholds
- Prioritizing Groups for Polling and Thresholds
- Viewing the Overriding Group—Examples
- Setting Priorities for Polling and Threshold Groups
- Setting Parameters for a Device, Interface, or Ports

### Table 3-5  Device Groups Priorities for Polling and Thresholds (continued)

<table>
<thead>
<tr>
<th>Device Groups in Priority Order</th>
<th>Parameters to Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optical Networking</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Switches and Hubs</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Server Fabric Switches</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>DSL and Long Reach Ethernet (LRE)</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Cisco Interfaces and Modules</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Network Management</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>User Defined Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Groups</td>
<td>None</td>
</tr>
<tr>
<td>Customizable Group A</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group B</td>
<td></td>
</tr>
<tr>
<td>Customizable Group C</td>
<td></td>
</tr>
<tr>
<td>Customizable Group 1</td>
<td>Polling and thresholds</td>
</tr>
<tr>
<td>Customizable Group 2</td>
<td></td>
</tr>
<tr>
<td>Customizable Group 3</td>
<td></td>
</tr>
<tr>
<td>Customizable Group 4</td>
<td></td>
</tr>
</tbody>
</table>

1. A device can have different overriding polling and threshold groups.

Viewing the Overriding Group—Examples

The Polling Parameter Summary and Threshold Parameter Summary pages provide information on the overriding groups for all devices in a specific group. The following procedures explain how to locate the overriding group for a port or interface:

- Viewing the Overriding Polling or Threshold Group for a Device
- Viewing the Overriding Polling Group for a Port or Interface
Viewing the Overriding Polling or Threshold Group for a Device
Use the summary page to identify a device’s overriding group.

Step 1
Select Monitor > Fault Settings > Setup from the menu.

Step 2
Do either of the following:
- To view the overriding polling groups, select Polling Parameters.
- To view the overriding threshold group, select Threshold Settings.

A device can have different overriding polling and threshold groups.

For example, if you assign a router to use the settings from a customizable polling group, it would still use the settings from its original threshold group.

Step 3
Select a device group and click View.

The appropriate summary page opens.

Step 4
Locate the device in which you are interested, and check the Overriding Group column.

Viewing the Overriding Polling Group for a Port or Interface

Step 1
Select Monitor > Fault Settings > Setup from the menu.

Step 2
Consider the port or interface type and check the appropriate system-defined group for that type, and select Threshold Settings.

Step 3
Select the port or interface group and click View.

For example, if an interface is in the 10MB-100MB Ethernet interface group, select Managing Thresholds, choose that group, click View. Table 3-1 appears.

Step 4
Click View Interfaces.

A complete list of interfaces is displayed. If you were searching for a port, the link would be View Ports.
- If the interface or port appears as a member, that group is the overriding group. (Ports and interfaces are only listed as members in the overriding group.)
- If the interface or port does not appear, repeat this process for all of the customizable groups until you locate the port or interface.

- Viewing Polling Parameters
- Previewing Polling Parameters
- Viewing Thresholds
- Previewing Thresholds

Setting Priorities for Polling and Threshold Groups

System-defined groups have a higher priority than customizable groups, but you can change the priorities as needed. This is helpful, for example, when you configure specific customizable groups of interest and want to give them the highest priority.
For information on how to view the overriding group for devices, ports and interfaces, see *Viewing the Overriding Group—Examples*.

**Step 1** Select **Monitor > Fault Settings > Setup > Priority Settings** from the menu.

The Setting Priorities page appears, displaying the groups in priority order.

**Step 2** Activate the radio button that corresponds to the group type, one of the following:

- **Polling groups**: Device Polling Groups
- **Threshold groups**:
  - Device Threshold Groups
  - Interface Threshold Groups
  - Access Port Threshold Groups
  - Trunk Port Threshold Groups

**Step 3** Rearrange the groups according to your preference (the closer the group is to the top of the list, the higher its priority):

- a. Select a group.
- b. Move the group up or down using the arrows.

**Step 4** Click **Save** to save the changes.

- **Note** The changes do not take effect until you apply them to LMS. See *Applying Polling and Threshold Changes*. 
Setting Parameters for a Device, Interface, or Ports

There are several ways in which you can control the parameters for a device, interface, or port. Polling and thresholds are always applied on a group level, not on a specific device, port, or interface level.

Note

Be careful when you change settings for a system-defined group. Your changes will affect the settings of all devices in the group.

To apply settings to a device or component that belongs to multiple groups, make sure the group with the desired settings is the overriding group (has the highest priority), as described in Setting Priorities.

To configure polling and threshold settings for a device:

- Adjust the polling and threshold settings for the LMS system-defined group to which the device belongs. If needed, you can verify the overriding group. This changes the settings for all devices in that system-defined group.
- Edit a customizable device group, apply the desired polling and threshold settings to the group, and verify the overriding group. In this way, you can create a group of specific devices that you need and specify settings for them.

To configure polling on interfaces and ports:

- Adjust the polling settings defined by the LMS system-defined group. If needed, you can verify the overriding group. This changes the polling settings for all interfaces and ports on devices in that system-defined group.
- Edit a customizable device group, apply the desired polling settings to the group, and verify the overriding group. In this way, only the ports and interfaces on specific devices are affected.

To configure thresholds on interfaces and ports:

- Adjust the threshold settings defined by the LMS system-defined port or interface group. If needed, you can verify the overriding group.

  Make sure the port or interface belongs to that group, as described in Viewing the Overriding Polling Group for a Port or Interface. This changes the threshold settings for all interfaces and ports in that system-defined group.

- Edit a customizable interface or port group, apply the desired threshold settings, and verify the overriding group. In this way, only the ports and interfaces on specific devices are affected.

For additional information see:

- Editing Polling Parameters
- Editing Thresholds
Threshold Configuration

See Managing Fault Thresholds for information on configuring and managing fault thresholds.

Managing Polling Parameters

To manage polling parameters, select Monitor > Fault Settings > Setup > Polling Parameters from the menu. This feature allows you to perform the following tasks:

- Viewing Polling Parameters
- Previewing Polling Parameters
- Editing Polling Parameters
- Restoring Factory Setting Polling Parameters
- Device Polling Settings

You can adjust polling parameters only on devices. Port and interface polling is controlled at the device level. Therefore, you can adjust polling for these devices and groups:

- All devices managed by LMS
- LMS System Defined Groups
- LMS Customizable Groups (for devices)

Viewing Polling Parameters

When you view polling parameters, you can see the devices that are members of the device group, and you can see the factory setting as well as current values for the polling parameters.

Devices that belong to multiple groups use the polling settings of the overriding group. Interface and port polling is controlled at the device level.

This means that switches have a specific polling setting. This setting determines when the switch ports are polled.

**Step 1** Select Monitor > Fault Settings > Setup > Polling Parameters from the menu.

**Step 2** Select any device group from the group selector.

See Selecting Groups for a list of such device groups.

**Step 3** Click the View button.

The Polling Parameter Summary tabular display opens in a separate window. This window displays the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name of the device group selected.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device function.</td>
</tr>
</tbody>
</table>
Managing Polling Parameters

Step 4

After viewing the polling parameters, close the tabular display.

For additional information, see Viewing the Overriding Group—Examples.

Previewing Polling Parameters

When you preview polling parameters, you can see the edited polling parameters before you apply the changes.

Note

Preview is supported only for Device Type Groups.

Step 1
Select Monitor > Fault Settings > Setup > Polling Parameters from the menu.

Step 2
Select any device group from the group selector.

Step 3
Click the Preview button.

The Polling Parameter Summary tabular display opens in a separate window. This window displays the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name of the device group selected.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device function.</td>
</tr>
</tbody>
</table>

Field—Name of the polling setting to which the values apply.
Interval (sec)—Factory setting for number of seconds between successive polls for the setting.
New Interval (sec)—Current number of seconds between successive polls for the setting.
Timeout (msec)—Factory setting for number of milliseconds before a poll request times out.
New Timeout (msec)—Current number of milliseconds before a poll request times out.
Retry—Factory setting for the number of times to retry a failed poll request.
New Retry—Current number of times to retry a failed poll request.
Enabled—Whether polling is enabled (True) or disabled (False).
Overriding Group—Device group from which polling parameter values are applied. (This is the highest priority device group to which the device belongs.)

If you want to change the polling parameters for a device, you can edit the settings for the overriding group. See Editing Polling Parameters.
### Step 4

After previewing the polling parameters, close the tabular display.

The Polling Parameter Summary report displays the edited parameters for the selected device group. You can see the preview of the edited parameters based on the grouping of the devices in the selected device group.

### Previewing Polling Parameters — Example

The following example will help you to understand the preview of the displayed edited polling parameters:

Let us consider the devices D1, D2, D3, and D4 belonging to the following four groups:

- Routers: D1 and D2
- Switches and Hubs: D2 and D3
- Customizable Group1: D1 and D3
- Customizable Group 2: D2 and D4

Let the Overriding Group order of the groups be:

- Customizable Group1
- Routers
- Switches and Hubs
- Customizable Group 2

Let the Environment Settings parameter for the groups be:

- Routers: 200
- Switches and Hubs: 300
- Customizable Group1: 400

### Field Explanation

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| Polling Parameters | • Parameter—Name of the polling setting to which the values apply.  
                       • Interval (sec)—Factory setting for number of seconds between successive polls for the setting.  
                       • New Interval (sec)—Current number of seconds between successive polls for the setting.  
                       • Timeout (msec)—Factory setting for number of milliseconds before a poll request times out.  
                       • New Timeout (msec)—Current number of milliseconds before a poll request times out.  
                       • Retry —Factory setting for number of times to retry a failed poll request.  
                       • New Retry —Current number of times to retry a failed poll request.  
                       • Enabled—Whether polling is enabled (True) or disabled (False).  
                       • Overriding Group—Device group from which polling parameter values are applied. (This is the highest priority device group to which the device belongs.) |
To edit the parameter Environment Settings of a device group and to see the preview, do the following:

**Step 1** Select **Routers** that contain D1 and D2

**Step 2** Edit the Environment Settings by changing it to 800

**Step 3** Click the Preview button to see the edited parameters

The Polling Parameter Summary report for Routers (D1 and D2) is displayed.

The edited Environment Settings value 800 will be displayed only against the device D2.

Although D2 belongs to the groups Routers, Switches and Hubs, and Customizable Group 2, Routers is the overriding group among them. Since D2 belongs to the overriding group Routers, the edited parameter 800 is displayed against D2.

D1 belongs to the groups Routers and Customizable Group1 where Customizable Group1 is the Overriding group. So instead of the edited value 800, the value 400 which belongs to Customizable Group1 will be displayed against D1.

For more information on Overriding Groups, see Viewing the Overriding Group—Examples. To change the priority of the Device groups, see Setting Priorities for Polling and Threshold Groups.

Although the polling parameters are saved in the database, they are not yet applied to the IP fabric. See Applying Polling and Threshold Changes.

### Editing Polling Parameters

When you edit polling parameters, you edit settings that are associated with device groups, not with individual devices.

**Step 1** Select **Monitor > Fault Settings > Setup > Polling Parameters** from the menu.

**Step 2** Select a device group for which you can set polling parameters.

See Selecting Groups for a list of such device groups.

**Step 3** Click the Edit button.

The Polling Parameters: Edit page appears, displaying the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>The parameters for the selected device group are displayed, including:</td>
</tr>
<tr>
<td></td>
<td>• Current values for each setting</td>
</tr>
<tr>
<td></td>
<td>• Whether values are the factory settings (Default check box selected)</td>
</tr>
<tr>
<td></td>
<td>• Whether polling is enabled for the settings (Enabled check box selected)</td>
</tr>
</tbody>
</table>

**Step 4** Change the parameters appropriately for each setting.

Each setting controls how frequently devices are polled for a particular type of data; for example, reachability.
• To reset all settings to factory settings, select the Default check box in the table heading.
• To disable polling for all settings, deselect the Enabled check box in the table heading.
• To set parameters for individual settings, enter data for the following parameters for each setting.

### Field Description Usage Notes

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Interval</td>
<td>Enter the number of seconds between successive polls for the setting.</td>
<td>See Device Polling Settings for the minimum interval for each polling setting.</td>
</tr>
<tr>
<td></td>
<td>Maximum value: 3600</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minimum value: 30</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Increment: 1</td>
<td></td>
</tr>
<tr>
<td>New Timeout</td>
<td>Enter the number of milliseconds allowed for a poll request before it times out.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minimum value: 10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maximum value: 60,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Increment: 1</td>
<td></td>
</tr>
<tr>
<td>New Retry</td>
<td>Enter the number of times to retry a failed poll request.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minimum value: 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maximum value: 10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Increment: 1</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>To reset the values for the setting, to the factory settings, select this check box.</td>
<td>To view factory settings, see Viewing Polling Parameters.</td>
</tr>
<tr>
<td></td>
<td>The Default check box in the table heading can override this setting.</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>To disable polling for this setting, deselect this check box. To enable polling, select it.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Enabled check box in the table heading can override this setting.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 5
To save the settings, either:

• Click **Save** to save the changes and display the Polling Parameters: Edit page again.

Or

• Click **OK** to save the changes and close the Polling Parameters: Edit page.

### Step 6
Click **Preview** to see the edited polling parameters before applying the changes.

The Polling Parameter Summary report displays the edited parameters for the selected device group. You can see the preview of the edited parameters based on the grouping of the devices in the selected device group. For more information, see the Previewing Polling Parameters — Example given in the Previewing Polling Parameters section.
Restoring Factory Setting Polling Parameters

You can restore all parameter settings for a device group to factory settings using this procedure. If, instead, you want to restore only a few settings, see Editing Polling Parameters.

Before You Begin
To review the factory settings for polling parameters before you apply them, view the Polling Parameter Summary for the device group. See Viewing Polling Parameters. Both current and factory settings displayed.

Step 1
Select Monitor > Fault Settings > Setup > Polling Parameters from the menu.

Step 2
Select a device group for which you can restore polling parameters. See Selecting Groups for a list of such device groups.

Step 3
Click the Factory Setting.
A confirmation dialog box appears.

Step 4
Click Yes.
The settings are stored in the database, but not yet applied to the IP fabric. See Applying Polling and Threshold Changes.

Device Polling Settings

lists the polling settings that are applicable to each device group (or type), along with the minimum and maximum polling interval for each setting.

The minimum interval is usually lower than the factory setting provided by LMS. See Viewing Polling Parameters, to obtain information about how to open a Polling Parameter Summary, which lists the factory settings for polling parameter values.

This section also describes the minimum and maximum values for Interval, Timeout, and Retry parameters.
### Table 3-6  Polling Settings for Device Groups (Device Types)

<table>
<thead>
<tr>
<th>Device Group Type (Device Type)¹</th>
<th>Polling Settings</th>
<th>Interval (in seconds)</th>
<th>Timeout</th>
<th>Retry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadband Cable</td>
<td>Reachability settings</td>
<td>240</td>
<td>700</td>
<td>3</td>
</tr>
<tr>
<td>Cisco Interfaces and Modules</td>
<td>Processor and memory utilization</td>
<td>240</td>
<td>700</td>
<td>3</td>
</tr>
<tr>
<td>Content Networking</td>
<td>Environment</td>
<td>240</td>
<td>700</td>
<td>3</td>
</tr>
<tr>
<td>DSL and Long Reach Ethernet (LRE)</td>
<td>Connector port and interface</td>
<td>240</td>
<td>700</td>
<td>3</td>
</tr>
<tr>
<td>Optical Networking</td>
<td>Access port</td>
<td>1200</td>
<td>700</td>
<td>3</td>
</tr>
<tr>
<td>Routers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and VPN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Fabric Switches</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage Networking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switches and Hubs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Universal Gateways and Access Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice and Telephony</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Management</td>
<td>Reachability settings</td>
<td>240</td>
<td>700</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Connector and port interface</td>
<td>240</td>
<td>700</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Access port</td>
<td>1200</td>
<td>700</td>
<td>3</td>
</tr>
</tbody>
</table>

1. All polling intervals have a minimum of 30 seconds and a maximum of 3600 seconds.
Applying Polling and Threshold Changes

Note

Your login determines whether you can perform this operation.

Changes to polling parameters and threshold values do not take effect until you apply changes, thereby reconfiguring LMS to use the new values.

The following explains the difference between saving your changes and applying your changes.

When you save changes, LMS performs the following tasks:

- Sets the polling and threshold settings of devices in the selected device group.
- Sets the overriding group, based on the priorities of the groups to which devices belong.

When you apply changes, LMS:

- Recalculates group membership, based on group priority.
- Uses the new polling and threshold settings to gather information from the devices.

Similarly, after you resume devices or device components that were suspended from polling, you must apply changes for the device elements to be polled.

Before You Begin

Applying changes is a CPU-intensive event that may take between one and five minutes to complete. Therefore, to minimize system impact, consider doing the following when possible:

- Consolidating changes to polling parameters and threshold values, thereby limiting the number of times you will need to apply them.
- Applying changes during a low-usage time.

To apply the polling and threshold changes:

Step 1

Select **Monitor > Fault Settings > Setup > Apply Changes** from the menu.

The Apply Changes page appears.

Step 2

Click **Yes** to apply the changes:

- If another user has already initiated applying changes, a message is displayed and changes are not applied again.
- If, since the last time changes were applied, polling parameter settings or threshold values have not changed and devices have not been suspended and then resumed, changes will not be applied.

Tip

You cannot directly verify that changes have been applied. However, you can do so indirectly. For example, in response to an event, you change a threshold value and apply changes. After LMS finishes applying changes, you can see whether LMS clears the event.
Configuring SNMP Trap Receiving and Forwarding

LMS can receive traps on any available port and forward them to a list of devices and ports. This capability enables LMS to work with other trap processing applications.

This section contains the following topics:

- Enabling Devices to Send Traps to LMS
- Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs
- Updating the SNMP Trap Receiving Port
- Configuring SNMP Trap Forwarding

LMS will only forward SNMP traps from devices in the LMS inventory.

It will not change the trap format—it will forward the raw trap in the format in which the trap was received from the device. However, you must enable SNMP on your devices and you must do one of the following:

- Configure SNMP to send traps directly to LMS
- Integrate SNMP trap receiving with an NMS or a trap daemon

The versions of SNMP traps supported by LMS are described in Polling—SNMP and ICMP. For information on forwarding processed and pass-through traps, see Processing SNMP Traps.

---

**Note**

The ports and protocols used by LMS are listed in the Installing and Migrating to Cisco Prime LAN Management Solution 4.1 document.

---

Enabling Devices to Send Traps to LMS

**Note**

If your devices send SNMP traps to a Network Management System (NMS) or a trap daemon, see Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs.

Since LMS uses SNMP MIB variables and traps to determine device health, you must configure your devices to provide this information. For any Cisco device that you want LMS to monitor, SNMP must be enabled and the device must be configured to send SNMP traps to the LMS server.

Make sure your devices are enabled to send traps to LMS by using the command line or GUI interface appropriate for your device.

This section explains:

- Enabling Cisco IOS-Based Devices to Send Traps to LMS
- Enabling Catalyst Devices to Send SNMP Traps to LMS
Enabling Cisco IOS-Based Devices to Send Traps to LMS

For devices running Cisco IOS software, enter the following commands:

```
(config)# snmp-server [community string] ro
(config)# snmp-server enable traps
(config)# snmp-server host [a.b.c.d] traps [community string]
```

where `[community string]` indicates an SNMP read-only community string and `[a.b.c.d]` indicates the SNMP trap receiving host (the LMS server).

For more information, see the appropriate command reference guide.

---

**Step 1** Log into Cisco.com.
**Step 2** Select Products & Services > Cisco IOS Software.
**Step 3** Select the Cisco IOS software release version used by your IOS-based devices.
**Step 4** Select Technical Documentation and select the appropriate command reference guide.

Enabling Catalyst Devices to Send SNMP Traps to LMS

For devices running Catalyst software, provide the following commands:

```
(enable)# set snmp community read-only [community string]
(enable)# set snmp trap enable all
(enable)# set snmp trap [a.b.c.d] [community string]
```

where `[community string]` indicates an SNMP read-only community string and `[a.b.c.d]` indicates the SNMP trap receiving host (the LMS server).

For more information, see the appropriate command reference guide.

---

**Step 1** Log into Cisco.com.
**Step 2** Select Products & Services > Cisco Switches.
**Step 3** Select the appropriate Cisco Catalyst series switch.
**Step 4** Select Technical Documentation and select the appropriate command reference guide.
Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs

You might need to complete one or more of the following steps to integrate SNMP trap receiving with other trap daemons and other Network Management Systems (NMSs):

- If you are integrating LMS with a remote version of HP OpenView or NetView, you must install the appropriate adapter on the remote HP OpenView or NetView (see Installing and Migrating to Cisco Prime LAN Management Solution 4.1. This guide also provides information on supported versions). You do not need to install any adapters if HP OpenView or NetView is installed locally.

- Add the host where LMS is running to the list of trap destinations in your network devices. See Enabling Devices to Send Traps to LMS. Specify port 162 as the destination trap port. (If another NMS is already listening for traps on the standard UDP trap port (162), use port 9000, which LMS will use by default.)

- If your network devices are already sending traps to another management application, configure that application to forward traps to LMS.

Table 3-7 describes scenarios for SNMP trap receiving and lists the advantages of each.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network devices send traps to port 162 of the host where LMS is running. LMS receives the traps and forwards them to the NMS.</td>
<td>• No reconfiguration of the NMS is required. • No reconfiguration of network devices is required. • LMS provides a reliable trap reception and forwarding mechanism. • NMS continues to receive traps on port 162. • Network devices continue to send traps to port 162.</td>
</tr>
<tr>
<td>NMS receives traps on default port 162 and forwards them to port 162 on the host where LMS is running.</td>
<td>• No reconfiguration of the NMS is required. • No reconfiguration of network devices is required. • LMS does not receive traps dropped by the NMS.</td>
</tr>
</tbody>
</table>

Updating the SNMP Trap Receiving Port

By default, LMS receives SNMP traps on port 162 (or, if port 162 is occupied, port 9000). If you need to change the port, you can do so. LMS supports SNMP V1, V2, and V3 traps for trap receiving.

**Step 1** Select **Monitor > Fault Settings > SNMP Traps > Receiving** from the menu.

**Step 2** Enter the port number in the Receiving Port entry box.

**Step 3** Click **Apply**.

For a list of ports that are already in use, see Installing and Migrating to Cisco Prime LAN Management Solution 4.1. If you have two instances of the DfmServer process running, traps will be forwarded from the first instance to the second instance.
Configuring SNMP Trap Forwarding

Note
Your login determines whether or not you can perform this task.

LMS will only forward SNMP traps from devices in the LMS inventory. LMS will not change the trap format—it will forward the raw trap in the format in which it was received from the device. All traps are forwarded in V1 (SNMP Version) format.

To configure SNMP Trap Forwarding:

Step 1
Select Monitor > Fault Settings > SNMP Traps > Forwarding from the menu.

Step 2
For each host, enter:

- An IP address or DNS name for the hostname.
- A port number on which the host can receive traps.
- A community string. The default value is public.

Step 3
Click Apply.

For additional information, see Processed SNMP Traps, Pass-Through SNMP Unidentified Traps, and Unidentified Traps.

Viewing Fault Device Details

This section explains:

- Fault Device Details
- Understanding the Detailed Device View
- Managing/Unmanaging a Single Device Component
- Performing Bulk Manage/Unmanage Operations

Fault Device Details

You can view the fault details of devices in LMS. To do so:

Step 1
Select Monitor > Fault Settings > Setup > Fault Device Details from the menu.

The Fault Device Details page appears.

Step 2
Select one or more devices from the device selector tree. You can also search for the devices using the simple and advanced search operations.
Step 3

Click **View**.

The Device Details report appears.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Fault Management display name of the device. Click this link to launch a Detailed Device View.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Type of the device. Examples are Switches and Hubs, Cisco Interfaces and Modules, and so on.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Device IP address.</td>
</tr>
<tr>
<td>Status</td>
<td>Current state of the device.</td>
</tr>
<tr>
<td>First Added</td>
<td>The first time the device was added into Fault Management.</td>
</tr>
<tr>
<td>Last Discovered</td>
<td>The time and date the device was last discovered.</td>
</tr>
</tbody>
</table>

To start a Detailed Device View for the device, click the Device Name link.

Understanding the Detailed Device View

To understand the Detailed Device View, see the following topics:

- Component Categories Pane
- System Information Pane
- Record Count
- Command Buttons Area
- Managing/Unmanaging a Single Device Component

**Component Categories Pane**

The component categories pane lists the components of the device: Environment, System, and Interface (what is shown depends on the device being viewed). The following are some examples of what you may see in these categories:

- Environment: Temperature, fan, power supply, voltage information
- System: Hard disk, RAM, processor, memory information
- Interface: Interface, port, card information; IP addresses on the device

**Note**

Avoid using non-US (e.g., 8 bit ASCII) characters in the description of an Interface. If you use these characters in an interface description, an error occurs when you try to change the managed state of a device in the Detailed Device View page.

From a Detailed Device View for an aggregate (containing) device, you can launch a Detailed Device View for the contained device. For example, for a router containing MSFCs, open a Detailed Device View for the router. From the router Detailed Device View, you can launch a new Detailed Device View for the MSFC.
System Information Pane
The system information pane provides information such as the system name, IP address, SysObjectID, system contact, and so forth. The device type determines what is displayed by the Detailed Device View. If the system information pane lists an attribute with no value, it is because of one of the following reasons:

- The attribute is not populated.
- The attribute is not configured correctly.
- The attribute does not apply to the device.

If the current view is of a parent (or containing) device—for example, a Catalyst 6513 switch with an MSFC card—the System Information Pane will contain a button, Launch New DDV For This Device button. If you click that button, a Detailed Device View for the MSFC is displayed.

You can suspend or resume device or component monitoring by clicking the Suspend or Resume button.

Record Count
The record count lists the number of information types available on the device.

Command Buttons Area
In addition to the Suspend and Resume buttons in the system information pane, the Command Button area provides other ways to respond to alerts.

Table 3-8 Detailed Device View—Command Buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Refreshes the Detailed Device View page. (The Detailed Device View is not automatically refreshed; you must do so manually.)</td>
</tr>
<tr>
<td>Close</td>
<td>Closes the Detailed Device View page.</td>
</tr>
</tbody>
</table>

Managing/Unmanaging a Single Device Component

You can unmanage or remanage device components using the Detailed Device View (cards, interfaces, ports, IP addresses, and so forth). If you unmanage a component, LMS will ignore subsequent events (including traps).

Note
You cannot resume a device component if the parent device is suspended. You must resume the parent device first. If a parent device is suspended, the device components are also suspended.

Step 1
From the device display, click a device in the Device Name column.

The Detailed Device View opens.

Step 2
Select the component with the instance you want to unmanage or manage.
Step 3 Locate the instance you want to unmanage or manage, and make your change using the list in the ManagedState column.

Note that:

- You can change the unmanaged state of an IP component of a device to managed state, only if its underlying interface is in a managed state.
- You cannot change the state of a management IP because it is not displayed in the Detailed Device View page.
- You can place the cursor on Details to see the Interface/Port details of a specific device. This option is available only for Port and Interface components.
- You cannot unmanage the interface of the management IP. Its status is static and there is no option to unmanage it.

Step 4 Click Submit.

If you resumed any devices (and you are finished making all of your monitoring status changes), select Monitor > Fault Settings > Setup > Apply Changes from the menu. This causes LMS to resume polling according to the polling and threshold settings for the device.

Since this action is CPU-intensive, wait until you have made all of your monitoring status changes before you apply them.

Performing Bulk Manage/Unmanage Operations

You can use ASL scripts to perform bulk manage and unmanage operations of interfaces, ports, IP addresses, processors, and memory, as described in this topic. In these procedures you create and then edit a generated file so that it reflects the management state you want. Then you apply the change to the LMS inventory, so that LMS will use your new settings when gathering device information.

In the following procedures, NMSROOT represents the LMS installation directory. By default, these directories are:

- Solaris or Soft Appliance: /opt/CSCOpx
- Windows: C:\Progra~1\CSCOpx (which stands for C:\Program Files\CSCOpx)

Managing Interfaces with ONDEMAND mode

Interfaces with ONDEMAND mode are not managed by default.

To manage them using the dmct1 CLI command, enter:

```
get Ethernet_Performance_Setting:: "Thresholds setting group"
::AnalysisModeOfSubInterfacePerformance ENABLED
invoke ICF_PolicyManager::ICF-PolicyManager reconfigure
```

For example:
```
get Ethernet_Performance_Setting:: "SET-CFG-Interface Groups/1 Gb Ethernet/Ethernet_Performance_Setting" ::AnalysisModeOfSubInterfacePerformance ENABLED
invoke ICF_PolicyManager::ICF-PolicyManager reconfigure
```
Performance Management

Performance Management describes the following topics:

- Auto Monitoring
- Managing Pollers
- Managing Templates

Auto Monitoring

The Auto Monitoring feature provides an option to monitor the Link Port groups or All Devices automatically. When you opt to monitor these groups, pollers are created based on the polling intervals. Table 4-1 describes the default auto-monitored parameters for Link Port groups and All Devices group.

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Template Name</th>
<th>Default Polling Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Port groups</td>
<td>Interface Utilization</td>
<td>15 minutes</td>
</tr>
<tr>
<td></td>
<td>Interface Errors</td>
<td>15 minutes</td>
</tr>
<tr>
<td></td>
<td>Interface Availability</td>
<td>15 minutes</td>
</tr>
<tr>
<td>All Device groups</td>
<td>Device Availability</td>
<td>5 minutes</td>
</tr>
<tr>
<td></td>
<td>CPU Utilization</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>
You can change the polling intervals and select a different interval. To do so:

**Step 1**
Select **Monitor > Performance Settings > Setup > Automonitor** from the menu.

The Auto Monitoring details window appears.

**Step 2**
Select one of the following values available in the Polling Interval drop-down list to modify the polling interval:
- 1 Minute
- 5 Minutes
- 15 Minutes
- 30 Minutes

To exclude the group from auto-monitoring, select **Don’t Monitor** from the drop-down list.

**Step 3**
Click **Apply**.

See **Viewing Poller Configuration Details** for details of the system pollers created.
See **Managing Pollers** for managing system pollers.

Activating or deactivating the system poller may take a few minutes, if the poller has a large number of devices associated with it.

The status of the Automonitor pollers could be one of the following:
- Active
- Inactive
- Instance Polling
- Instance Not Found
- Updating Database

### Managing Pollers

Poller Management is one of the main features of Cisco Prime LMS. Poller Management page allows you to create and manage Pollers. A Poller is a collection of devices and template MIB variables configured in LMS to monitor the utilization and availability levels of devices that are connected to the network.

From the Poller Management page, you can create a Poller, modify the configuration of a Poller, delete a Poller, stop a Poller from polling the devices, view polling failures and so on.

To access the Poller Management page, select **Monitor > Performance Settings > Setup > Pollers**. The List of Pollers dialog appears.

**Table 4-2** describes the fields and buttons in the List of Pollers dialog box.
### Table 4-2 List of Pollers Field/Button Description

<table>
<thead>
<tr>
<th>Field / Button Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poller Name</td>
<td>Displays the Poller name. For example, XYZ Router. Click on the Name hyperlink to view the details of the Poller created.</td>
</tr>
<tr>
<td>Interval</td>
<td>Polling interval assigned to the poller. Polling interval is duration after which LMS queries the MIB variable on the device. Here the duration is calculated in terms of minutes and hours. For example, if the Polling Interval for a Poller is set as 15 minutes and the first polling cycle starts at 10:00 a.m., the next polling cycle is scheduled to start at 10:15 a.m.</td>
</tr>
<tr>
<td>No. of Devices</td>
<td>Number of devices added to the Poller.</td>
</tr>
<tr>
<td>No. of Templates</td>
<td>Number of templates added to the Poller.</td>
</tr>
</tbody>
</table>
| Status              | Status of a Poller. The following Poller status is displayed:  
  - Active—LMS is currently polling for device instances.  
  - Inactive—LMS has stopped polling for device instances. |
| Missed Cycles       | Number of polling interval cycles missed during polling. For example, if the Polling Interval for a Poller is set as 15 minutes and the first polling cycle starts at 10:00 a.m., the next polling cycle is scheduled to start at 10:15 a.m. If the polling cycle that started at 10.00 a.m. does not complete before 10:15 a.m., then the next polling cycle will start only at 10:30 a.m. The polling cycle missed at 10:15 is called Missed Cycle. The following are some of the possible reasons that may cause Missed Cycles:  
  - Frequent SNMP time-outs  
  - Delayed network response  
  - Unreachable devices |
| Poll Start Time     | Displays the last polling cycle start time. For example, Mon, Apr 21 2008, 15:30:05 |
| Poll End Time       | Displays the last polling cycle end time. For example, Mon, Apr 21 2008, 15:45:05 |
| Poller Type         | Displays the type of pollers. The poller types are historic and system. |
| Create (button)     | Creates a Poller. See Creating a Poller. |
| Clear Failures (button) | Clears failures recorded for a Poller. See Clearing Failures. |
| Clear Missed Cycles (button) | Clears all the polling interval cycles missed for a Poller. See Clearing Missed Cycles. |
Managing Pollers

You can perform the following tasks from the List of Pollers dialog box:

- **Creating a Poller**
- **Editing a Poller**
- **Deleting a Poller**
- **Deactivating a Poller**
- **Activating a Poller**
- **Selecting Instances**
- **Viewing Failures**
- **Clearing Failures**
- **Clearing Missed Cycles**
- **Filtering Poller List**
- **Viewing Poller Configuration Details**

### Creating a Poller

You can create a Poller by adding devices and selecting appropriate templates to poll the devices. You can also set polling frequencies to poll the devices. The Poller polls the devices for the template MIB variable and collects the device data.

You can use the polled data to analyze the utilization and availability of devices through reports. For more information, see the Reports Online help.
To enter poller settings for system pollers, select **Monitor > Performance Settings > Setup > Automonitor**.

To create a Poller:

**Step 1**
Select **Monitor > Performance Settings > Setup > Pollers** from the menu.
The List of Pollers dialog box appears.

**Step 2**
Click **Create**.
The Select Data Source and Templates page appears, displaying the Devices and Templates dialog box.

*Table 4-3* describes the fields in the Select Data Source and Templates dialog box.

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Data Source</td>
<td>Select one of the following data sources:</td>
</tr>
<tr>
<td></td>
<td>• Device</td>
</tr>
<tr>
<td></td>
<td>• Device Groups</td>
</tr>
<tr>
<td></td>
<td>• Port Groups</td>
</tr>
<tr>
<td></td>
<td>You can do basic and advanced search of devices in the Device selector.</td>
</tr>
<tr>
<td><strong>Device Selector</strong></td>
<td></td>
</tr>
<tr>
<td>Search Input</td>
<td>Enter your search expression in this field.</td>
</tr>
<tr>
<td></td>
<td>You can enter only instance name and not device name for the search input.</td>
</tr>
<tr>
<td>Search</td>
<td>Use the search icon to perform a simple search of devices, after you have</td>
</tr>
<tr>
<td></td>
<td>entered your search input.</td>
</tr>
<tr>
<td></td>
<td>For more information on how to use Device Selector, see *Administration</td>
</tr>
<tr>
<td></td>
<td>of Cisco Prime LAN Management Solution 4.1*.</td>
</tr>
<tr>
<td>Advanced Search</td>
<td>Search for devices by specifying a set of rules.</td>
</tr>
<tr>
<td></td>
<td>For more information on Advanced Search, see *Administration of Cisco</td>
</tr>
<tr>
<td></td>
<td>Prime LAN Management Solution 4.1*.</td>
</tr>
<tr>
<td>All</td>
<td>Click <strong>All</strong> to view all the devices added to the Device Credential</td>
</tr>
<tr>
<td></td>
<td>Repository in a hierarchical format (tree view).</td>
</tr>
<tr>
<td></td>
<td>Check the check boxes to select the devices.</td>
</tr>
<tr>
<td>Search Results</td>
<td>Displays all your Simple or Advanced search results. You can select all</td>
</tr>
<tr>
<td></td>
<td>devices, clear all devices, or select a few devices from the list.</td>
</tr>
<tr>
<td>Selection</td>
<td>Displays all devices that you have selected using the All or Search</td>
</tr>
<tr>
<td></td>
<td>Results tab.</td>
</tr>
<tr>
<td><strong>Poller Details</strong></td>
<td></td>
</tr>
<tr>
<td>Poller Name</td>
<td>Enter a descriptive name for the Poller.</td>
</tr>
<tr>
<td></td>
<td>The name can contain a mix of alphabets, numerals, and some special</td>
</tr>
<tr>
<td></td>
<td>characters (such as - . : ).</td>
</tr>
</tbody>
</table>
Managing Pollers

Step 3
Select one of the following radio buttons:
- Device
- Port Group
- Device Group

If you have selected Device Selector, select the required devices from the device tree.
If you have selected Port Group Selector, select the required port groups.
If you have selected Device Group Selector, select the required device groups.

Step 4
Add devices to the Poller by selecting devices from the Device Selector pane.

For more information on how to use Device Selector, see Administration of Cisco Prime LAN Management Solution 4.1.

When the automonitoring feature disabled, we recommend you to select the device groups for poller creation instead of selecting device instances.

Table 4-3 Data Source and Templates Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling Interval</td>
<td>Select a poll interval from the drop-down list. Polling Interval is the duration after which LMS queries the MIB variable on the device. Polling Interval is set as 5 minutes, by default.</td>
</tr>
</tbody>
</table>

**Templates**

<table>
<thead>
<tr>
<th>Available Templates</th>
<th>Displays the list of System-defined and User-defined templates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected Templates</td>
<td>Displays the list of templates selected for polling.</td>
</tr>
</tbody>
</table>

- Add (button) Adds templates to the Selected Templates list.
- Remove (button) Removes templates from the Selected Templates list.
- Add User Defined Templates (button) Creates and adds user-defined templates to the Available Templates list.

**Poller Preferences**

- Poll all Instances Polls all the instances of the device for the selected template.
  
  For example,
  1. Create a Poller by adding a device.
  2. Select Interface Utilization template.
  3. Select the Poll all Instances check box.

  In this case, all the interfaces in the device are polled for the Interface Utilization data.

- Threshold Only If you check Threshold Only, the polled data will not be stored. Threshold data will be maintained if you have configured thresholds for this poller.

  If you check this option, no data from this poller will be used while generating Poller reports.
Step 5  Enter a descriptive name for the Poller in the Poller Name field.

Step 6  Choose a poll interval from the Polling Interval drop-down list.

The default poll interval is set as 5 minutes, but you can make polling occur at any of the following intervals:

- 1 minute
- 5 minutes
- 15 minutes
- 30 minutes
- 1 hour
- 2 hours
- 4 hours
- 8 hours

Step 7  Add templates to the Poller by selecting templates from the Available Templates list in the Templates pane.

To select more than one template hold down the Ctrl key.

Step 8  Click **Add** to add the templates to the Selected Templates list.

Or

Click **Remove** to remove the templates from the Selected Templates list.

Step 9  Click **Add User Defined Templates** to create user-defined templates.

You can use the Add User Defined Templates button not only to create new templates, but also to add the newly created templates to the Available Templates list. For more information, see Creating a Template.

You cannot create user-defined templates when you select Port groups as data source.

If the port groups selector is selected as the data source, only the interface related templates are listed.

Step 10  Go to the Poller Preferences pane in the Select Data Source and Templates dialog box. Either:

a.  Check **Poll all Instances** to poll all the instances of the device for the selected template.

   This option is disabled if your data source is Device Groups or Port Groups.

b.  Check **Threshold Only** to create a Poller that does not store the polled data. However, it stores the thresholds created for this poller.

   A pop-up message appears:

   If you check Threshold Only, the polled data will not be stored. Threshold data will be maintained if you have configured thresholds for this poller. Click OK to proceed.

c.  Click **OK**.

d.  Click **Finish** in the Select Data Sources and Templates dialog box to complete creating the poller.

Or

e.  Go to Step 11 to continue.
Step 11  Click Next.

Note  The Next button is disabled when you select your data source as Device Groups or Port Groups.

Cisco Prime LMS polls the devices to get the instance information, indicated by a progress bar.

The instance query process may take several minutes based on the number of devices selected, SNMP timeout value, device or network slowness.

The Select Instances page appears, displaying the Available Instances dialog box. You can search and select instances using the Available Instances dialog box. For more information, see Instance Selector. Interfaces that are administratively down will not be shown in the Select Instances page. For more information, see Selecting Instances.

Table 4-4 describes the fields in the Available Instances dialog box.

<table>
<thead>
<tr>
<th>Field/Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Input</td>
<td>Enter your search expression in this text field. You can enter only a single instance name in</td>
</tr>
<tr>
<td></td>
<td>this field. The search string is not case sensitive. You can enter only instance name and not</td>
</tr>
<tr>
<td></td>
<td>device name for the search input. To search multiple instances, you can enter the instance name</td>
</tr>
<tr>
<td></td>
<td>with wildcard character *. This will locate the instances that match the text string that you</td>
</tr>
<tr>
<td></td>
<td>enter.</td>
</tr>
<tr>
<td>Search</td>
<td>Use this icon to perform a Simple search, after you have entered your search input. See</td>
</tr>
<tr>
<td></td>
<td>Performing Simple Search.</td>
</tr>
<tr>
<td>Advanced Search</td>
<td>Use this icon to perform an Advanced search. See Performing Advanced Search.</td>
</tr>
<tr>
<td>All</td>
<td>Lists all the devices you have selected in the Select Devices and Templates page in a</td>
</tr>
<tr>
<td></td>
<td>hierarchical format (tree view). Check the check box to select the instance. You can select all</td>
</tr>
<tr>
<td></td>
<td>instances, clear all instances, or select a few instances from the list.</td>
</tr>
<tr>
<td>Search Results</td>
<td>Displays all your Simple or Advanced search results and you can select all instances, clear all</td>
</tr>
<tr>
<td></td>
<td>instances, or select a few instances from the list.</td>
</tr>
<tr>
<td>Selection</td>
<td>Lists all the instances that you have selected in the All or Search Results tab or through a</td>
</tr>
<tr>
<td></td>
<td>combination of both. You can also use this tab to deselect the instances you have already</td>
</tr>
<tr>
<td></td>
<td>selected. You can perform more than one search and can accumulate your selection of instances.</td>
</tr>
<tr>
<td>Refresh (button)</td>
<td>Click Refresh to repoll the devices to get instance information.</td>
</tr>
</tbody>
</table>

Step 12  Select the required instances from the instance tree.
Step 13  Click Next.
The Poller Summary page appears, displaying the Poller configuration details.
To modify the Poller configuration, click Back until you reach the dialog box you want.
Table 4-5 describes the fields in the Poller Summary page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the Poller name.</td>
</tr>
<tr>
<td>Summary</td>
<td>Polling Interval Displays the time interval selected for polling.</td>
</tr>
<tr>
<td></td>
<td>Instance Details Displays the instances selected in a tree structure:</td>
</tr>
<tr>
<td></td>
<td>• Device name—Device selected for polling.</td>
</tr>
<tr>
<td></td>
<td>• Template name—Template applied for polling.</td>
</tr>
<tr>
<td></td>
<td>• Instance name—Instance selected for polling.</td>
</tr>
</tbody>
</table>

Step 14  Click Finish.
The Poller details are added to the database.
A pop-up message appears confirming Poller creation.

Step 15  Click OK and the List of Pollers dialog box appears, displaying the Poller.
The data polled is stored in the database and you can use the data to generate Poller reports.
An audit trail message is logged in the database.
Instance Selector

You can use the Available Instances dialog box to search and select instances in a device. You can search for instances using a simple search or an advanced search.

Table 4-4 describes the fields and tabs in the Available Instances dialog box.

Performing Simple Search

You can enter your search criteria in the Search Input field and search for the instances using the Search icon. You can enter only instance name and not device name for the search input.

Note the following points when you perform a simple search.

- You can use the wildcard character * to search for multiple instances that match the text string that you enter.
- If you are not using the wildcard character, make sure that you enter the full instance name.

Performing Advanced Search

Use the Advanced Search icon to open the Define Advanced Search Rule pop-up window and specify a rule to perform an Advanced search.

Table 4-6 describes the fields and buttons in the Define Advanced Search Rule window.

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
<td>Select a variable from the drop-down list. For example, Instance Name. The list of variables for Advanced Search are:</td>
</tr>
<tr>
<td></td>
<td>- Device Name</td>
</tr>
<tr>
<td></td>
<td>- Template Name</td>
</tr>
<tr>
<td></td>
<td>- Instance Name</td>
</tr>
<tr>
<td>Operator</td>
<td>The operator to be used in the rule. The list of operators are:</td>
</tr>
<tr>
<td></td>
<td>- Starts with</td>
</tr>
<tr>
<td></td>
<td>- Ends with</td>
</tr>
<tr>
<td></td>
<td>- Equals</td>
</tr>
<tr>
<td></td>
<td>- Contains</td>
</tr>
<tr>
<td>Search Expression</td>
<td>Enter your search expression in this text field.</td>
</tr>
<tr>
<td>Search (button)</td>
<td>Used to search for instances based on the defined rule.</td>
</tr>
<tr>
<td>Clear (button)</td>
<td>Clears the Search Expression field.</td>
</tr>
<tr>
<td>Cancel (button)</td>
<td>Cancels Advanced search.</td>
</tr>
</tbody>
</table>

If you want to perform a new search, click **Clear** before selecting any new instances.
Example—Using Advanced Search

The following example describes the procedure for selecting instances using Advanced search.

To perform Advanced search:

Step 1
Click the Advanced Search icon in the Available Instances dialog box.

The Define Advanced Search Rule dialog box appears.

Step 2
Create a search rule expression. To do so:
   a. Select Variable as Instance Name
   b. Select Operator as equals
   c. Enter the search expression as Supervisor

Step 3
Click Search.

The instances that satisfy the specified rule appear in the Available Instances dialog box.

Editing a Poller

You can edit a Poller to update or change the selection of devices, templates, instances, and polling frequencies using the edit wizard.

You can edit only one Poller at a time. If you select multiple Pollers using the check box, the Edit button is disabled. You cannot edit the Poller Name field.

You cannot edit the system pollers.

To edit a Poller:

Step 1
Select Monitor > Performance Settings > Setup > Pollers from the menu.

The List of Pollers dialog box appears.

Step 2
Select the Poller by checking the corresponding check box against the Poller Name.

Step 3
Click Edit.

The Select Devices and Templates dialog box appears, displaying the earlier settings.

See Creating a Poller for the description of fields that appear in the Select Devices and Templates dialog box.

You cannot select a different data source while editing pollers. However, you can modify the same data source.

For example, if you have selected Device Selector while creating pollers, you can add or delete devices. You cannot select other data sources from Device Group Selector or Port Group Selector.

Step 4
Make the necessary changes to the Device Selector, Poller Details, and Templates panes.
Step 5
Go to the Poller Preferences pane in the Select Devices and Templates dialog box. Either:

a. Check **Poll all Instances** to select all instances of the template MIB variable.

b. Check **Threshold Only** to create a Poller that does not store the polled data. However, it stores the thresholds created for this poller.

   A pop-up message appears:
   
   If you check Threshold Only, the polled data will not be stored. Threshold data will be maintained if you have configured thresholds for this poller. Click OK to proceed.

c. Click **OK**.

d. Click **Finish** in the Select Devices and Templates dialog box to complete updating the Poller.

   Or

e. Go to **Step 6** to continue.

Step 6
Click **Next**.

If any new devices or templates are added, LMS polls the devices to get the instance information, indicated by a progress bar.

The Available Instances dialog box appears, displaying the instances selected earlier in a tree format. If there are no changes to the devices or templates, only the instances that you have selected earlier appear in the Available Instances dialog box in a tree format.

To add more instances to the present selection:

a. Click **Refresh** in the Available Instances dialog box.

   The Select Instances page reloads, displaying all the available instances in a tree format. The pre-selections will be preserved even after Refresh.

b. Select the required instances.

   See Creating a Poller for more information on fields that appear in the Available Instances dialog box.

Step 7
To continue, either:

- Complete editing Poller information by clicking **Finish** from the Available Instances dialog box.

Or

- Go to **Step 8** to continue.

Step 8
Click **Next**.

The Poller Summary page appears, displaying the Poller configuration summary.

To modify the Poller configuration, click **Back** until you reach the dialog box you want. See Creating a Poller for the description of the fields that appear in the Poller Summary page.

Step 9
Click **Finish**.

The Poller details are updated in the database.

A pop-up message appears confirming that the Poller is updated successfully. The List of Pollers dialog box appears, displaying the Poller.

The data polled is stored in the database and you can use it to generate reports. An audit trail message is logged.
Deleting a Poller

You can delete one or more Pollers using the Delete button on the List of Pollers dialog box. Before a Poller is deleted, you are prompted to confirm the deletion because you cannot restore a Poller that you have deleted from the database. If you delete a Poller the polled data is also deleted.

You cannot edit the system pollers.

To delete a Poller:

**Step 1** Select **Monitor > Performance Settings > Setup > Pollers** from the menu.

The List of Pollers dialog box appears.

**Step 2** Select the Poller by checking the appropriate check box.

You can select multiple Pollers by checking their respective check boxes.

**Step 3** Click **Delete**.

A message appears, prompting you to confirm the deletion.

**Step 4** Click **OK** to delete the Poller.

Or

Click **Cancel** to cancel the operation.

If you choose to click **OK**, a message appears that the Poller is deleted successfully. The List of Pollers dialog box appears.

When you delete a Poller, the following data is also deleted:

a. Poller mapping information associated with the template.

b. Threshold configuration information associated with the Poller.

Deactivating a Poller

If you do not want the Poller to poll a device for a MIB variable, you can deactivate it using the De-activate button on the List of Pollers dialog box. You can select multiple Pollers and deactivate them at the same time.

To deactivate a Poller:

**Step 1** Select **Monitor > Performance Settings > Setup > Pollers** from the menu.

The List of Pollers dialog box appears.

**Step 2** Select the Poller to be deactivated by checking the check box.

**Step 3** Click **De-activate**.

A message appears, prompting you to confirm the deactivation.
Step 4  Click **OK** to deactivate the Poller.

Or

Click **Cancel** to cancel the operation.

If you choose to click **OK**, a message appears that the Poller is changed to inactive state.

The List of Pollers dialog box appears, displaying the status of the Poller as **Inactive**. The license count for polling the number of devices is not reduced when you deactivate a poller.

### Activating a Poller

If you want an inactive Poller to start polling a device for MIB variables, you can activate it using the Activate button on the List of Pollers dialog box. You can select multiple Pollers and activate them together.

To activate a Poller:

**Step 1**  Select **Monitor > Performance Settings > Setup > Pollers**.

The List of Pollers dialog box appears.

**Step 2**  Select the Poller to be activated by checking the appropriate check box.

**Step 3**  Click **Activate**.

A message appears, prompting you to confirm the activation.

**Step 4**  Click **OK** to activate the Poller.

Or

Click **Cancel** to cancel the operation.

If you choose to click **OK**, a message appears that the Poller is changed to Active state. The List of Pollers dialog box appears, displaying the status of the poller as **Active**. If you activate a Poller, the polling starts at the next cycle time specified in the polling interval.

### Viewing Failures

You can view failures that occurred during polling, in a tabular format. Polling for MIB variables may fail because of various reasons. These are:

- Unreachable devices
- Improper credentials
- MIB variable not found
- SNMP Timeout

LMS logs only the failures of last 24 hours in the database.
To view failures for a specific Poller:

**Step 1** Select **Monitor > Performance Settings > Setup > Pollers.**

The List of Pollers dialog box appears.

**Step 2** Click the link on the Status column to see the failures for that specific Poller.

The link in the status column is available only when a failure is recorded. Only the failures of last 24 hours are recorded and the Poller status is updated, as shown in the example, and appears as a link.

Example:

Active with Errors (82).

Here 82 is the number of polling errors occurred during the last 24 hours.

Table 4-7 describes the fields in the Failure View page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIB Variable</td>
<td>Displays the MIB variable. For example, ifInErrors</td>
</tr>
<tr>
<td>Instance</td>
<td>Displays the MIB variable instance. For example, VLAN-1</td>
</tr>
</tbody>
</table>
| Failure Status| • Transient—Either the device is down or the SNMP credentials are incorrect. In this case, the Poller will poll for the device only after three polling cycles  
• Permanent—Polled MIB variables or instances are not available. In this case, the Poller will poll for the MIB variables or instances only after six polling cycles |
| Failure Count | Number of failures recorded.                                                |
| Last Failed Reason | Reason for the last failure. For example, Request Timed-Out. Device may be down. |
| Last Failed   | Time of last failure. For example, Mon, Apr 21 2008, 17:30:15               |

### Clearing Missed Cycles

You can clear all the polling interval missed cycles recorded in the database for a Poller by clicking the Clear Missed Cycles button in the List of Pollers dialog box.

To clear missed cycles of a specific Poller:

**Step 1** Select **Monitor > Performance Settings > Setup > Pollers.**

The List of Pollers dialog box appears.

**Step 2** Select a Poller with missed cycles recorded during the last 24 hours.

**Step 3** Click **Clear Missed Cycles.**

A message appears, prompting you to confirm the Clear Missed Cycles operation.
Step 4    Click OK to clear the missed cycles recorded for the Poller.

Or

Click Cancel to cancel the operation.

If you click OK, a message appears that the missed cycles were cleared successfully for the Poller.

Step 5    Click OK.

The List of Pollers dialog box appears, displaying the status of the Poller without any recorded missed cycles.

---

**Clearing Failures**

You can clear all the failures recorded in the database for a Poller by clicking the Clear Failures button on the List of Pollers dialog box.

To clear failures of a specific Poller:

---

**Step 1**    Select Monitor > Performance Settings > Setup > Pollers.

The List of Pollers dialog box appears.

**Step 2**    Select a Poller with failures recorded during the last 24 hours.

**Step 3**    Click Clear Failures.

A message appears, prompting you to confirm the clear failure operation.

**Step 4**    Click OK to clear the failures recorded for the Poller.

Or

Click Cancel to cancel the operation.

If you choose to click OK, a message appears that the failures were cleared successfully for the Poller.

**Step 5**    Click OK.

The List of Pollers dialog box appears, displaying the status of the Poller without any recorded failures.

---

**Viewing Poller Configuration Details**

You can view the configuration details of a Poller showing the template name and the instances selected for polling each device, in a tabular format.

To view a Poller configuration:

---

**Step 1**    Select Monitor > Performance Settings > Setup > Pollers.

The List of Pollers dialog box appears.

**Step 2**    Click on the Poller name link.

The Poller View page appears, displaying the Poller configuration details.
Table 4-8 describes the fields available in the Poller View page.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>Templates associated with the Poller.</td>
</tr>
<tr>
<td>Instances</td>
<td>Displays the MIB variable instance in the device.</td>
</tr>
</tbody>
</table>

Filtering Poller List

This section describes how you can use the filter option to display the Poller information based on a specific criteria.

To filter a Poller:

2. Select a criteria for filtering from the drop-down list.
3. Enter the data to be filtered.
4. Click Show.

The List of Pollers dialog box appears, displaying the Poller information based on the filter criteria.

Table 4-9 describes the criteria to filter.

<table>
<thead>
<tr>
<th>Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
</table>
| Poller Name     | Select Poller Name and enter the data. You can use any of the following methods to filter by entering:  
|                 | • Complete Poller name                           |
|                 | • Any three consecutive characters of the Poller name |
|                 | • Any wildcard characters of the Poller name (such as *a, a*, *a*) |
| Interval        | Select Interval and choose a duration from the drop-down list. |
| Status          | Select Status and choose a status from the drop-down list.  
|                 | Example: Active or Inactive.                     |

Selecting Instances

LMS runs an internal process to check the device and interface status and to store the status in the memory and in the database. This check happens every $N$ hours, where $N$ can be configured by editing the property value Interval Time in the Properties file. The value for $N$ should be an integer. The property file can be found at the following location:
Managing Pollers

- In Solaris or Soft Appliance:

  \[ \text{NMSROOT}/\text{MDC}/\text{tomcat}/\text{webapps}/\text{upm}/\text{WEB-INF}/\text{classes/com/cisco/nm/upm/properties/common/UPM.properties} \]

- In Windows:

  \[ \text{NMSROOT/\text{MDC/tomcat/webapps/upm/WEB-INF/classes/com/cisco\nm/upm\properties\common/UPM.properties} \]

where \$NMSROOT\ is the default Cisco Prime LMS installation directory.

For every polling cycle, the status of the device or interface status as maintained in the memory is checked. Table 4-10 describes the behavior of pollers for device and interface related templates during polling cycle:

**Table 4-10  Poller Behavior during Poling Cycle**

<table>
<thead>
<tr>
<th>Type</th>
<th>Status</th>
<th>Poller Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Up</td>
<td>All the templates are polled.</td>
</tr>
<tr>
<td></td>
<td>Down</td>
<td>Only the device and interface availability templates are polled.</td>
</tr>
<tr>
<td>Interface</td>
<td>Up</td>
<td>All the interface related templates are polled.</td>
</tr>
<tr>
<td></td>
<td>Down</td>
<td>Only interface availability template is polled.</td>
</tr>
</tbody>
</table>

During the process idle time, if any new poller is created or any poller is edited by adding new device, this check does not happen as the status of the newly added device is not available in the LMS database memory.

This status will be available from the next cycle of this process or the next polling cycle of the newly created or edited poller.

- If the new poller is created with the Device Availability template, the Device Availability status is polled
- If the new poller is created with the Interface Availability template, the Interface Availability status is polled.

The default behavior as mentioned in Table 4-10. You can change this by configuring the values of Related Variables in the property file. The Table 4-11 describes the poller behavior for different Related Variable values:

**Table 4-11  Poller Behavior for Related Variable values**

<table>
<thead>
<tr>
<th>Related Variable Name</th>
<th>Value</th>
<th>Poller Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Status</td>
<td>Enable</td>
<td>If the device is down, then only device availability template is polled. If the device is up then all the templates are polled.</td>
</tr>
<tr>
<td></td>
<td>Disable</td>
<td>Device status is not polled.</td>
</tr>
<tr>
<td>Interface Status</td>
<td>Enable</td>
<td>If the interface is down, then only interface availability template is polled. If the interface is up then all the templates are polled.</td>
</tr>
<tr>
<td></td>
<td>Disable</td>
<td>Interface status is not polled.</td>
</tr>
</tbody>
</table>
Polling MIB Objects Exceeding Limit

LMS supports polling up to 100,000 MIB object variables. If the object polled exceeds the limit of 100,000, performance of the system may be slower.

See Installing and Migrating to Cisco Prime LAN Management Solution 4.1 for the scalability limits of polling MIB variables.

More MIB variables are being polled when the following type of pollers poll devices with more instances:

- Automonitoring pollers
- User-defined pollers

If you do not want the Poller to poll a device for a MIB variable, you can deactivate it. You can also select multiple Pollers and deactivate them at the same time.

See Deactivating a Poller to deactivate the pollers to stop polling a device.

Managing Templates

Templates are a logical group of MIB variables that allow you to monitor the performance parameters of a device (such as CPU, memory, interface) for utilization and availability levels.

From the Template Management page you can create a user-defined template, modify the configuration of a user-defined template, export and import a user-defined template, delete a user-defined template, and so on.

The following template types are used in LMS:

- System-defined Templates
- User-defined Templates

This section also contains:

- Creating a Template
- Editing a Template
- Deleting a Template
- Copying a Template
- Exporting a Template
- Importing a Template
- Filtering Template List
- Viewing Template Details

System-defined Templates

System-defined templates help you to easily monitor devices. System-defined templates provide most of the common network parameters that you need to monitor a device connected to the network. These templates cannot be deleted or modified. By default, System-defined templates are loaded when LMS is installed.
Table 4-12 describes the list of System-defined templates used in LMS.

<table>
<thead>
<tr>
<th>Template Name</th>
<th>MIB Variables Polled</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Utilization</td>
<td>Primary Set:</td>
<td>Monitors the CPU utilization percentage of a device.</td>
</tr>
<tr>
<td></td>
<td>cpmpCPUTotal5minRev (1.3.6.1.4.1.9.9.109.1.1.1.1.8)</td>
<td>The MIB variables in the primary and fallback sets provide the percentage</td>
</tr>
<tr>
<td></td>
<td>Fallback Set 1:</td>
<td>CPU utilization information of a device.</td>
</tr>
<tr>
<td></td>
<td>cpmpCPUTotal5min (1.3.6.1.4.1.9.9.109.1.1.1.1.5)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fallback Set 2:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>avgBusy5 (1.3.6.1.4.1.9.2.1.58)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fallback Set 3:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hrProcessorLoad (1.3.6.1.2.1.25.3.3.1.2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fallback Set 4:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cseSysCPUUtilization (1.3.6.1.4.1.9.9.305.1.1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fallback Set 5:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>apChassisMgrExtSubModuleCPUAverage (1.3.6.1.4.1.2467.1.34.17.1.14)</td>
<td></td>
</tr>
<tr>
<td>Device Availability</td>
<td>Primary Set:</td>
<td>Monitors the availability of a device in a network.</td>
</tr>
<tr>
<td></td>
<td>sysUpTime</td>
<td></td>
</tr>
<tr>
<td>Environmental</td>
<td>Primary Set:</td>
<td>Monitors the environmental temperature in a device.</td>
</tr>
<tr>
<td>Temperature</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ciscoEnvMonTemperatureStatusIndex (1.3.6.1.4.1.9.9.13.1.3.1.1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ciscoEnvMonTemperatureStatusDescr (1.3.6.1.4.1.9.9.13.1.3.1.2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ciscoEnvMonTemperatureStatusValue (1.3.6.1.4.1.9.9.13.1.3.1.3)</td>
<td></td>
</tr>
<tr>
<td>Interface Availability</td>
<td>Primary Set:</td>
<td>Monitors the interface availability in a device.</td>
</tr>
<tr>
<td></td>
<td>ifOperStatus (1.3.6.1.2.1.2.2.1.8)</td>
<td></td>
</tr>
<tr>
<td>Interface Errors</td>
<td>Primary Set:</td>
<td>Monitors the interface errors in a device.</td>
</tr>
<tr>
<td></td>
<td>ifInErrors (1.3.6.1.2.1.2.2.1.14)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ifOutErrors (1.3.6.1.2.1.2.2.2.1.20)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ifInDiscards (1.3.6.1.2.1.2.2.1.13)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ifOutDiscards (1.3.6.1.2.1.2.2.1.19)</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4-12  System-defined Templates Used in LMS (continued)

<table>
<thead>
<tr>
<th>Template Name</th>
<th>MIB Variables Polled</th>
<th>Description</th>
</tr>
</thead>
</table>
| Interface Utilization    | Primary Set: ifInOctets (1.3.6.1.2.1.2.2.1.10)  
ifOutOctets (1.3.6.1.2.1.2.2.1.16)  
ifSpeed (1.3.6.1.2.1.2.2.1.5)  
Formula used for Interface Rx Utilization:  
\[
\text{Input Utilization} = \frac{\text{ifInOctets} \times 8 \times 100}{\text{ifSpeed}} 
\]  
Formula used in fallback set for Interface Tx Utilization:  
\[
\text{Output Utilization} = \frac{\text{ifOutOctets} \times 8 \times 100}{\text{ifSpeed}} 
\]  
Fallback Set:  
ifHCInOctects (1.3.6.1.2.1.31.1.1.1.6)  
ifHCOutOctects (1.3.6.1.2.1.31.1.1.1.10)  
ifHighSpeed (1.3.6.1.2.1.31.1.1.1.15)  
Formula used in fallback set for Interface 64bit Rx Utilization:  
\[
\text{Input Utilization} = \frac{\text{ifHCInOctects} \times 8 \times 100}{\text{ifHighSpeed} \times 1000 \times 1000} 
\]  
Formula used for Interface 64bit Tx Utilization:  
\[
\text{Output Utilization} = \frac{\text{ifHCOutOctects} \times 8 \times 100}{\text{ifHighSpeed} \times 1000 \times 1000} 
\] | Monitors the interface utilization of a device.  
64-bit counters are polled for high-speed interfaces (greater than 20 mbps) and 32-bit counters for low speed interfaces (less than 20 mbps).  
If the device is running with SNMPv1 image, all interfaces that are associated with the device, will poll for 32-bit Interface Utilization counters, without considering the ifspeed value.  
If the device is running with SNMPv2 or SNMPv3 images, the ifspeed value is checked for the interface.  
The ifspeed value is checked before polling the 32-bit and 64-bit counters. |
| Memory Utilization       | Primary Set:  
CiscoMemoryPoolUsed  
ciscoMemoryPoolFree  
Formula used in Primary Set:  
\[
\text{MemoryUtilization} = \frac{\text{CiscoMemoryPoolUsed}}{\text{CiscoMemoryPoolUsed} + \text{CiscoMemoryPoolFree}} \times 100 
\]  
Fallback Set 1:  
ceSysSysMemoryUtilization (1.3.6.1.4.1.9.9.305.1.1.2)  
Fallback Set 2:  
hStorageSize (1.3.6.1.2.1.25.2.3.1.5)  
hStorageUsed (1.3.6.1.2.1.25.2.3.1.6)  
Formula used in Fallback Set 2:  
\[
\text{MemoryUtilization} = \frac{\text{hStorageUsed}}{\text{hStorageSize}} \times 100 
\] | Monitors the memory utilization percentage of a device.  
The MIB variable in the fallback set 1 cseSysMemoryUtilization provides the percentage memory utilization data of a device. |
| PoE Port Utilization     | Primary Set:  
cpeExtPsePortPwrAllocated (1.3.6.1.4.1.9.9.402.1.2.1.7)  
cpeExtPsePortPwrAvailable (1.3.6.1.4.1.9.9.402.1.2.1.8)  
cpeExtPsePortPwrConsumption (1.3.6.1.4.1.9.9.402.1.2.1.9)  
Monitors the power utilization percentage and power losses of a device. |
Managing Templates

In System-defined templates, if the MIB variable in the primary set is not available, an alternate MIB variable in the fallback set stored in the device is selected. This fallback mechanism is applied in all the system-defined templates except for Interface Utilization template.

This fallback logic is applied during Poller creation and an appropriate MIB variable is selected for polling. System-defined templates support all Cisco devices that support the following MIB files:

- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENVMON-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PROCESS-MIB
- ENTITY-MIB
- OLD-CISCO-CHASSIS-MIB
- RFC1213-MIB
- IF-MIB
- CISCO-POWER-ETHERNET-EXT-MIB
- POWER-ETHERNET-MIB
- CISCO-RTTMON-MIB
- ROOT-OID-MIB
- CISCO-ENERGYWISE-MIB

### Table 4-12 System-defined Templates Used in LMS (continued)

<table>
<thead>
<tr>
<th>Template Name</th>
<th>MIB Variables Polled</th>
<th>Description</th>
</tr>
</thead>
</table>
| PoE PSE Consumption      | pethMainPseConsumptionPower(1.3.6.1.2.1.105.1.3.1.1.4)  
                          | pethMainPsePower (1.3.6.1.2.1.105.1.3.1.1.2)  
                          | Formula used in Primary Set:  
                          |                                                                                     |
|                          | PowerUtilization = \left( \frac{\text{pethMainPseConsumptionPower}}{\text{pethMainPsePower}} \right) \times 100  
                          |                                                                                     |
|                          | Monitors the power utilization percentage and power losses of a device.               |                                                                                     |
| EnergyWise Port Power Usage | Primary Set:  
                          | cewEntEnergyUsage (1.3.6.1.4.1.9.9.683.1.6.1.8)  
                          | cewEntEnergyUnits (1.3.6.1.4.1.9.9.683.1.6.1.7)  
                          | Formula used in the Primary Set:  
                          |                                                                                     |
|                          | EnergyWise Port Power Usage = \frac{\text{ewEntEnergyUsage}}{(\text{ewEntEnergyUnits})} \times 10^2  
                          |                                                                                     |
|                          | Monitors the power usage on a port in a device.                                       |                                                                                     |
| EnergyWise Device Power Usage | Primary Set:  
                          | cewEntEnergyUsage (1.3.6.1.4.1.9.9.683.1.6.1.8)  
                          | cewEntEnergyUnits (1.3.6.1.4.1.9.9.683.1.6.1.7)  
                          | Formula used in the Primary Set:  
                          |                                                                                     |
|                          | EnergyWise Device Power Usage = \frac{\text{ewEntEnergyUsage}}{(\text{ewEntEnergyUnits})} \times 10^2  
                          |                                                                                     |
|                          | Monitors the power usage on all ports in a device.                                    |                                                                                     |
User-defined Templates

Cisco Prime LMS allows you to create your own templates by grouping new MIB variables or by leveraging MIB variables from System-defined templates to suit your requirements. These templates are called user-defined templates.

You can add or delete MIB variables in a user-defined template. After the user-defined template is created, the template is listed in the List of Templates page.

To access the Template Management page, select Monitor > Performance Settings > Setup > Templates.

The List of Templates page appears, displaying the templates configured, in a tabular format. Table 4-13 describes the fields and buttons in the List of Templates page.

Table 4-13 List of Templates Field Description

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>Name of the template.</td>
</tr>
<tr>
<td>No. of MIB Variables</td>
<td>Number of MIB variables associated with the template.</td>
</tr>
<tr>
<td>No. of Pollers</td>
<td>Number of Pollers associated with the template.</td>
</tr>
<tr>
<td>Associated</td>
<td></td>
</tr>
<tr>
<td>Created By</td>
<td>User who created the template.</td>
</tr>
<tr>
<td></td>
<td>Example: System or Admin.</td>
</tr>
<tr>
<td>Filter (button)</td>
<td>Select the filter criteria and enter the data.</td>
</tr>
<tr>
<td></td>
<td>Use one of the following filter criteria and click Show:</td>
</tr>
<tr>
<td></td>
<td>• Template Name</td>
</tr>
<tr>
<td></td>
<td>• Created By</td>
</tr>
<tr>
<td></td>
<td>See Filtering Template List.</td>
</tr>
<tr>
<td>Create (button)</td>
<td>Creates a template. See Creating a Template.</td>
</tr>
<tr>
<td>Edit (button)</td>
<td>Modifies a template. See Editing a Template.</td>
</tr>
<tr>
<td>Delete (button)</td>
<td>Deletes a template. See Deleting a Template.</td>
</tr>
<tr>
<td>Copy (button)</td>
<td>Creates a template from an existing System-defined or User-defined template. See Copying a Template.</td>
</tr>
<tr>
<td>Export (button)</td>
<td>Exports a template to a directory location. See Exporting a Template.</td>
</tr>
<tr>
<td>Import (button)</td>
<td>Imports a template from a directory location. See Importing a Template.</td>
</tr>
</tbody>
</table>
You can perform the following tasks from the List of Templates page:

- Creating a Template
- Editing a Template
- Deleting a Template
- Copying a Template
- Exporting a Template
- Importing a Template
- Filtering Template List
- Viewing Template Details

## Creating a Template

This section explains how to create a user-defined template. You can create a user-defined template by grouping new MIB variables. You can also create user-defined templates during Poller creation using the Add User Defined Template option.

To create a template:

### Step 1

Select **Monitor > Performance Settings > Setup > Templates**.

The List of Templates dialog box appears.

### Step 2

Click **Create**.

The Select MIB Variables page appears, displaying the MIB Variables dialog box. You can search and select MIB variables from the MIB Variables dialog box. For more information, see MIB Variable Selector.

Table 4-14 describes the field and tabs in the MIB Variables dialog box.

<table>
<thead>
<tr>
<th>Field/Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>Enter the template name. The name can contain a mix of alphabets, numerals, and some special characters (such as - _ . # @ $ &amp;).</td>
</tr>
<tr>
<td>Show MIB</td>
<td>Displays the MIB files as a drop-down list.</td>
</tr>
<tr>
<td>Search Input</td>
<td>Enter your search expression in this text field.</td>
</tr>
<tr>
<td>Search</td>
<td>Use the icon to perform a simple search, after you have entered your search input. For more information, see Performing Simple Search.</td>
</tr>
</tbody>
</table>

To add new MIB files to the drop-down list, see the Load MIB Files section in Administration of Cisco Prime LAN Management Solution 4.1.
Step 3 Enter a descriptive template name in the Template Name field.

Step 4 Select a MIB file from the Show MIB drop-down list.
A MIB tree for the selected MIB file is displayed under the All tab.

Step 5 Add MIB variables by selecting the required MIB variables from the MIB tree.
You can also use the Search option to select MIB variables.
Only integer MIB variables are displayed in the MIB tree and not string MIB variables. For example, ifDescription is a string MIB variable and will not be displayed in the MIB tree.
You cannot add MIB variables from two different tables in the MIB tree.

Step 6 Click Next.
The MIB Alias Name dialog box appears.

Step 7 Click Finish.
A message appears confirming that the template is created successfully.
The List of Templates dialog box appears, displaying the template.

<table>
<thead>
<tr>
<th>Field/Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Lists all the MIB variables associated with the MIB file selected from the Show MIB drop-down list in a hierarchical format (tree view). Check the check boxes to select the MIB variables. You can select all MIB variables, clear all MIB variables, or select a few MIB variables from the list.</td>
</tr>
<tr>
<td>Search Results</td>
<td>Displays all your search results. You can select all MIB variables, clear all MIB variables, or select a few MIB variables from the list.</td>
</tr>
<tr>
<td>Selection</td>
<td>Lists all the MIB variables that you have selected in the All or Search Results tab or through a combination of both. You can also use this tab to deselect the MIB variables you have already selected.</td>
</tr>
</tbody>
</table>

**Table 4-15 Select MIB Variables Fields (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIB Variable</td>
<td>Displays the MIB variables selected in Step 5.</td>
</tr>
<tr>
<td>Alias Name</td>
<td>Displays a default alias name for the MIB variable. You can assign a descriptive name as the alias name for the MIB variable. After you have named the MIB variable with an alias name, the variable appears with this alias name throughout the application.</td>
</tr>
</tbody>
</table>
MIB Variable Selector

You can use the MIB Variables dialog box to search and select MIB variables from a MIB file. You can search for MIB variables using a Simple search. For more information, see Performing Simple Search. Table 4-14 describes the fields and tabs in the MIB Variable selector window.

Performing Simple Search

You can enter your search expression in the Search Input field and search for the instances using the Search icon.

Note the following points when you perform a simple search:

- You can use the wildcard character * to search for multiple MIB variables that match the text string that you entered.
- If you are not using the wildcard character, make sure that you enter the full MIB variable name.

Editing a Template

You can make changes to the selection of MIB variables in an existing user-defined template using the Edit button in the List of Templates dialog box. You cannot edit the template name or select another MIB file from the Show MIB list.

When you modify the template by adding new variables, or by removing existing variables, the changes are reflected in all active Pollers associated with the template.

- You cannot edit System-defined templates.
- You can edit only one template at a time. If you select multiple templates using the check box, the Edit button is disabled.

To edit a template:

Step 1  Select Monitor > Performance Settings > Setup > Templates.
        The List of Templates dialog box appears.
Step 2  Select the template by checking the corresponding check box.
Step 3  Click Edit.
        The Select MIB Variables page appears, displaying the MIB Variables dialog box.
Step 4  Make the necessary selections to the MIB variables from the MIB tree.
        You can also add additional MIB variables to the template. You cannot add MIB variables from two different tables.
Chapter 4    Performance Management

Managing Templates

Step 5  Click Next.
The MIB Alias Name dialog box appears.
To easily identify the MIB variable, use an alias name.
See Creating a Template for the description of the fields that appear in the MIB Alias Name dialog box.

Step 6  Click Finish.
A message appears confirming that the template is updated successfully.
The List of Templates dialog box appears, displaying the template.

Deleting a Template

You can delete an existing user-defined template using the Delete button on the List of Templates dialog box. You can select and delete multiple user-defined templates using the check box selection. You cannot delete System-defined templates.
The Delete button is enabled only after you have selected the template.

• Before deleting a template, you are prompted to confirm the action, as you cannot restore a template that is deleted from the database.
• You cannot delete a template if it is part of any Poller. If you try to do so, an appropriate error message appears.
• If you select both System-defined and user-defined templates for deletion, an appropriate message appears prompting you to delete only the user-defined templates.

To delete a template:

Step 1  Select Monitor > Performance Settings > Setup > Templates.
The List of Templates dialog box appears.

Step 2  Select a template by checking the check box.
You can select multiple User-defined templates by checking the respective check box.
If you select both System-defined and User-defined templates for deletion, you will be prompted to delete only the User-defined templates.

Step 3  Click Delete.
A message appears prompting you to confirm the deletion.

Step 4  Click OK to delete the User-defined template.
Or
Click Cancel to cancel the operation.
The List of Templates dialog box appears.
Copying a Template

You can copy and create a new template from an existing System-defined or User-defined template using the Copy button on the List of Templates dialog box.

To copy from an existing template:

Step 1 Select Monitor > Performance Settings > Setup > Templates.
   The List of Templates dialog box appears.
Step 2 Select the template by checking the appropriate check box.
Step 3 Click Copy.
   The Select MIB Variables page appears, displaying the MIB Variables dialog box.
Step 4 Enter a name in the Template Name field.
Step 5 Make the necessary MIB variable selection from the MIB tree.
Step 6 Click Next.
   The MIB Alias Name dialog box appears. To easily identify the MIB variable, use an alias name.
See Creating a Template for the description of the fields that appear in the MIB Alias Name dialog box.
Step 7 Click Finish.
   A message appears confirming that the template is created successfully.
   The List of Templates dialog box appears, displaying the template.

Exporting a Template

You can export a template to a directory path. The exported file is in XML format. You can export both System-defined templates and User-defined templates.

To export a template:

Step 1 Select Monitor > Performance Settings > Setup > Templates.
   The List of Templates dialog box appears.
Step 2 Select the template you want to export by checking the corresponding check box.
Step 3 Click Export.
   The Export Template dialog box appears.
   You can either:
   a. Enter a descriptive name in the File Name field to which the template is exported.
   b. Click OK to export and close the Export Template dialog box.
   Or
   a. Click Browse to select an existing filename to which the template is exported.
   The Server Side File Browser dialog box appears.
   b. Select an existing filename from the directory content area.
c. Click OK to close the Server Side File Browser dialog box.

d. Click OK to export and close the Export Template dialog box.

   A pop-up message appears with the following message: File name already exists. Are you sure you want to overwrite it?

   Click OK to overwrite the existing file with the new template contents or Cancel to select another filename by clicking Browse.

If you click OK, the template is exported to the specified directory location.

A message appears confirming that the template is successfully exported.

Table 4-16 describes the fields in the Server Side File Browser.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>The directory path to export the template file. You are allowed to export the template only to the following directory path:</td>
</tr>
<tr>
<td></td>
<td>• In Windows, $NMSROOT\hum\templateEx</td>
</tr>
<tr>
<td></td>
<td>• In Solaris or Soft Appliance, $NMSROOT/hum/templateEx</td>
</tr>
<tr>
<td></td>
<td>$NMSROOT is the default Cisco Prime LMS installation directory.</td>
</tr>
<tr>
<td>Directory Content</td>
<td>Displays the files and folders in the directory path. You can select a file or a folder in the directory path.</td>
</tr>
</tbody>
</table>

**Importing a Template**

You can import a template from the location where the LMS application is installed. The imported data need to be in XML format.

To import a template:

**Step 1** Select Monitor > Performance Settings > Setup > Templates.

The List of Templates dialog box appears.

**Step 2** Click Import.

The Import Template dialog box appears.

**Step 3** Click Browse to select the directory path where the template file is located.

The Server Side File Browser dialog box appears.

See Exporting a Template for the description of the fields that appear in the Server Side File Browser dialog box.

**Step 4** Locate and select the template file from the directory location.
Step 5  Click OK to close the Server Side File Browser dialog box.

Step 6  Click OK to import and close the Import Template dialog box.

A message appears confirming that the template is successfully imported.
The List of Templates dialog box appears, displaying the template.

Filtering Template List

This section describes how you can use the Show option to filter the template information based on a specific criteria.

To filter a template:

Step 1  Select Monitor > Performance Settings > Setup > Templates.
The List of Templates dialog box appears.

Step 2  Select a criteria from the drop-down list.

Step 3  Enter the data to be filtered.

Step 4  Click Show.
The List of Templates dialog box appears, displaying the template information based on filter criteria.

Table 4-17 describes the criteria you can use for filtering.

<table>
<thead>
<tr>
<th>Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
</table>
| Template Name       | Select Template Name and enter the data. You can use any of the following methods to filter by entering:  
  • Complete template name  
  • Any three consecutive characters of the Template name  
  • Any wildcard characters of the Template name (such as *a, a*, *a*) |
| Created By          | Select Created By and enter the name of user who created the template. For example, System or Admin  
  You can use any of the following methods to filter by entering:  
  • Complete username  
  • Any three consecutive characters of the user name |
Viewing Template Details

This section helps you to understand the details of a template such as Template Name, MIB variables used in the template, number of Pollers associated with the template and so on.

You can view the details of a template from the List of Templates dialog box.

To view the details of a template:

| Step 1 | Select **Monitor > Performance Settings > Setup > Templates**.  
The List of Templates dialog box appears. |
| Step 2 | Click on the template name link.  
A pop-up appears, displaying the details of the template.  
**Table 4-18** describes the fields in the Template Details page. |

**Table 4-18** Template Details Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>Displays the template name.</td>
</tr>
</tbody>
</table>
| MIB Variables | MIB variables associated with the template. For example, cpmCPU
total5minRev. |
| Pollers Configured | Displays the Poller name.                    |
| Created By | Name of the user who created the template. For example, System or Admin. |
About Monitoring Dashboards

This section provides an overview of the following dashboards:

- Monitoring Dashboard
- EnergyWise Dashboard
- Identity Dashboard

See *Getting Started with Cisco Prime LAN Management Solution 4.1* for information on:

- List of portlets and dashboards in LMS
- Changing the look and feel of the portlets.
- Adding portlets to dashboards
- Refreshing portlets

**Monitoring Dashboard**

You can access the Monitoring dashboard using:

- **My Menu > Default Dashboards > Monitoring**
- **Monitor > Dashboards > Monitoring**

Monitoring Dashboard has the following portlets:

- N-Hop View
- High Severity Faults
- Syslog Summary
- Syslog Alerts
- Alerts Summary
- Fault Events Summary
- IPSLA Violation Summary
- Syslog Messages
- Top N Syslog Sender
- Highest Latency
- Highest Jitter
- Lowest Availability
- IPSLA Availability
- CPU Utilization Summary Chart
- Custom Top /Bottom N Records
- Device Availability
- Interface Availability
- Histo-Graph It
- Live Graph-It
- TOP-N Interface Discards
- TOP-N Interface Errors
- TOP-N Interface Utilization
- TOP-N Memory Utilization
- TOP-N-POE Utilization
- TOP-N CPU Utilization
- Performance Threshold Information
- Performance TrendWatch Information
- TOP-N Environmental Temperature
- NAM Top N Statistics Portlet
- NAM Attribute Value
- IPSLA Collector Information
- IPSLA Device Categorization
EnergyWise Dashboard

You can access the EnergyWise dashboard using:
- **Work Centers > EnergyWise > Dashboard**
- **My Menu > Default Dashboards > EnergyWise**
- **Monitor > Dashboards > EnergyWise**

The various EnergyWise portlets are:
- EnergyWise - Power Consumption
- EnergyWise - Total Savings Graph
- EnergyWise - Savings Trend Graph
- EnergyWise - Current Power Consumption
- EnergyWise - Policy Override
- EnergyWise - Policy Groups

See *Technology Work Centers in Cisco Prime LAN Management Solution 4.1* for more information.

Identity Dashboard

You can access the Identity dashboard using:
- **Work Centers > Identity > Dashboard**
- **My Menu > Default Dashboards > Identity**
- **Monitor > Dashboards > Identity**

The various Identity portlets are:
- Identity - Security Modes Distribution
- Identity - 802.1x Agentless
- Identity - Authenticated Users
- Identity - Authentication Trend
- Identity - Authorization Trend
- User Tracking Summary

See *Technology Work Centers in Cisco Prime LAN Management Solution 4.1* for more information.
Monitoring Dashboard

This chapter explains the list of default dashboards in Monitoring Dashboard (see List of Default Portlets in Monitoring Dashboard) and the following portlets in the dashboard:

- N-Hop View
- High Severity Faults
- Syslog Summary
- Syslog Alerts
- Alerts Summary
- Fault Events Summary
- IPSLA Violation Summary
- Syslog Messages
- Top N Syslog Sender
- Highest Latency
- Highest Jitter
- Lowest Availability
- IPSLA Availability
- CPU Utilization Summary Chart
- Custom Top /Bottom N Records
- Device Availability
- Interface Availability
- Histo-Graph It
- Live Graph-It
- TOP-N Interface Discards
- TOP-N Interface Errors
- TOP-N Interface Utilization
- TOP-N Memory Utilization
- TOP-N-POE Utilization
- TOP-N CPU Utilization
- Performance Threshold Information
List of Default Portlets in Monitoring Dashboard

The following portlets appear by default in the Monitoring Dashboard:

- Performance TrendWatch Information
- TOP-N Environmental Temperature
- NAM Top N Statistics Portlet
- NAM Attribute Value
- IPSLA Collector Information
- IPSLA Device Categorization

See *Getting Started with Cisco Prime LAN Management Solution 4.1* for the list of dashboards and portlets in LMS 4.1.

In a multi-server setup, all performance management portlets display the data specific to that server only.

List of Default Portlets in Monitoring Dashboard

The following portlets appear by default in the Monitoring Dashboard:

- High Severity Faults
- Syslog Summary
- Syslog Alerts
- Alerts Summary
- Fault Events Summary
- Syslog Messages
- Top N Syslog Sender
- Device Availability
- Interface Availability
- TOP-N Interface Discards
- TOP-N Interface Errors
- TOP-N Interface Utilization
- TOP-N Memory Utilization
- TOP-N CPU Utilization
- N-Hop View
- IPSLA Violation Summary
- Histo-Graph It
- Live Graph-It

To see the other portlet details, you must add them to the Monitoring Dashboard.

See *Getting Started with Cisco Prime LAN Management Solution 4.1* for information on:

- Changing the look and feel of the portlets.
- Adding portlets to dashboards
- Refreshing portlets
N-Hop View

N-Hop View portlet is an HTML based light weight feature. This is much faster than the regular Topology services.

This portlet displays an N-hop view from a specified device. It should be used to view a limited set of devices.

Using N-Hop View, you can:

- Select any device from the map and choose to see the Device dashboard report is launched. It displays performance details for the device.
- Select any link from the Topology map and choose to see the Interface Report for that particular link displaying data for the last one hour.
- Select any device to cross-launch Software Distribution and NetConfig page
- Select any IPSLA capable device, right click and choose Show Collector or Create Collector. The corresponding Collector Management page is launched. You can either create new collectors or view existing ones for Layer 3 devices. An error appears if you do this on a Layer 2 device.
- View the details of Fault History Report and Fault Alerts
- Access a device using Telnet. To do so, choose a device, right click and choose Telnet.
- View the following information in the map:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>IP Address of the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>device name</td>
<td>Name of the device</td>
</tr>
<tr>
<td>sysName</td>
<td>sysName</td>
</tr>
<tr>
<td>sysContact</td>
<td>Contact person for that device</td>
</tr>
<tr>
<td>sysLocation</td>
<td>Physical location of the device</td>
</tr>
<tr>
<td>sysOID</td>
<td>Value of the System Object Identifier MIB variable of the device</td>
</tr>
</tbody>
</table>
- To view information, right click anywhere on the map and select the required value. The selected information is displayed for all devices.

- To hide the displayed information, right click anywhere on the map and select **Show/Hide Labels**. Move the mouse over the label to display this relevant information.

You can drag the labels anywhere inside the map. To set it to its original position, right click in the map and choose **Reset Draggables**.

You can view the details about a single device or link.

- Click the link **Show Properties** at the top right corner. (It toggles between Show Properties and Hide Properties). You can also move the IP address of the devices using the cursor.

- Choose a device or link. Properties of the device or link are displayed as shown in Table 6-1.

### Table 6-1 Device and Link Details of N-Hop Portlet

<table>
<thead>
<tr>
<th>Device Details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device name</td>
<td>Name of the device</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the device</td>
</tr>
<tr>
<td>status</td>
<td>Indicates if the device is up or down</td>
</tr>
<tr>
<td>imageVer</td>
<td>Version details of the image installed in the device</td>
</tr>
<tr>
<td>sysLocation</td>
<td>Physical location of the device</td>
</tr>
<tr>
<td>sysName</td>
<td>sysName</td>
</tr>
<tr>
<td>sysContact</td>
<td>Contact person for that device</td>
</tr>
<tr>
<td>sysOID</td>
<td>Value of the System Object Identifier MIB variable of the device</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Link Details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Status</td>
<td>Indicates if the link is up or down</td>
</tr>
<tr>
<td>Device IP</td>
<td>IP Address of the device. Shown for both devices between which the link is configured.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface in the device. Shown for both devices between which the link is configured.</td>
</tr>
</tbody>
</table>

You can click the Configuration icon in the N-Hop View to configure the portlet.

To configure the N-Hop View portlet:

**Step 1**

From the banner, click the Add Portlet icon at the top right corner of the page.

A popup window appears. To expand and collapse the sections, click the arrow next to the section title. Each section in this window contains a list of portlets.

**Step 2**

Click CiscoWorks and select **Monitor**.

A list of portlets appears.

**Step 3**

Click **Add** against the N-Hop View portlet.

The configuration screen is displayed.
Step 4  Enter the IP address or the Device name of the root device in the Root Device field.
If the device you specify is not managed by LMS, it will display an error message such as “The root
device you specified is not managed by LMS”

Step 5  Enter the number of hops in the Hop count field.
The Network Topology map is drawn for the specified number of hops.

Step 6  Add the device to the critical device poller by checking the Poll Devices check-box.
LMS polls the network periodically. If you need to monitor the status of a certain device more frequently,
add it to the critical device poller.
This device is removed from the critical poller list when you close the N-Hop View portlet window.

Step 7  Check the Show Fault Monitor Alerts check box to display the Fault Alerts.
- Check the Critical check box to display only the critical alerts.
- Check the Warning check box to display only the warning alerts.
- Check the Informational check box to display only the informational alerts.
You can also check the Critical, Warning, and Informational check boxes to display all the critical,
warning and informational alerts.

Step 8  Select the time interval from the Refresh Every drop-down list. The interval can be either in minutes or
hours.
By default, the portlet refreshes the topology map every 2 minutes. If you set the time interval, it
refreshes accordingly. For every refresh, the data is fetched from the last polling cycle of the critical
device poller.

Step 9  Click Save to view the portlet with the configured settings.

---

Note  You can also add this portlet to other application and view it.

---

**High Severity Faults**

In the High Severity Faults portlet, you can view the details of high severity faults.
The High Severity Faults portlet provides a consolidated real-time view of the operational status of your
network. When a fault occurs in the network, LMS generates an event. All events occurring on the same
device are rolled into a single fault.
You can also use Notification Services to change the standard event name to a more meaningful one. Click the High Severity Faults portlet header link to view the details of faults in Fault Monitor.

To configuring High Severity Faults:

**Step 1** Move the mouse over the title bar of the High Severity Faults portlet to view the icons.

**Step 2** Click the Configuration icon.

You can:
- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed Refresh time.
- Select the number of faults to be displayed in the portlet from the No. of Faults to be Displayed drop-down list.

For example, if you select the number of faults as 3, the details of any three alerts are displayed in the portlet.

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

Table 6-2 lists High Severity Faults portlet details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Displays the respective icon for the severity levels of the faults: Critical, Warning, and Informational</td>
</tr>
<tr>
<td>Status</td>
<td>Lists the fault status such as:</td>
</tr>
<tr>
<td></td>
<td>- Active—Fault is active. All suspended devices remain active.</td>
</tr>
<tr>
<td></td>
<td>- Cleared—Fault is no longer alive. When the fault has been in the Cleared state for 20 minutes, it expires and it is removed from the display.</td>
</tr>
<tr>
<td></td>
<td>- Acknowledged—Fault was manually acknowledged by a user from the Fault Monitor page.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Device name or IP address. You can click the Device Name link to navigate to the Device Center (Troubleshooting workflow) page.</td>
</tr>
<tr>
<td>Event Name</td>
<td>Identifies event name. Events are sorted based on the time of the most recent event status changes.</td>
</tr>
<tr>
<td>Component Name</td>
<td>Device component name.</td>
</tr>
<tr>
<td>Creation Time</td>
<td>Date and time when event appeared</td>
</tr>
<tr>
<td>Owned By</td>
<td>Name of the user owning the fault</td>
</tr>
</tbody>
</table>

You can click the name in the title bar to navigate directly to the Fault Monitor page.

**Syslog Summary**

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

The portlet displays the top 10 syslog summary reports.
There are options to view the graph as a chart or as a grid.

To configure the Syslog Summary portlet:

**Step 1** Move the mouse over the title bar of the High Severity portlet to view the icons.

**Step 2** Click the Configuration icon.

You can:
- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed refresh time.
- Select the number of rows to be displayed in the portlet from the No. of Rows to be Displayed drop-down list.
- Select the Show graph check box.

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

---

### Syslog Alerts

In the Syslog Alerts portlet you can view the error messages, or informational messages about events such as exceptions, and device configuration changes.

To configure the Syslog Alerts portlet:

**Step 1** Move the mouse over the title bar of the High Severity portlet to view the icons.

**Step 2** Click the Configuration icon.

You can:
- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed refresh time.
- Select the number of records to be displayed in the portlet from the Show Last Records drop-down list.
- To view the exception period report, enable the Only Exception period report check box.

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

---

**Table 6-3** lists the Syslog Alert portlet details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Displays the device name.</td>
</tr>
<tr>
<td>Emergency</td>
<td>Number of emergency messages in the last 24 hours.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Alert state in the last 24 hours.</td>
</tr>
<tr>
<td>Critical</td>
<td>Critical state in the last 24 hours.</td>
</tr>
</tbody>
</table>
You can click the portlet name in the title bar to navigate directly to the Report Generator page.

**Alerts Summary**

The Alerts and Summary portlet will capture the alerts and notification details of various LMS applications. This will provide a launch point for various alarms and notification events within LMS.

The Alerts summary portlet will provide the total number of alerts or events for the following in the LMS: applications.

- Discrepancies
- Best Practices Deviations
- High Severity Alerts
- S0, S1, S2 Syslog Alerts
- IPSLA Violations
- Threshold Violations

You can click the alerts count given in the portlet to view the details of the respective application. However, you cannot change the Refresh interval. This is because the Refresh interval is set to five minutes.

**Fault Events Summary**

The Fault Events Summary portlet displays the information about the events that were encountered on the devices based on the severity such as critical or informational.

Table 6-3 lists the Fault Events Summary portlet details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events Name</td>
<td>Name of the event such as Operationally Down, OutofRange, HighErrorRate, Unresponsive and so on.</td>
</tr>
<tr>
<td>Severity</td>
<td>Type of severity of the device such as critical, or informational.</td>
</tr>
<tr>
<td>No. of devices</td>
<td>Total number of devices affected by the severity.</td>
</tr>
</tbody>
</table>
To configure Fault Events Summary portlet:

**Step 1**
Move the mouse over the title bar of the Fault Events Summary portlet to view the icons.

**Step 2**
Click the Configuration icon.

**Step 3**
Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed Refresh time.

**Step 4**
Expand the icon against the Critical check box.
It displays the list of Critical events. You can select the check box against the respective critical events to display the events in the portlet. Expand the icon against the Informational check box.
It displays the list of Informational events. You can select the check box against the respective informational events to display the events in the portlets.

**Note**
You can select a maximum of 20 events to be displayed in the portlet.

**Step 5**
Click **Save** to view the portlet with the configured settings such as the Events Name, Severity and the No.of Devices.
Click the device count link against the corresponding Events to navigate to the Alerts and Activities page.

---

**IPSLA Violation Summary**

IPSLA Violation Summary portlet displays the Violation summary count of collectors.
This portlet displays seven Violation Summary details such as rfactor, MOS, ICPF, Errors, Latency, Jitter and others.
You can configure the refresh time and the violation summary details for rfactor, MOS, ICPF, Errors and so on.
To configure IPSLA Violation Summary Details portlet:

**Step 1**
Click the configuration icon in the IPSLA Violation Summary portlet.
The configuration page appears.

**Step 2**
Expand the group and select the check box against each variable.

**Step 3**
Click the Save button.
The selected variable appears in the portlet.

**Note**
In the IPSLA Violation Summary reports, the source device and the target device displays only the IP Address and not the Display Name.
Syslog Messages

The Syslog Message portlet displays the top N Syslog messages of the last 24 hours.
You can choose the custom reports type from the drop-down box. The portlet also displays the details
such as device name, time stamp, severity.

To configure Syslog Message portlet:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Move the mouse over the title bar of the Syslog Messages portlet to view the icons.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Configuration icon.</td>
</tr>
<tr>
<td>3</td>
<td>Select the Auto Refresh check box to auto refresh the portlet content at the set time.</td>
</tr>
</tbody>
</table>
| 4    | Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items
     in the portlet get refreshed at the changed Refresh time. |
| 5    | Select the message from the Message drop-down list. |
| 6    | Select the number of rows to be displayed in the portlet from the No.of Rows to be Displayed drop-down
     list. |
| 7    | Select the optional columns check box such as Mnemonic, Facility and Message to be displayed in the
     portlet. |
| 8    | Select the severity from the Severity check box. |
| 9    | Click **Save** to view the configured portlet with the changed settings. |

The items in the portlet get refreshed at the changed Refresh time.

**Table 6-5** lists the Syslog Message details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Refresh</td>
<td>Select the Auto Refresh to refresh the details in the portlet at the set time.</td>
</tr>
<tr>
<td>Refresh Every</td>
<td>Select the hour and minute from the Refresh Every drop-down list.</td>
</tr>
<tr>
<td>Messages</td>
<td>Select the messages to be displayed in the portlet from the Message drop-down list.</td>
</tr>
<tr>
<td>No.of Rows to be displayed</td>
<td>Select the number of rows to be displayed in the portlet from the drop-down list.</td>
</tr>
<tr>
<td>Optional columns — You can select any of the check boxes such as Mnemonic, Facility or Message</td>
<td>Select the optional check box such as Mnemonic, Facility or Message.</td>
</tr>
</tbody>
</table>
|                           | • If you select the Mnemonic check box, the mnemonic details such as CONFIG_1, RESTART and others
   will be displayed in the column. | |
|                           | • If you select the Facility check box, the facility details will be displayed in the column.    |
|                           | • If you select the Message check box, the syslog message will be displayed in the column.       |
| Severity                  | Check the severity from the severity check box.                                                |
Top N Syslog Sender

The Top N Syslog Sender portlet displays the total number of Syslogs during the last 24 hours, based on the severity type that you configured.

To configure Top N Syslog Sender portlet:

Step 1  Move the mouse over the title bar of the Top N Syslog Sender portlet to view the icons.
Step 2  Click the Configuration icon.
Step 3  Select the Auto Refresh check box to auto refresh the portlet content at the set time.
Step 4  Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the Refresh time you set.
Step 5  Select the message from the Message drop-down list.
Step 6  Select the number of rows to be displayed in the portlet from the No.of Rows to be Displayed drop-down list.
Step 7  Select the type of severity to be displayed in the portlet from the Severity check box.
Step 8  Click Save to view the configured portlet with the changed settings.

Table 6-6 lists the Top N Syslog Sender portlet details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Displays the device name.</td>
</tr>
<tr>
<td>Severity</td>
<td>Severity that has been configured on the portlet. For example, if you have checked the Severity 1 and Severity 2 check boxes, then only S1 and S2 will appear in the portlet.</td>
</tr>
<tr>
<td>Count</td>
<td>Total number of devices with their severity numbers. For example, if Device A has the following number of severity: Device A: S1=2 Device A: S2=3 Then total number of severity in Device A is 5. You can click the number to view the severity details.</td>
</tr>
</tbody>
</table>

Highest Latency

In the Highest Latency portlet, you can view the time taken for an IP packet to travel from source to target and back.

Latency is defined as the time taken for an IP packet to travel from source to target and back.

The collectors (by default there are five collectors) with higher latency are listed first, followed by other collectors. This arrangement helps the administrator to closely monitor the collectors with highest latency.
To configure Highest Latency:

**Step 1** Move the mouse over the title bar of the Highest Latency portlet to view the icons.

**Step 2** Click the Configuration icon.

**Step 3** Select the Auto Refresh check box to auto refresh the portlet content at the set time.

**Step 4** Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the Refresh time you set.

**Step 5** Select the number of collectors to be displayed from the No.of Collectors to be Displayed drop-down list. For example, if you select 5, the details of five collectors are displayed in the portlet.

**Step 6** Click **Save** to view the configured portlet with the changed settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector Name</td>
<td>Name of the collector.</td>
</tr>
<tr>
<td>Operation Type</td>
<td>Lists the type of IPSLA operations.</td>
</tr>
<tr>
<td>Latency</td>
<td>Time taken for an IP packet to arrive from the Source to Target and back.</td>
</tr>
</tbody>
</table>

Table 6-7 lists the Highest Latency portlet details.

**Note**

You can click the value of latency to view the Real time Latency Graph details in the IPSLA Monitoring function.

You can click the portlet name in the title bar to navigate directly to the corresponding page in the application.

**Highest Jitter**

The inter-packet delay between any two consecutive data packets sent from the source to target router and back is referred to as Jitter.

The collectors with the highest jitter are listed first, followed by other collectors. This arrangement helps the Administrator to monitor closely the collectors with highest jitter.

To configure Highest Jitter:

**Step 1** Move the mouse over the title bar of the Highest Jitter portlet to view the icons.

**Step 2** Click the Configuration icon.

**Step 3** Select the Auto Refresh check box to auto refresh the portlet content at the set time.

**Step 4** Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the Refresh time you set.
Step 5 Select the number of collectors to be displayed from the No. of Collectors to be Displayed drop-down list. For example, if you select 7, the details of seven collectors are displayed in the portlet.

Step 6 Click Save to view the configured portlet with the changed settings.

Table 6-8 lists the Highest Jitter portlet details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector Name</td>
<td>Name of the collector.</td>
</tr>
<tr>
<td>Operation Type</td>
<td>Type of operation.</td>
</tr>
<tr>
<td>SD Jitter (Source Destination Jitter)</td>
<td>Source destination jitter count.</td>
</tr>
<tr>
<td>DS Jitter (Destination Source Jitter)</td>
<td>Destination source jitter count.</td>
</tr>
</tbody>
</table>

Note You can click the value of the count of the SD Jitter or DS Jitter to view Real time Latency Graph details in IPSLA Monitoring function.

You can click the portlet name in the title bar to navigate directly to the corresponding page in the application.

Lowest Availability

Checks the reachability of the target device from the source router using the latency information. The availability is reported in percentage.

The Lowest Availability portlet measures the availability of services such as FTP, DHCP, HTTP, TCP Connect, RTP, DNS, ICMP, UDP, and DSLw on the target device.

The collectors are listed in ascending order of availability to help the administrator closely monitor the collectors with lowest availability.

To configure Lowest Availability:

Step 1 Move the mouse over the title bar of the Lowest Availability portlet to view the icons.

Step 2 Click the Configuration icon.

Step 3 Select the Auto Refresh check box to auto refresh the portlet content at the set time.

Step 4 Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the Refresh time you set.

Step 5 Select the number of collectors to be displayed from the No. of Collectors to be Displayed drop-down list. For example, if you select 7, the details of seven collectors are displayed in the portlet.

Step 6 Click Save to view the configured portlet with the changed settings.
Table 6-9 lists the Lowest Availability portlet details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector Name</td>
<td>Name of the collector.</td>
</tr>
<tr>
<td>Operation Type</td>
<td>Lists the IPSLA operation such as ICMP Jitter and so on.</td>
</tr>
<tr>
<td>Availability Percentage</td>
<td>Availability of target or service in percentage.</td>
</tr>
</tbody>
</table>

You can click the portlet name in the title bar to navigate directly to the corresponding page in the application.

**IPSLA Availability**

The Availability Dashboard will display the following details:
- Operation Types
- Number of Collectors
- Availability percentage ranges.

If you click the Availability percentage number, it displays the Availability Report.

The Availability Report page contains the following details:
- Collector Name — The name of the collector.
- Source Device — The name of the source device. However, the source device displays only the IP address and not the display name.
- Target Device — The name of the target device. However, the Target device displays only the IP address and not the display name.
- Operation — The name of the operation.
- Availability Percentage — Details of the availability percentage.

You can customize and configure the IPSLA Availability Dashboard portlet.

In the configuration screen, the Operation Types and User Defined Collector Groups are displayed.
- To view the Operation Types, expand the button.
- To select the Operation Types, check the check box adjacent to the Operation Types

Based on configuration this portlet will display both selected operation types groups and selected user defined collectors groups.

If no operation type groups and user defined collector groups are created, then the portlet will display the error message.
CPU Utilization Summary Chart

The CPU Utilization Summary Chart portlet displays the CPU usage details of the devices monitored using LMS Device Performance Management functionality. The CPU Utilization data is summarized and displayed in a pie-chart for all the devices for a specific time interval.

You can click the pie-chart to navigate to the CPU Utilization report. The portlet also displays the total number of CPU instances for CPU utilization.

If there is no data in the CPU Utilization Summary Chart portlet, it displays the following message:

No data found. Click here to configure pollers. Please check HUMPortal.log for more details.

You can click the here link to launch the Poller Management page. The Poller Management page allows you to configure pollers.

If there is data in the CPU Utilization Summary Chart portlet, it displays the following message along with the data.

Click here to configure more pollers.

You can click the here link to launch the Poller Management page. The Poller Management page allows you to configure more Pollers.

Table 6-10 displays the color and CPU Utilization summary status of the device.

<table>
<thead>
<tr>
<th>Color</th>
<th>CPU Utilization Summary Status in percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>CPU utilization from 0 to 10%</td>
</tr>
<tr>
<td>Yellow</td>
<td>CPU utilization from 10 to 30%</td>
</tr>
<tr>
<td>Orange</td>
<td>CPU utilization from 30 to 80%</td>
</tr>
<tr>
<td>Red</td>
<td>CPU utilization from 80 to 100%</td>
</tr>
</tbody>
</table>

You can set the time interval as 1 hour, 1 day, 7 days, 15 days, or 30 days. However by default the time interval is 1 hour.

You can customize and configure the CPU Utilization Summary Chart portlet.

To configure the CPU Utilization Summary Chart portlet:

**Step 1** Move the mouse over the title bar of the CPU Utilization Summary Chart portlets.

**Step 2** Click the Configuration icon.

- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the refresh time that you set.
- Select the time interval from the Time Interval drop-down list. The CPU Utilization summary is shown for the selected time interval.

For example, if you select **7 Days**, the details of the CPU utilization for the last seven days is displayed.

**Step 3** Click Save to view the portlet with the configured settings.
Custom Top /Bottom N Records

You can create a portlet for custom template MIB variable. This portlet will enable you to view the highest as well as the lowest number of reports on user-defined templates for which pollers have been created.

This is a multi-instance portlet.

For example, if you monitor a device for the tcpMaxConn using the user-defined templates for 15 devices, you will see the highest number of records and the lowest number of records for this object.

This will be retrieved in the custom portlet where you can specify to show the top 10 records based on the tcpMaxConn values or bottom 10 records based on the tcpMinConn values.

Currently Top N/Bottom N Records reports are available only for all templates.

Table 6-11 displays the Custom Top/Bottom N Records details.

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Refresh</td>
<td>Check the Auto Refresh check box if you want to auto-refresh the configuration details.</td>
</tr>
<tr>
<td>Refresh Every</td>
<td>Select the hour and minute from the Refresh Every drop-down list.</td>
</tr>
<tr>
<td>Template Name</td>
<td>Select the template name from the template drop-down list. For example, Custom template.</td>
</tr>
<tr>
<td>Variable Name</td>
<td>Select the variable name from the Variable Name drop-down list. For example, IFOutErrors, IFOutOctets and so on.</td>
</tr>
<tr>
<td>Number of rows to be displayed</td>
<td>Select the rows from the drop-down list. For example, if you select 5, then five rows will be displayed in the portlet.</td>
</tr>
<tr>
<td>Sort Order</td>
<td>Select either Top N or Bottom N radio buttons.</td>
</tr>
<tr>
<td></td>
<td>• If you select Top N, the details are sorted from the highest to the lowest order.</td>
</tr>
<tr>
<td></td>
<td>• If you select Bottom N, then the details are sorted from the lowest to the highest order.</td>
</tr>
<tr>
<td>Time Interval</td>
<td>Select the time interval from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>If you select Time Interval, as 1 day, it will display the configured details for one day.</td>
</tr>
<tr>
<td>Field Display</td>
<td>Select either the Max or Min check box.</td>
</tr>
</tbody>
</table>

To configure Top/Bottom N Records:

**Step 1**  Move the mouse over the title bar of the Top/Bottom N Records portlets.

**Step 2**  Click the Configuration icon.

The Custom-Top/Bottom N Configuration page appears. You can do the following:

• Select the minute and hour from the Refresh Every drop-down list to change the Refresh time.
  The items in the portlet get refreshed at the Refresh time that you set.

• Check the Auto Refresh check box, if you want to auto-refresh the time that you set.

• Select the template name from the Template Name drop-down list.
Device Availability

The Device Availability portlet enables you to view the availability status of the devices in the network. The following information is displayed as a pie chart in the Device Availability portlet.

- Availability of all managed devices in the last \( N \) number of hours or days. Where \( N \) is period of time in hours or days. For example, 5 hours.
- Information about the last polled devices.

If all the devices are reachable, the following message appears in green:

- All devices are available as per the last polled cycle.

If some of the devices are unreachable, the following message appears in red:

- Last Poll Status: For instance, 6 (7 %) devices of 81 are not available.

You can click the pie-chart to navigate to the Device Availability report.

Table 6-12 displays the color and the percentage of the availability status of the device.

<table>
<thead>
<tr>
<th>Color</th>
<th>Availability Status of the Devices in Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Average availability of the device in this category is between 90 to 100%.</td>
</tr>
<tr>
<td>Yellow</td>
<td>Average availability of the device in this category is between 50 to 90%</td>
</tr>
<tr>
<td>Orange</td>
<td>Average availability of the device in this category is between 10 to 50%.</td>
</tr>
<tr>
<td>Red</td>
<td>Average availability of the device in this category is between 0 to 10%.</td>
</tr>
</tbody>
</table>

You can customize and configure the Device Availability portlet.
To configure Device Availability portlet:

**Step 1**  Move the mouse over the title bar of the Device Availability portlets.

**Step 2**  Click the Configuration icon.

You can do any of the following:

- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time.
  The items in the portlet get refreshed at changed refresh time.
- Select the time interval from the Time Interval drop-down list.
  The Device Availability details are shown for the selected time interval.

For example, if you select **7 Days**, the details of the devices available for the last seven days will be displayed.

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

### Interface Availability

The Interface Availability portlet enables you to view the availability status of the interfaces in the network.

The following information is displayed as a pie chart in the Interface Availability portlet.

- Availability of all managed interfaces in the last $N$ number of hours or days.
  Where $N$ is period of time in hours or days. For example, 5 hours.
- Information about the last polled interfaces.

If all the interfaces are reachable, the following message appears in green:

**All interfaces are available as per the last polled cycle**

If some of the interfaces are unreachable, the following message appears in red.

**Last Poll Status:** For instance, 6 (7 %) interfaces of 81 are not available

You can click the pie-chart to navigate to the Interface Availability report.

**Table 6-13** displays the color and the percentage of the availability status of the interfaces.

<table>
<thead>
<tr>
<th>Color</th>
<th>Availability Status of the Interfaces in Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Average availability of the interfaces in this category is between 90 to 100%.</td>
</tr>
<tr>
<td>Yellow</td>
<td>Average availability of the interfaces in this category is between 50 to 90%</td>
</tr>
<tr>
<td>Orange</td>
<td>Average availability of the interfaces in this category is between 10 to 50%.</td>
</tr>
<tr>
<td>Red</td>
<td>Average availability of the interfaces in this category is between 0 to 10%.</td>
</tr>
</tbody>
</table>

You can customize and configure the Interface Availability portlet.
To configure Interface Availability portlet:

**Step 1** Move the mouse over the title bar of the Interface Availability portlets.

**Step 2** Click the Configuration icon.

You can do any of the following:

- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at changed refresh time.
- Select the time interval from the Time Interval drop-down list. The Interface Availability details are shown for the selected time interval.

For example, if you select **7 Days**, the details of the interfaces available for the last seven days will be displayed.

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

---

**Histo-Graph It**

Histo-Graph It portlet enables you to query the information of a particular MIB variable in a device for a specified period of time and generate a graph.

You can select two MIB variables from the configuration field and generate an overlay graph through Histo-Graph It portlet.

Enter the details in the corresponding fields and click the SaveIt button to generate the graph. For more information on field details, see Table 6-14.

After the graph appears, you can select the Export icon to export the data to either CSV or XML format.

The graph is displayed along with a link named Bookmark This Link. Right click and select **Bookmark This Link** to bookmark the graph.

You can also click the pop-out option to view the graph in a separate pop-up window.

The graph that appears in the separate pop-up window will not refresh automatically. Auto refresh option is applicable only to the graph that is part of the Graph It portlet.

To generate Historical Graph:

**Step 1** Go to the Histo-Graph It portlet.

**Table 6-14** describes the fields in the Histo-Graph It portlet.

<table>
<thead>
<tr>
<th>Field /Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Enter the device name. For instance, 3500XL.</td>
</tr>
<tr>
<td>Template Name</td>
<td>Enter the template name from the template drop-down list.</td>
</tr>
<tr>
<td>Available MIB</td>
<td>MIB variable polled for the device. For example, ciscoMemoryPoolFree.</td>
</tr>
<tr>
<td>Available Instances</td>
<td>MIB variable instances available in the device. For example, Processor.</td>
</tr>
</tbody>
</table>
Chapter 6 Monitoring Dashboard

Histo-Graph It

Step 2
Enter a device name in the Device Name field.

The Available MIB drop-down list populates the list of MIB variables polled for the device and select a template from the list.

Step 3
Select a MIB variable from the Available MIB drop-down list.

The Available Instances drop-down list populates the list of MIB variable instances in the device.

Step 4
Select a MIB variable instance from the Available Instances drop-down list.

Step 5
Either:
- Select an interval from the Interval drop-down list.

Or
- Select the start date and end date from the respective fields.

The Date Picker is enabled only when you select Custom for the Interval.

Note
After modifying the time (hh:mm) click the data again on the pop-up calendar to reflect the time change in the portlet.

Table 6-14 Histo-Graph It Portlet

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Variable/Remove Variable</td>
<td>The Add Variable/Remove Variable is a link.</td>
</tr>
<tr>
<td></td>
<td>• If you click <strong>Add Variable:</strong></td>
</tr>
<tr>
<td></td>
<td>You can add more than one Device Name, MIB Variable and Available Instance for another device.</td>
</tr>
<tr>
<td></td>
<td>• If you click <strong>Remove Variable:</strong></td>
</tr>
<tr>
<td></td>
<td>You can remove the Second Variable.</td>
</tr>
<tr>
<td>Interval</td>
<td>Displays the list of intervals as a drop-down list such as:</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Hour</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Day</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Week</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Quarter</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Year</td>
</tr>
<tr>
<td></td>
<td>• Custom</td>
</tr>
<tr>
<td></td>
<td>You can select <strong>Custom</strong> to customize the time interval.</td>
</tr>
<tr>
<td>Start Date</td>
<td>Select the start date from the Date Time picker.</td>
</tr>
<tr>
<td>End Date</td>
<td>Select the end date from the Date Time picker.</td>
</tr>
<tr>
<td>Refresh Every</td>
<td>Select the Refresh hour and minute from the drop-down list.</td>
</tr>
<tr>
<td>Graph It</td>
<td>Click the Graph It button to generate a graph.</td>
</tr>
<tr>
<td></td>
<td>A pop-up window appears displaying a graph with the device details along with the selected MIB variable and its instances.</td>
</tr>
</tbody>
</table>
**Step 6**  Click **Graph It**.
A line graph is generated displaying the historical data for the device.

**Step 7**  Select the **Export** icon at the top right corner to export the data to either CSV or XML formats.

---

**Live Graph-It**

Live Graph-It portlet enables you to do real-time monitoring for any MIB variable that belongs to a device that is managed by Device Credential Repository. You need not create any poller for this device or MIB variable.

Live Graph can be plotted for any devices that are managed in the Device Credential Repository. After you enter the device name, template and variable name, instance querying will be done for that devices. **Table 6-15** lists the Live Graph It portlet details.

**Table 6-15**  *Live Graph It portlet details*

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Every</td>
<td>Select the Refresh time. The refreshing time intervals will be the following:</td>
</tr>
<tr>
<td></td>
<td>• 30 seconds</td>
</tr>
<tr>
<td></td>
<td>• 45 seconds</td>
</tr>
<tr>
<td></td>
<td>• 60 seconds</td>
</tr>
<tr>
<td></td>
<td>However, 30 seconds will be the minimum refreshing interval.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Enter the device name.</td>
</tr>
<tr>
<td>Template Name</td>
<td>Enter the template name.  For example, CPU Utilization.</td>
</tr>
<tr>
<td>Variable Name</td>
<td>Enter the variable name.  For example, cpmCPUTotal5minRev.</td>
</tr>
<tr>
<td>Available Instances</td>
<td>Enter the instance from the drop-down list such as CPU Processor, I/O and so on.</td>
</tr>
</tbody>
</table>

To configure Live Graph It portlet:

**Step 1**  Go to Live Graph It portlet and click the Configuration icon. The configuration screen appears.

**Step 2**  Select the time interval from Refresh Every drop-down list. The refreshing intervals will be 30 sec, 45 sec and 60 sec. The minimum refreshing interval is 30 seconds.

**Step 3**  Enter the device name in the Device Name field.

**Step 4**  Select the template name from the Template Name drop-down list. For example, customtemp

**Step 5**  Select the variable name from the Variable Name drop-down list. For example, IfinDiscards.
Step 6: Select the number of instances from the Available Instances drop-down list.

Step 7: Click the Graph It button.

The monitoring graph will appear as a pop-up browser window.

The graph is displayed along with a link named Link to this page. Right click and select Bookmark This Link to bookmark the graph or you can Add to Favorites, if you are using IE.

### TOP-N Interface Discards

The Interface Discards portlet displays the information about the number of packets discarded in an interface in the particular time interval.

These packets are prevented from being delivered to a high-layer protocol. Such packets are discarded to free up the buffer space.

The Interface IN Discards are the number of inbound packets discarded and the Interface Out Discards are the number of outbound packets that are discarded.

If there is no data in the TOP-N Interface Discard portlet, it displays the following message:

No data found. Click here to configure pollers. Please check HUMPortal.log for more details.

You can click the here link to launch the Poller Management page. The Poller Management page allows you to configure pollers.

If there is data in the TOP-N Interface Discard portlet, it displays the following message along with the data:

Click here to configure more pollers.

You can click the here link to launch the Poller Management page. The Poller Management page allows you to configure more pollers.

Table 6-16 displays the Interface Discards portlet details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface IN Discards</td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device. For example, 3500XL.</td>
</tr>
<tr>
<td></td>
<td>You can click the Device Name link to launch the Device Center page.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interfaces such as Gigabit Ethernet 1/1 (Gi3/3), Gigabit Ethernet 5/7 (Gi5/7) and so on.</td>
</tr>
<tr>
<td></td>
<td>You can click the Interface link to launch the Interface report page.</td>
</tr>
<tr>
<td>IFInDiscards (packets/sec)</td>
<td>Number of packets discarded per second.</td>
</tr>
</tbody>
</table>
You can customize and configure the Interface Discard portlet.

To configure Interface Discards portlet:

**Step 1** Move the mouse over the title bar of the Interface Discards portlet to view the icons.

**Step 2** Click the configuration icon.

You can:

- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed refresh time.
- Select the number of rows to be displayed in the portlet from the No. of rows to be displayed drop-down list.
  
  For example, if you select 5, five rows will be displayed in the portlet.
- Select the time interval from the Time Interval drop-down list.
  
  For example, if you select 7 Days, the details of the interface discards for the last seven days will be displayed.

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

### Table 6-16  TOP-N Interface Discards Portlet Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface OUT Discards</td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device. For example, 3500XL. The display name is the name you enter in the Device Center page. You can click the Device Name link to launch the Device Center page.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interfaces such as Gigabit Ethernet 1/1 (Gi3/3), Gigabit Ethernet 5/7 (Gi5/7) and so on. You can click the Interface link to launch the Interface report page.</td>
</tr>
<tr>
<td>IFOut Discards (pkts/sec)</td>
<td>Number of packets discarded each second.</td>
</tr>
</tbody>
</table>

You can customize and configure the Interface Discard portlet.

To configure Interface Discards portlet:

**Step 1** Move the mouse over the title bar of the Interface Discards portlet to view the icons.

**Step 2** Click the configuration icon.

You can:

- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed refresh time.
- Select the number of rows to be displayed in the portlet from the No. of rows to be displayed drop-down list.
  
  For example, if you select 5, five rows will be displayed in the portlet.
- Select the time interval from the Time Interval drop-down list.
  
  For example, if you select 7 Days, the details of the interface discards for the last seven days will be displayed.

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

### TOP-N Interface Errors

The Top-N Interface Errors portlet displays the information about the number of errors in an interface.

The Top-N Interface Errors display information on devices having highest interface errors as IfInError and IfOutError.

The Interface IN Errors are the number of inbound packets with the errors and the Interface Out Errors are the number of outbound packets with errors.

If there is data in the TOP-N Interface Errors portlet, it displays the following message:

**No data found. Click here to configure pollers. Please check HUMPortal.log for more details.**

You can click the *here* link to launch the Poller Management page. The Poller Management page allows you to configure pollers.
If there is data in the TOP-N Interface Errors portlet, it displays the following message along with the data:

Click here to configure more pollers.

You can click the here link to launch the Poller Management page. The Poller Management page allows you to configure more pollers.

Table 6-17 displays the Interface Errors portlet details.

### Table 6-17 TOP-N Interface Errors Portlet Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface OUT Errors</strong></td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device. For example, 3500XL.</td>
</tr>
<tr>
<td></td>
<td>You can click the Device Name link to launch the Device Center page.</td>
</tr>
<tr>
<td>Interface</td>
<td>Displays the Interfaces such as Gigabit Ethernet 1/1 (Gi3/3), Gigabit Ethernet 5/7 (Gi5/7) and so on.</td>
</tr>
<tr>
<td></td>
<td>You can click the Interface link to launch the Interface report page</td>
</tr>
<tr>
<td>IFOutErrors (pkts/sec)</td>
<td>Packets in each second of the outgoing interface errors.</td>
</tr>
<tr>
<td><strong>Interface IN Errors</strong></td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device. For example, 3500XL.</td>
</tr>
<tr>
<td></td>
<td>You can click the Device Name link to launch the Device Center page.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interfaces such as Gigabit Ethernet 1/1 (Gi3/3), Gigabit Ethernet 5/7 (Gi5/7) and so on.</td>
</tr>
<tr>
<td></td>
<td>You can click the Interface link to launch the Interface report page</td>
</tr>
<tr>
<td>IFInErrors (pkts/sec)</td>
<td>Packets in each second of the incoming interface errors.</td>
</tr>
</tbody>
</table>

You can customize and configure the Interface Errors portlet.
To configure Interface Errors portlet:

**Step 1** Move the mouse over the title bar of the Interface Errors portlet to view the icons.

**Step 2** Click the configuration icon.

You can:
- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed refresh time that you set.
- Select the number of rows to be displayed in the portlet from the No. of rows to be displayed drop-down list.
  
  For example, if you select 10, then ten rows will be displayed in the portlet.
- Select the time interval from the Time Interval drop-down list.
  
  For example, if you select 7 Days, the Interface Errors for the last seven days will be displayed.

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

---

**TOP-N Interface Utilization**

The Interface Utilization portlet displays information on the devices with the highest and lowest utilization based on the configuration.

If there are no data in the TOP-N Interface Utilization portlet, it displays the following message:

*No data found. Click here to configure pollers. Please check HUMPPortal.log for more details.*

You can click the **here** link to launch the Poller Management page. The Poller Management page allows you to configure pollers.

If there is data in the TOP-N Interface Utilization portlet, it displays the following message along with the data:

*Click here to configure more pollers.*

You can click the **here** link to launch the Poller Management page. The Poller Management page allows you to configure more pollers.

**Table 6-18** displays the Interface Utilization portlet details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device. For example, 3500XL. You can click the Device Name link to launch the Device Center page.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interfaces such as Gigabit Ethernet 1/1 (Gi3/3), Gigabit Ethernet 5/7 (Gi5/7) and so on. You can click the Interface link to launch the Interface report page</td>
</tr>
<tr>
<td>Tx%</td>
<td>Percentage of transmitted utilization.</td>
</tr>
<tr>
<td>Rx%</td>
<td>Percentage of received utilization.</td>
</tr>
</tbody>
</table>
The Top N calculations and sorting will be done based on the sum of the percentage of the packets transmitted (Tx%) and the percentage of the packets received (Rx%).

Table 6-19 displays the color and the percentage of transmitted packets.

<table>
<thead>
<tr>
<th>Color</th>
<th>Percentage of Packets Transmitted (Tx%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Transmitted packets from 0 to 50%.</td>
</tr>
<tr>
<td>Yellow</td>
<td>Transmitted packets from 50 to 70%.</td>
</tr>
<tr>
<td>Orange</td>
<td>Transmitted packets from 70 to 90%.</td>
</tr>
<tr>
<td>Red</td>
<td>Transmitted packets from 90 to 100%.</td>
</tr>
</tbody>
</table>

Table 6-20 displays the color and the percentage of the received packets.

<table>
<thead>
<tr>
<th>Color</th>
<th>Percentage of Packets Received (Rx%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Received packets from 0 to 50%.</td>
</tr>
<tr>
<td>Yellow</td>
<td>Received packets from 50 to 70%.</td>
</tr>
<tr>
<td>Orange</td>
<td>Received packets from 70 to 90%.</td>
</tr>
<tr>
<td>Red</td>
<td>Received packets from 90 to 100%.</td>
</tr>
</tbody>
</table>

You can configure and customize the Interface Utilization portlet.

To configure Interface Utilization portlet:

**Step 1** Move the mouse over the title bar of the Interface Utilization portlet to view the icons.

**Step 2** Click the configuration icon.

You can:

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

- Select the number of rows to be displayed in the portlet from the No. of rows to be displayed drop-down list.

  For example, if you select five, then five rows will be displayed in the portlet.

- Select the Sort Order Top N radio button to sort the utilization in ascending order or Bottom N radio button to sort the utilization in descending order.

- Select the time interval from the Time Interval drop-down list.

  For example, if you select 7 Days, the details of the Interface Utilization for the last seven days will be displayed.

**Step 3** Click **Save** to view the portlet with the configured settings.
TOP-N Memory Utilization

The Memory Utilization portlet displays information about the memory usage of all devices. It also displays the device name, instance name and the percentage of minimum, maximum and average memory utilized.

No data found. Click here to configure pollers. Please check HUMPortal.log for more details.

You can click the here link to launch the Poller Management page. The Poller Management page allows you to configure pollers.

If there is data in the TOP-N Memory Utilization portlet, it displays the following message along with the data:

Click here to configure more pollers.

You can click the here link to launch the Poller Management page. The Poller Management page allows you to configure more pollers.

Table 6-21 displays the color and the percentage of the memory utilization of the device.

<table>
<thead>
<tr>
<th>Color</th>
<th>Memory Utilization of the Device in Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Memory utilization of the device from 0 to 50%</td>
</tr>
<tr>
<td>Yellow</td>
<td>Memory utilization of the device from 50 to 70%</td>
</tr>
<tr>
<td>Orange</td>
<td>Memory utilization of the device from 70 to 90%</td>
</tr>
<tr>
<td>Red</td>
<td>Memory utilization of the device from 90 to 100%</td>
</tr>
</tbody>
</table>

Note: The Avg % is displayed by default in the portlet. However, the Max % and Min % have to be configured to view it in the portlet.

Table 6-22 displays the Memory Utilization portlets

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device. For example, 3500XL. You can click the Device Name link to launch the Device Center page.</td>
</tr>
<tr>
<td>Instance Name</td>
<td>Instance name such as DRAM, FLASH, MALLOC, Processor and so on.</td>
</tr>
<tr>
<td>MIN (%)</td>
<td>Percentage of the minimum memory utilized by the device.</td>
</tr>
<tr>
<td>MAX%</td>
<td>Percentage of the maximum memory utilized by the device.</td>
</tr>
<tr>
<td>AVG %</td>
<td>Percentage of average memory utilized by the device.</td>
</tr>
</tbody>
</table>

You can configure and customize the Memory Utilization portlet.
To configure Memory Utilization portlet:

**Step 1** Move the mouse over the title bar of the Memory Utilization portlet to view the icons.

**Step 2** Click the configuration icon. You can:

- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed refresh time that you set.
- Select the number of rows to be displayed in the portlet from the No. of rows to be displayed drop-down list.
  
  For example, if you select 5, then five rows will be displayed in the portlet.
- Select the Max or Min check box to display both the maximum or minimum field in the portlet.
- Select the Time interval from the Time Interval drop-down list.
  
  For example, if you select 1 Hour, then the memory utilization for the last one hour will be displayed.

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

## TOP-N-POE Utilization

The power utilization summary of network devices is displayed as PSE wise and port wise components in the TOP-N-POE Utilization portlet.

In this portlet you can configure components, such as PSE-wise summary and port-wise summary.

This portlet also displays the minimum, maximum and average power utilization of network devices in the LMS.

### Table 6-23  TOP-N-POE Utilization Portlet

<table>
<thead>
<tr>
<th>Fields/Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Refresh</td>
<td>Check the Auto Refresh check box for the data to be refreshed at the given interval.</td>
</tr>
<tr>
<td>Refresh Every</td>
<td>Select the hour and minute from the Refresh Every drop-down list.</td>
</tr>
<tr>
<td>Report</td>
<td>By default, the PSE reports appear. However, you can check Port to view the details.</td>
</tr>
<tr>
<td>No.of Reports to be displayed</td>
<td>Select the number of reports to be displayed in the portlet from the drop down list.</td>
</tr>
<tr>
<td>Sort Order</td>
<td>Select either Top N or Bottom N radio button.</td>
</tr>
<tr>
<td></td>
<td>- Select Top N radio button to sort the utilization in ascending order.</td>
</tr>
<tr>
<td></td>
<td>- Select Bottom N radio button to sort the utilization in descending order.</td>
</tr>
</tbody>
</table>
To configure TOP-N-POE Utilization portlet:

**Step 1** Go to TOP-N-POE Utilization portlet.

**Step 2** Click the configuration icon.

The configuration screen appears.

- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed Refresh time that you set.
- Select the Port check box to view the Port details also in the portlet.
- Select the number of rows to be displayed in the portlet from the No. of rows to be displayed drop-down list.

  For example, if you select **5**, then five rows will be displayed in the portlet.

- Select the Sort Order Top N radio button to sort the utilization in ascending order or Bottom N radio button to sort the utilization in descending order.
- Select the Time interval from the Time Interval drop-down list.

  For example, if you select **1 Hour**, the memory utilization for the last one hour will be displayed.

- Select the Display field check box.

  - If you check the Max check box, only the maximum power utilization or power consumption details will be displayed in the portlet.
  - If you check the Min check box, only the minimum power utilization or power consumption details will be displayed in the portlet.

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

### Table 6-23 TOP-N-POE Utilization Portlet

<table>
<thead>
<tr>
<th>Fields/Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Interval</td>
<td>Select the time interval from the time interval drop-down list.</td>
</tr>
<tr>
<td>Display Fields</td>
<td>Check <strong>Min</strong> or <strong>Max</strong> or both the check boxes.</td>
</tr>
<tr>
<td></td>
<td>• If you check <strong>Min</strong>:</td>
</tr>
<tr>
<td></td>
<td>Only the minimum percentage of power utilization and power consumption</td>
</tr>
<tr>
<td></td>
<td>appears in the portlet.</td>
</tr>
<tr>
<td></td>
<td>• If you check <strong>Max</strong>:</td>
</tr>
<tr>
<td></td>
<td>Only the maximum percentage of power utilization and power consumption</td>
</tr>
<tr>
<td></td>
<td>appears in the portlet.</td>
</tr>
</tbody>
</table>
TOP-N CPU Utilization

The TOP-N-CPU Utilization portlet displays information about the devices that have the highest CPU utilization percentage.

It also displays the device name, CPU instance and percentage of the minimum, maximum and the average CPU memory utilized by the device.

If there is no data in the TOP-N CPU Utilization portlet, it displays the following message:
No data found. Click here to configure pollers. Please check HUMPortal.log for more details.

You can click the here link to launch the Poller Management page. The Poller Management page allows you to configure pollers.

If there is data in the TOP-N CPU Utilization portlet, it displays the following message along with the data:
Click here to configure more pollers.
You can click the here link to launch the Poller Management page. The Poller Management page allows you to configure more pollers.

Table 6-24 displays the color and the percentage of the CPU Utilization of the device.

Table 6-24 Color and Percentage of CPU Utilization of the Device

<table>
<thead>
<tr>
<th>Color</th>
<th>CPU Utilization of the Device in Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>CPU Utilization of the device from 0 to 10%</td>
</tr>
<tr>
<td>Yellow</td>
<td>CPU Utilization of the device from 10 to 30%</td>
</tr>
<tr>
<td>Orange</td>
<td>CPU Utilization of the device from 30 to 80%</td>
</tr>
<tr>
<td>Red</td>
<td>CPU Utilization of the device from 80 to 100%</td>
</tr>
</tbody>
</table>

Table 6-25 lists the TOP-N CPU Utilization portlet details.

Table 6-25 TOP-N CPU Utilization Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device. Click the Device Name link to navigate to the Device Center page.</td>
</tr>
<tr>
<td>CPU Instance</td>
<td>Instance, which occupies the CPU at the particular period of time.</td>
</tr>
<tr>
<td>MIN%</td>
<td>Minimum CPU utilization percentage value in a device.</td>
</tr>
<tr>
<td>MAX%</td>
<td>Maximum CPU utilization percentage value in a device.</td>
</tr>
<tr>
<td>AVG%</td>
<td>Average CPU utilization percentage value in a device.</td>
</tr>
</tbody>
</table>

Note
The maximum and minimum fields appear in the portlet only if they are configured. The Average % field appears by default in the portlet.

You can customize and configure the TOP-N-CPU Utilization portlet.
To configure TOP-N-CPU Utilization portlet:

**Step 1** Move the mouse over the title bar of the TOP-N-CPU portlet to view the icons.

**Step 2** Click the Configuration icon. You can:

- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed refresh time.
- Select the number of rows to be displayed in the portlet from the No. of rows to be displayed drop-down list.
  
  For example, if you select 5, then five rows will be displayed in the portlet.
- Select the Max or the Min check box to display either the maximum or minimum fields in the portlet.
- Select the Time interval from the Time Interval drop-down list.
  
  For example, if you select 1 Hour, the CPU Utilization details for the last one hour will be displayed.

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

### Performance Threshold Information

The Performance Threshold Information portlet provides information about the threshold violation details such as threshold name, time when the violation took place, the violation value, and device name. The Performance Threshold Information portlet also displays the latest \( N \) number of violations.

If there is no data in the Performance Threshold Information portlet, it displays the following message:

Currently Thresholds have not been configured. Click here to configure.

You can click the here link to launch the Threshold Setup page. The Threshold Setup page allows you to configure thresholds.

**Table 6-26** displays the Performance Threshold Information portlet details.

**Table 6-26** Performance Threshold Information Portlet Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Thresholds Configured</td>
<td>Displays the number of thresholds configured. You can click the number to navigate to the List of Thresholds information page.</td>
</tr>
<tr>
<td>No. of Violations in Last “N” time interval.</td>
<td>Displays the number of violations occurred in the configured Time Interval. The violations are based on the severity level such low, medium and critical. The Critical Violation is displayed by default in the portlet. However, the medium and low violations have to be configured to view it in the portlet.</td>
</tr>
<tr>
<td></td>
<td>• If the violation is low, it is displayed in green.</td>
</tr>
<tr>
<td></td>
<td>• If the violation is medium, it is displayed in orange.</td>
</tr>
<tr>
<td></td>
<td>• If the violation is critical, it is displayed in red.</td>
</tr>
<tr>
<td>Threshold Details</td>
<td></td>
</tr>
<tr>
<td>Threshold Name</td>
<td>Name of the threshold. For instance, CPU Threshold.</td>
</tr>
</tbody>
</table>
Chapter 6  Monitoring Dashboard

Performance Threshold Information

You can customize and configure the Performance Threshold Information portlet.

To configure the Performance Threshold Information portlet:

1. Move the mouse over the title bar of the Performance Threshold Information portlet to view the icons.
2. Click the Configuration icon. You can:
   - Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed refresh time that you set.
   - Select the severity field such as Low, Medium, or Critical from the Severity display field’s drop-down list to set the severity levels.
     For instance, select the Low check box if you want to display the low level threshold information in the Performance Threshold Information portlet.
     By default, Critical will be displayed in the Performance Threshold Information portlet.
   - Select the number of rows to be displayed in the portlet from the No. of rows to be displayed drop-down list.
     For example, if you select 5, five rows will be displayed in the portlet.
3. Click Save to view the portlet with the configured settings.

Viewing Threshold Violation Report:

You can also view the Threshold Violation Reports based on the severity levels such as Low, Medium and Critical.

To view the Threshold Violation Report:

1. Go to Performance Threshold Information portlet and click the count against the severity levels.

   The Threshold Report page appears.

   For instance, if you click the number against the severity level Low, the threshold report based on the lowest severity appears. The report is also based on the time interval you have selected such as 1 hour or 1 day.

   **Note**  The Threshold Report page displays the entire generated reports. However the portlet displays only a maximum of twenty generated reports.
Performance TrendWatch Information

Performance TrendWatch portlet displays a list of configured TrendWatch. Each TrendWatch name will have a link to launch the corresponding report.

There are two options available to sort the report based on the severity and the TrendWatch name.

Table 6-27  Performance TrendWatch portlet details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.of TrendWatch configured</td>
<td>Total number of TrendWatch that are configured.</td>
</tr>
<tr>
<td>No.of Violations in the last 15 days</td>
<td>Total number of violations that occurred during the last 15 days.</td>
</tr>
<tr>
<td>TrendWatch Details</td>
<td></td>
</tr>
<tr>
<td>TrendWatch Name</td>
<td>Name of the TrendWatch.</td>
</tr>
<tr>
<td>Count</td>
<td>The total number of the TrendWatch.</td>
</tr>
<tr>
<td></td>
<td>The count is displayed when you select the TrendWatch radio button.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td></td>
<td>The Device name is displayed only when you select the Severity level radio button.</td>
</tr>
<tr>
<td>Severity Levels</td>
<td>Displays the severity level.</td>
</tr>
<tr>
<td></td>
<td>For example, S1, S2 for severity levels 1, severity level 2, and so on.</td>
</tr>
<tr>
<td></td>
<td>The severity level is displayed only when you select the Severity level radio button.</td>
</tr>
<tr>
<td>Last Time Stamp</td>
<td>Last time stamp of the TrendWatch.</td>
</tr>
</tbody>
</table>

You can customize and configure the Performance TrendWatch portlet.

To configure the Performance TrendWatch portlet:

**Step 1**  Move the mouse over the Performance TrendWatch portlet and click the Configure icon to:

- Select the Auto Refresh check box to refresh the portlet details at the set time interval.
- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the Refresh time that you set.
- Select the Content Summary radio button to sort the content in summary order or Content Details radio button to sort the order of the content details.
- Select the Group Severity levels radio button to group the TrendWatch based on the severity or select the TrendWatch radio button to group according to the TrendWatch details.
- Select the number of rows to be displayed in the portlet from the No. of rows to be displayed drop-down list.
  - For example, if you select 5, five rows will be displayed in the portlet.
- Select the time interval from the Time Interval drop-down list. For example, one day, one week, one month, and so on.

**Step 2**  Click Save to view the portlet with the configured settings.
TOP-N Environmental Temperature

The TOP N Environmental Temperature portlet enables you to monitor the temperature of the various devices.

The portlet displays the device name, instance name and the average temperature of each device.

You can customize and configure the TOP-N-Environmental Temperature portlet.

To configure the TOP-N-Environmental Temperature portlet:

**Step 1**
Move the mouse over the TOP-N-Environmental Temperature portlet and click the Configure icon to:

- Select the Auto Refresh check box to refresh the portlet details at the set time interval.
- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed refresh time that you set.
- Select the number of rows to be displayed in the portlet from the No. of rows to be displayed drop-down list.
- Select Celsius radio button, if you want to set the unit of measurement in Celsius.
  
  Or
  
  - Select the Fahrenheit radio button, if you want to set the unit of measurement in Fahrenheit.
  - Select the Max check box, if you want to display the list of devices with maximum temperature
  - Or
  - Select Min check box, if you want to display the list of devices with minimum temperature.
  - Select the time interval from the Time Interval drop-down list. For example, 1 hour, 1 day, 7 days, 15 days and 30 days.

**Step 2**
Click the Save button to save all the configured details.

NAM Top N Statistics Portlet

NAM refers to Cisco Network Analysis Module Traffic Analyzer. The NAM offers flow-based traffic analysis of applications, hosts, and conversations, performance-based measurements on application, server, and network latency, quality of experience metrics for network-based services such as voice over IP (VoIP) and video.

Only NAM 4.1 is supported in LMS. See the NAM 4.1 Online help for more details.

If you configure NAM 5.0 or higher version, this portlet displays HTTP 500 error.

NAM Top N Statistics portlet displays the protocol, traffic, or average application report of a selected interface or data source monitored from a NAM IP Address.

To configure the NAM Top N Statistics portlet:

**Step 1**
Move the mouse over the NAM Top N Statistics portlet and click the Configure icon to:

- Select the Auto Refresh check box to refresh the portlet details at the set time interval.
- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed refresh time that you set.
Step 2  Select an IP Address of NAM modules that are configured in LMS, from the NAM IP field.
See the Admin Online help for the details on configuring NAM.

Step 3  Select a report type to be viewed. The available report types are:
- Protocol
- Traffic
- AvgApplication

Note  If you have configured NAM 5.0 or higher version and selected the report type as AvgApplication, this portlet displays No Data Available instead of HTTP 500 error.

Step 4  Select an interface from the list of interfaces set up from the Data Source field.
Step 5  Click Save to view the portlet with the configured settings.

### NAM Attribute Value

The NAM Attribute Value portlet displays the various data monitored for an application, a server, or a service by a NAM using an external or internal data source.

Only NAM 4.1 is supported in LMS. See the NAM 4.1 Online help for more details and description of the parameters monitored.

If you configure NAM 5.0 or higher version, this portlet displays HTTP 500 error.

The following table displays the various parameters that could be monitored by a NAM:

<table>
<thead>
<tr>
<th>Category</th>
<th>Parameters Monitored</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td></td>
</tr>
<tr>
<td>AppProtocol</td>
<td>• Bytes/s</td>
</tr>
<tr>
<td></td>
<td>• Packets/s</td>
</tr>
<tr>
<td>ART Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Number of Responses</td>
</tr>
<tr>
<td></td>
<td>• Number of Late Responses</td>
</tr>
<tr>
<td></td>
<td>• AvgApplicationDelay</td>
</tr>
<tr>
<td></td>
<td>• MinApplicationDelay</td>
</tr>
<tr>
<td></td>
<td>• MaxApplicationDelay</td>
</tr>
<tr>
<td></td>
<td>• AvgNetworkDelay</td>
</tr>
<tr>
<td></td>
<td>• MinNetworkDelay</td>
</tr>
<tr>
<td></td>
<td>• MaxNetworkDelay</td>
</tr>
<tr>
<td></td>
<td>• AvgTotalDelay</td>
</tr>
<tr>
<td></td>
<td>• MinTotalDelay</td>
</tr>
<tr>
<td></td>
<td>• MaxTotalDelay</td>
</tr>
</tbody>
</table>
## NAM Attribute Value

### Parameters Monitored

<table>
<thead>
<tr>
<th>Category</th>
<th>Parameters Monitored</th>
</tr>
</thead>
<tbody>
<tr>
<td>ART Client Server</td>
<td>• Number of Responses</td>
</tr>
<tr>
<td></td>
<td>• Number of Late Responses</td>
</tr>
<tr>
<td></td>
<td>• AvgApplicationDelay</td>
</tr>
<tr>
<td></td>
<td>• MinApplicationDelay</td>
</tr>
<tr>
<td></td>
<td>• MaxApplicationDelay</td>
</tr>
<tr>
<td></td>
<td>• AvgNetworkDelay</td>
</tr>
<tr>
<td></td>
<td>• MinNetworkDelay</td>
</tr>
<tr>
<td></td>
<td>• MaxNetworkDelay</td>
</tr>
<tr>
<td></td>
<td>• AvgTotalDelay</td>
</tr>
<tr>
<td></td>
<td>• MinTotalDelay</td>
</tr>
<tr>
<td></td>
<td>• MaxTotalDelay</td>
</tr>
<tr>
<td>Server</td>
<td>• In Bytes/s</td>
</tr>
<tr>
<td>Host Statistics</td>
<td>• In Packets/s</td>
</tr>
<tr>
<td></td>
<td>• Out Bytes/s</td>
</tr>
<tr>
<td></td>
<td>• Out Packets/s</td>
</tr>
<tr>
<td></td>
<td>• Non-Unicast/s</td>
</tr>
<tr>
<td>Service</td>
<td></td>
</tr>
<tr>
<td>Voice Quality</td>
<td>—</td>
</tr>
</tbody>
</table>

To configure the NAM Attribute Value portlet:

**Step 1** Move the mouse over the NAM Attribute Value portlet and click the Configure icon to:
- Select the Auto Refresh check box to refresh the portlet details at the set time interval.
- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed refresh time that you set.

**Step 2** Select an IP Address of NAM modules that are configured in LMS, from the NAM IP field. See the Admin Online help for the details on configuring NAM.

**Step 3** Select an object family from the list:
- Application
- Server
- Service

**Step 4** Select a category for the selected object family.

**Step 5** Select one or more parameters from the Parameters list.

**Step 6** Select an interface from the list of interfaces set up from the Data Source field.

**Step 7** Click **Save** to view the portlet with the configured settings.
IPSMA Collector Information

A collector is defined as an entity that encompasses a source router, a target device, an operation, and the collector schedule details.

You must configure the refresh time in the portlets.

Table 6-28 lists IPSMA Collector Information portlet details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Displays the state of the collector. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Deleting</td>
</tr>
<tr>
<td></td>
<td>• Pending</td>
</tr>
<tr>
<td></td>
<td>• Scheduled</td>
</tr>
<tr>
<td></td>
<td>• Dormant</td>
</tr>
<tr>
<td></td>
<td>• Config Failed</td>
</tr>
<tr>
<td></td>
<td>• Source Not Responding</td>
</tr>
<tr>
<td></td>
<td>• Completed</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Stopped and Configuring</td>
</tr>
</tbody>
</table>

Number of Collectors | Displays the number of collectors in the respective state.  |
Licensed Collectors   | Displays the total number of licensed collectors.              |

Note: You can click the number link to navigate to the IPSMA Collector Management page.

Table 6-29 lists the Collector Information status details.

<table>
<thead>
<tr>
<th>Collector Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleting</td>
<td>Collector is being deleted.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>Collector is scheduled for a future date and time.</td>
</tr>
<tr>
<td>Dormant</td>
<td>Collector is in dormant state and will start polling at the next polling interval.</td>
</tr>
<tr>
<td>Config Failed</td>
<td>Configuration of the collector failed on the source router.</td>
</tr>
<tr>
<td>Source Not Responding</td>
<td>Source router is not responding to configuration or reconfiguration of the collector or for polling the statistics. This problem could occur because of invalid credentials or because the device is not reachable.</td>
</tr>
<tr>
<td>Completed</td>
<td>Collector has reached its end time and LMS will not poll this collector again.</td>
</tr>
<tr>
<td>Running</td>
<td>Collector is configured at the source router and polling is in progress.</td>
</tr>
</tbody>
</table>
Table 6-29  Collector Information State

<table>
<thead>
<tr>
<th>Collector Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopped</td>
<td>Collector has been manually stopped and is not being polled by LMS.</td>
</tr>
<tr>
<td>Configuring</td>
<td>Configuration of the collector is in progress.</td>
</tr>
</tbody>
</table>

### IPSLA Device Categorization

The devices added from Device Credential Repository are categorized based on the availability of IPSLA. IPSLA is a feature built into Cisco Internetworking Operating System (IOS) and is used by most Cisco routers and switches.

IPSLA source is a device from which you initiate operations for measuring network performance statistics. IPSLA targets are destination devices for which you want to gather network performance statistics. However, some target devices are Responder enabled.

You must configure the refresh time in the portlets.

Table 6-30 lists Device Categorization portlet details.

Table 6-30 Device Categorization

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSLA</td>
<td>IPSLA is a portfolio of technology embedded in most devices that run Cisco IOS software. This allows you to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce the frequency of network outages. IPSLA uses active traffic monitoring- the generation of traffic in a continuous, reliable and predictable manner-for measuring network performance.</td>
</tr>
<tr>
<td>Count</td>
<td>Lists the number of IPSLA enabled devices in LMS. Click the number to view the IPSLA Devices details.</td>
</tr>
</tbody>
</table>
Using Topology Services

Topology Services is an application that enables you to view and monitor your network including the links, and the ports of each link.

Topology Services displays the network topology of the devices discovered by LMS through Topology Maps. Besides these maps, the application generates numerous reports that help you to view the physical and logical connectivity in detail.

Note

If the Cisco Prime LMS server is not DNS resolvable from the client, see Launching Topology Services when the Server is not DNS Resolvable.

This chapter contains:

- Understanding Topology Services
- Starting Topology Services
- Using Topology Services Legend
- Understanding Topology Services Main Window
- Using Topology Services Main Window
- Understanding Network Topology Views
- Using Network Views
- Understanding Cluster Switches
- Using Topology Filters
- Using Find in Network Topology Views
- Understanding Summary View
- Upgrading Network Topology Views
- N-Hop View Portlet
- Using Microsoft Visio With Topology Views
- Working With Links
- Time Domain Reflectometry Reports
- Working With Devices
- Displaying Network Topology and Layer-2 Services Reports
- Monitoring Protocol Filter by Port
Understanding Topology Services

You can use Topology Services to:

- View detailed network information about all devices (see Working With Devices), links (see Working With Links), and ports (see Displaying Port Attributes) in your network.
- Display the physical and logical services in your network. See Understanding Network Topology Views.
- Open network management tools from the network views.
- Segment your network logically and manage workgroups that use VLANs.
- View port, device, and trunk attributes; view and find port information in a VTP domain; and configure VLANs on a trunk.
- Display reports about inconsistencies or misconfigurations in your physical or logical network setup.
- Configure and manage Etherchannel and Trunk links between devices.
- Configure and visualize Spanning Tree Protocol.
- Configure and manage Inter-VLAN Routing (IVR).
- Run Time Domain Reflectometry (TDR) test between devices.
- View the bandwidth utilization across the links in your network.

Starting Topology Services

Select Monitor > Monitoring Tools > Topology Services from the menu, to start the Topology Services.

You must install the Java plug-in to access Topology Services from a client. If you are prompted to install the Java plug-in, download and install it using the installation screens.

The next time you start the application, it automatically uses the plug-in. For more information on the Java Plug-in, see the Online help for Administration of Cisco Prime LAN Management Solution 4.2.

Before You Begin

Before launching Topology Services, check whether the daemon is up and the ANIServer process is running.

If the daemon is down, you should:

- Restart the daemon by entering:
  - For Windows: `net start crmdmgt.d`
  - For Solaris or Soft Appliance: `/etc/init.d/dmgtd`
Starting Topology Services

- Check whether the daemon is up and running by entering `pdshow` at the command prompt.

If the ANIServer is terminated, you should:
- Restart ANIServer by entering `pdexec ANIServer` at the command prompt and try again.
- Check whether the ANIServer process is up and running by entering `pdshow ANIServer` at the command prompt.

You should also verify that:
- Your network is set up properly.
- The Cisco Prime LMS Server is set up properly and running.

This section contains the following:
- Prerequisites to Launch Topology Services
- Launching Topology Services when the Server is not DNS Resolvable
- Launching Topology Services from Windows Client
- Launching Topology Services from Clients Using Internet Explorer 8.0 Browser

**Prerequisites to Launch Topology Services**

To access LMS Topology Services, we recommend that you install Java Plug-in version 1.6.0_24. If the client machine is installed with the JRE Update version equal to or higher than the recommended version, then Topology Services is launched in the client machine.

If the client machine is installed with an Update version equal to or higher than the recommended JRE version (1.6.0_24), then Topology Services will be launched only if either one of two versions is selected.

If the user selects the recommended JRE as well as the higher Update version of JRE, Topology Services will be launched with the higher Update version of JRE.

For example, LMS 4.2 requires JRE 1.6.0_24 to launch Topology Services. If the client machine is installed with an Update version higher than JRE 1.6.0_24, say 1.6.0_25, and user selects JRE 1.6.0_25, then Topology Services is launched with JRE 1.6.0_25.

**Launching Topology Services when the Server is not DNS Resolvable**

The Cisco Prime LMS client must be able to resolve the hostname of the Cisco Prime LMS server to server's IP Address, through DNS.

If the Cisco Prime LMS server is not DNS resolvable, Cisco Prime LMS client can access it with the IP address itself, by performing the following steps:

**Step 1**
Open the orb.properties file.

Solaris or Soft Appliance: `NMSROOT/lib/classpath`

Windows: `NMSROOT/lib/classpath`

where `NMSROOT` is the directory where you have installed Cisco Prime LMS.

**Step 2**
Set the property as follows:

`jacob.dns.enable=off`
Starting Topology Services

Step 3  Go to Admin > Trust Management > Local Server > Certificate Setup.
The Certificate Setup page appears.

Step 4  Enter the IP Address of the Cisco Prime LMS Server in the Hostname textbox.

Step 5  Populate the other columns as explained in the Online help for Administration of Cisco Prime LAN Management Solution 4.2.

Step 6  Click Apply to generate the self-signed certificate.

Step 7  Restart the daemons. See the Online help for Administration of Cisco Prime LAN Management Solution 4.2 for instructions.

You will be able to launch Topology Services with the IP address itself.

Launching Topology Services from Windows Client

In LMS 3.1, Visibroker is migrated to JacORB.

While launching Topology Services, check whether the hostname is DNS resolvable or edit the hosts file in the Windows client.

If the mapping is not available, you need to edit the hosts file by adding the IP Address details for the LMS Server in the following format:

IPAddress Hostname

The Hostname entry can be of the form hostname, example. You can access the hosts file in the Windows client from the following location:

%SYSTEMROOT%\system32\drivers\etc

For launching Topology Services in Windows 7 client, the current user should have full permissions to the three Jar files, which is downloaded to the local system when launching Topology Services for the first time.

Launching Topology Services from Clients Using Internet Explorer 8.0 Browser

Sometimes, Internet Explorer 8.0 blocks the software and file downloads. Because of this, Topology Services may not launch properly.

To allow the software and file downloads in Internet Explorer 8.0 and launch Topology Services:

Step 1  Open Internet Explorer.

Step 2  Click Tools > Internet Options.
The Internet Options dialog box opens.

Step 3  Click the Security tab.

Step 4  Click Custom level... from the Security level for this zone panel.
The Security Settings dialog box opens.

Step 5  Select the Enable option for the Automatic prompting for file downloads field.

Step 6  Click OK to go to the Internet Options dialog box.
Step 7 Click OK.

Sometimes, Topology Services and Java console may launch twice for a single click in Internet Explorer 8.0.

To overcome this:

Step 1 Open Internet Explorer.
Step 2 Click Tools > Internet Options.
   The Internet Options dialog box opens.
Step 3 Click the Advanced tab.
Step 4 Scroll down to the Security Section.
Step 5 Uncheck the Enable SmartScreen Filter check box.
Step 6 Click OK.

Using Topology Services Legend

The Topology Services Legend explains the use of icons and colors in network views. You can refer the Legend to identify devices in your network and their status. The Legend includes all manageable devices, including devices that might be in your network. Color indicators described in the Legend enable you to quickly determine the status of your network.

To display the Legend:

Step 1 Select Monitor > Monitoring Tools > Topology Services.
   The Topology Services Main Window appears.
Step 2 Select Help > Legend from the menu.
   The Color and Icon Legend window opens. For details, see Table 8-1.
Step 3 Click Close to close the window.

Table 7-1 Color and Icon Legend

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icons</td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Ethernet VLAN" /></td>
<td>Ethernet VLAN</td>
</tr>
<tr>
<td><img src="image" alt="Filter On" /></td>
<td>Filter On</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="image" alt="Symbol CO" /></td>
<td>FDDI Ring</td>
</tr>
<tr>
<td><img src="image" alt="Symbol Link Port" /></td>
<td>Link Port</td>
</tr>
<tr>
<td><img src="image" alt="Symbol Network Topology View" /></td>
<td>Network Topology View (Topology Map)</td>
</tr>
<tr>
<td><img src="image" alt="Symbol Switch Port" /></td>
<td>Switch Port</td>
</tr>
<tr>
<td><img src="image" alt="Symbol Router" /></td>
<td>Router</td>
</tr>
<tr>
<td><img src="image" alt="Symbol Serial Bus" /></td>
<td>Serial Bus</td>
</tr>
<tr>
<td><img src="image" alt="Symbol Switch" /></td>
<td>Switch</td>
</tr>
<tr>
<td><img src="image" alt="Symbol Unknown VLAN" /></td>
<td>Unknown VLAN</td>
</tr>
<tr>
<td><img src="image" alt="Symbol Switch Cloud" /></td>
<td>Switch Cloud</td>
</tr>
<tr>
<td><img src="image" alt="Symbol Virtual Switching System" /></td>
<td>Virtual Switching System (VSS)</td>
</tr>
<tr>
<td><img src="image" alt="Symbol WAN Switch" /></td>
<td>WAN Switch</td>
</tr>
<tr>
<td><img src="image" alt="Symbol Embedded Router" /></td>
<td>Embedded Router</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td><img src="image" alt="Embedded Switch" /></td>
<td>Embedded Switch</td>
</tr>
<tr>
<td><img src="image" alt="Embedded SBC" /></td>
<td>Embedded SBC</td>
</tr>
<tr>
<td><img src="image" alt="End Station" /></td>
<td>End Station</td>
</tr>
<tr>
<td><img src="image" alt="Integrated Communications System" /></td>
<td>Integrated Communications System</td>
</tr>
<tr>
<td><img src="image" alt="Layer 2 and Layer 3 Switch Router" /></td>
<td>Layer 2 and Layer 3 Switch Router</td>
</tr>
<tr>
<td><img src="image" alt="Application Server" /></td>
<td>Application Server</td>
</tr>
<tr>
<td><img src="image" alt="Hub" /></td>
<td>Hub</td>
</tr>
<tr>
<td><img src="image" alt="Switch Probe" /></td>
<td>Switch Probe</td>
</tr>
<tr>
<td><img src="image" alt="Voice Gateway" /></td>
<td>Voice Gateway</td>
</tr>
<tr>
<td><img src="image" alt="Access Point" /></td>
<td>Access Point</td>
</tr>
<tr>
<td><img src="image" alt="Optical Services Router" /></td>
<td>Optical Services Router</td>
</tr>
<tr>
<td><img src="image" alt="Cisco ONS Series Device" /></td>
<td>Cisco ONS Series Device</td>
</tr>
</tbody>
</table>
### Table 7-1 Color and Icon Legend (continued)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Content Engine" /></td>
<td>Content Engine</td>
</tr>
<tr>
<td><img src="image" alt="Content Server Switch" /></td>
<td>Content Server Switch</td>
</tr>
<tr>
<td><img src="image" alt="DSL Switch" /></td>
<td>DSL Switch</td>
</tr>
<tr>
<td><img src="image" alt="Switch Stack" /></td>
<td>Switch Stack</td>
</tr>
<tr>
<td><img src="image" alt="Storage Switch" /></td>
<td>Storage Switch</td>
</tr>
<tr>
<td><img src="image" alt="Add Row" /></td>
<td>Add Row</td>
</tr>
<tr>
<td><img src="image" alt="LMS Server Unknown" /></td>
<td>LMS Server Unknown</td>
</tr>
<tr>
<td><img src="image" alt="LMS Server Idle or Running" /></td>
<td>LMS Server Idle or Running</td>
</tr>
<tr>
<td><img src="image" alt="Restricted Topology View" /></td>
<td>Restricted Topology View</td>
</tr>
<tr>
<td><img src="image" alt="Broadband Router" /></td>
<td>Broadband Router</td>
</tr>
<tr>
<td><img src="image" alt="Cisco CallManager" /></td>
<td>Cisco CallManager</td>
</tr>
<tr>
<td><img src="image" alt="Cluster Commander Switch" /></td>
<td>Cluster Commander Switch</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Device</td>
<td>Navigate Down</td>
</tr>
<tr>
<td></td>
<td>Link in Forwarding State</td>
</tr>
<tr>
<td></td>
<td>Link in Blocking State</td>
</tr>
<tr>
<td></td>
<td>Isolated VLAN</td>
</tr>
<tr>
<td></td>
<td>Community VLAN</td>
</tr>
<tr>
<td></td>
<td>Two-way Community VLAN</td>
</tr>
<tr>
<td></td>
<td>Closed Folder</td>
</tr>
<tr>
<td></td>
<td>Domain Folder</td>
</tr>
<tr>
<td></td>
<td>Open Folder</td>
</tr>
<tr>
<td></td>
<td>Layer Map</td>
</tr>
<tr>
<td></td>
<td>Route Switch Module (RSM) Switch</td>
</tr>
</tbody>
</table>
### Table 7-1 Color and Icon Legend (continued)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Display All Rows</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Begin</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Stop Tree</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Unknown Device</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Zoom to Fit</td>
</tr>
</tbody>
</table>

#### Icon Colors
- ![Icon](image) Major Fault (red)
- ![Icon](image) OK (green)

#### Links
- ![Icon](image) Active (black)
- ![Icon](image) Inactive (red)
- ![Icon](image) Not in network (red dashes)
- ![Icon](image) Unknown (blue)
Table 7-1  Color and Icon Legend (continued)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![icon]</td>
<td>Link virtualization status as black link displays that both the interfaces connecting devices are a part of VRF</td>
</tr>
<tr>
<td>![icon]</td>
<td>Link virtualization status as cyan link displays only one interface is a part of VRF</td>
</tr>
<tr>
<td>![icon]</td>
<td>Link virtualization status as grey link displays no interface is a part of VRF</td>
</tr>
<tr>
<td>![icon]</td>
<td>Non Cisco device</td>
</tr>
</tbody>
</table>

1. Device is not reachable using SNMP or the device is down.

Table 7-2 lists the special scenarios for Layer 2/Layer 3 Switch Routers.

For example, the switch is running Catalyst operating system and the router is an RSM or MSFC module, and if either the switch or the router is unreachable the topology map displays the icon as:

Table 7-2  Icons for Discrepancies of Layer 2/Layer 3 Switch Router

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![icon]</td>
<td>Router is reachable, but switch is unreachable using SNMP.</td>
</tr>
<tr>
<td>![icon]</td>
<td>Router is unreachable using SNMP, but switch is reachable.</td>
</tr>
</tbody>
</table>
Understanding Topology Services Main Window

You can access the LAN Edge, Layer 2, and Unconnected Devices network views of managed domains discovered in your network, and you can filter, access, or view network information or status. For more information, see Table 7-3.

This section contains Understanding Tree View.

Table 7-3  Topology Services Main Window Components

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Usage Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu</td>
<td>Contains Topology Services commands.</td>
<td>See Topology Services Menu Reference for more information.</td>
</tr>
<tr>
<td>Toolbar</td>
<td>Provides quick access to frequently used menu options.</td>
<td>To show or hide the toolbar, select View &gt; Show Toolbar.</td>
</tr>
</tbody>
</table>
| Tree View | Access the LAN Edge, Layer 2, and Unconnected Devices network views of managed domains. | • Right-click items that you want to display, and select View > Display View to display network views.  
  • Single-click items to display summary information in the Summary View. |
| Summary View | Displays configuration information about the items displayed in the Tree View. | Click and drag column headings to change the order in which they appear. |
| Status Bar | Displays Topology Services system messages on the left and the Status button on the right. | Click the color-coded Status button to open LMS Server Status Information window.  
  In this window you can view Data Collection status. |
Understanding Tree View

The Tree View displays the discovered network objects in a hierarchical list. This list includes managed domains and available network views.

Table 7-4 Understanding Tree View

<table>
<thead>
<tr>
<th>Folder</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domains</td>
<td>VTP Domains</td>
<td>Displays and monitors the details of the VLANs in your network. Sometimes includes special cases labeled NULL or NO_VTP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NULL—Lists devices that are in transparent mode and that support VTP, but that do not have configured domain names. Each of these devices is identified in the list by its IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NO_VTP—Lists devices that do not support VTP. Each of these devices is identified in the list by its IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>However, devices that do not support VTP but support VLANs (for example, Catalyst 2900XL Standard Edition switches) will be placed in the NO_VTP domain.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Devices that do not support VLANs and VTP (for example, Catalyst 1900 Standard Edition switches) will be placed in the domain category of the neighbor device.</td>
</tr>
<tr>
<td>Network Views</td>
<td>LAN Edge View</td>
<td>Shows network connectivity between Layer 3 devices that have routing characteristics. Devices without Layer 3 connectivity are displayed in switch cloud network views.</td>
</tr>
<tr>
<td>Layer 2 View</td>
<td></td>
<td>Displays Layer 2 information about your network, including LAN switches, routers, multilayer switching devices, hubs, and switch probes.</td>
</tr>
<tr>
<td>Unconnected Devices View</td>
<td></td>
<td>Displays devices for which connectivity information could not be obtained.</td>
</tr>
<tr>
<td>VTP Views</td>
<td></td>
<td>Displays devices that are participating in VTP domains, and their neighbors.</td>
</tr>
<tr>
<td>Topology Groups</td>
<td>System Defined Groups</td>
<td>Displays a top-level container for standard groups that are accessible to and used by most LMS users. This also includes a set of predefined groups.</td>
</tr>
<tr>
<td></td>
<td>User Defined Groups</td>
<td>Displays a top-level container where individual LMS users create their own groups.</td>
</tr>
</tbody>
</table>
Using Topology Services Main Window

You can use Topology Services Main Window for displaying the discovered VTP domains, VLANs, and access the LAN Edge view, Layer 2 view, and the Unconnected Devices view.

The topic contains:
- Navigating in Main Window
- Understanding the Status Bar
- Using Find in Main Window

Navigating in Main Window

You can display VTP domains and VLANs from the Main Window. You can also access the LAN Edge, Layer 2, and Unconnected Devices network views of managed domains discovered in your network, and you can filter, access, or view network information or status.

Figure 7-1 displays the Topology Services Main Window.
Table 7-5 describes the areas in the Topology Services Main Window.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu</td>
<td>Contains Topology Services commands.</td>
<td>See Topology Services Main Window Reference for more information.</td>
</tr>
<tr>
<td>Toolbar</td>
<td>Provides quick access to frequently used menu options.</td>
<td>To show or hide the toolbar, select View &gt; Show Toolbar.</td>
</tr>
</tbody>
</table>
| Tree View| Displays discovered VTP domains and VLANs. Access the LAN Edge, Layer 2, and Unconnected Devices network views of managed domains. | Right-click items that you want to display, and select View > Display View to display network views.  
Single-click items to display summary information in the Summary View. |
| Summary View | Displays configuration information about the items displayed in the Tree View. | Click and drag column headings to change the order in which they appear.                                                                   |
| Status Bar | Displays Topology Services system messages on the left and the Status button on the right. | Click the color-coded Status button to view status.  
This dialog box displays the Data Collection status. It also displays the time at which the most recent Data Collection was completed. |
Understanding the Status Bar

The status bar displays information about the current status of the Topology Services application, and includes a button that you can click to view the current network Data Collection statistics. Figure 7-2 describes sections of the Status Bar.

**Figure 7-2 Status Bar**

![Status Bar Diagram]

Table 7-6 describes different parts of a Status Bar.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology Services</td>
<td>Messages about the status of Topology Services appear on the left side of the status bar. These messages typically are displayed at the start and end of a task that is performed within Topology Services.</td>
</tr>
<tr>
<td>Discovery Status</td>
<td>A color-coded Data Collection Server status message appears in a button on the right side of the status bar:</td>
</tr>
<tr>
<td></td>
<td>- Green—Denotes that Topology Services is able to communicate with the Data Collection Server. The status message is either <strong>Running</strong>, denoting that one or more discovery processes in the Data Collection server are in discovery; or <strong>Idle</strong>, denoting that there are no discoveries currently active in the Data Collection Server.</td>
</tr>
<tr>
<td></td>
<td>- Red—Denotes that the Data Collection Server is down or unreachable. In this case, the status message is <strong>Unknown</strong>. Click this button to open the Discovery Information window. This window displays detailed information on all Discovery processes.</td>
</tr>
<tr>
<td>Restricted View</td>
<td>A lock icon appears when LMS is integrated with ACS Server and Topology is set to display only authorized devices. For details, see Restricted Topology View.</td>
</tr>
</tbody>
</table>
Using Find in Main Window

You can use the Find option to locate specific items in your network. Your search is restricted to either the Tree View or Summary View. You cannot search both views simultaneously in Topology Services. Select the view based on the item you want to locate.

To use the Find option in the Main Window:

**Step 1**
Select **Edit > Find** from the menu.

**Step 2**
Enter the required information as described in the Main Window Find Field Descriptions table.

**Step 3**
Click **Next** to find items that match your search criteria.
Select **Edit > Find Next** to quickly repeat your last search.

### Table 7-7 Main Window Find Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search For</td>
<td>Enter the search string</td>
<td>Search by any string, partial or complete.</td>
</tr>
<tr>
<td>Search In</td>
<td>Select either of these views:</td>
<td>The Find function searches only the selected item in the specified view, and those items that appear below your selection in the view. To search an entire view, you must select the first (top) item in that view.</td>
</tr>
<tr>
<td>Options</td>
<td>Select from these options:</td>
<td>• Ignore Case—Select this option to allow matches in any case.</td>
</tr>
<tr>
<td></td>
<td>• Exact Match</td>
<td>• Exact Match—Select this option to find entries that match the search string exactly.</td>
</tr>
</tbody>
</table>

Understanding Network Topology Views

A Network View is a graphical representation of the devices in your network. You can use Network Views to see different aspects of your network. Only devices and links discovered in your network are displayed.

While you use Topology Services, the listed devices and links change dynamically to display what the LMS Server discovers in your network.

Network Views provide various abstract views of your network. Table 7-3 describes the Network Topology window components.

You can use Network Views to see different aspects of your network. Only devices and links discovered in your network are displayed in topology maps.

As you use Network Topology Views, the listed devices and links change dynamically to display devices and links that Data Collection detects in your network.
Table 7-8 provides a list of functions that you can perform in Network Topology Views.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displaying Network Views</td>
<td>Access and display network views</td>
</tr>
<tr>
<td>Changing Network Topology View Layouts</td>
<td>Displays logical and physical services in your network</td>
</tr>
<tr>
<td>Working With Links</td>
<td>Displays information about the links between discovered devices</td>
</tr>
<tr>
<td>Working With Application Servers</td>
<td>Displays and access application servers in your network</td>
</tr>
<tr>
<td>Displaying Port Attributes</td>
<td>Displays information about the status of device ports in your network</td>
</tr>
<tr>
<td>Displaying Aggregate Link Attributes</td>
<td>Displays information about any aggregate links that you have created in your network</td>
</tr>
<tr>
<td>Displaying Service Attributes</td>
<td>Displays information about the available services in your network</td>
</tr>
<tr>
<td>Customizing Network Topology Views</td>
<td>Modifies network views to suit your individual network management needs</td>
</tr>
<tr>
<td>Using Topology Filters</td>
<td>Use filters or the Find function to locate specific devices, or specific kinds of devices</td>
</tr>
</tbody>
</table>

This topic contains:
- Navigating in Network Topology Views
- Connecting Securely to Devices From Clients
- Displaying Network Views
- Using Panner to View Topology Maps

**Navigating in Network Topology Views**

You can use Network Topology Views to see different aspects of your network. Only devices and links discovered in your network are displayed in network views.

As you use network views, devices and links change dynamically to display changes that the LMS Server discovers in your network. See Table 7-9:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu</td>
<td>Contains Topology Services commands.</td>
<td>See Network Topology View Menu Reference for more information.</td>
</tr>
<tr>
<td>Toolbar</td>
<td>Provides quick access to frequently used menu options.</td>
<td>To show or hide the toolbar, select View &gt; Show Toolbar.</td>
</tr>
</tbody>
</table>
### Table 7-9  Network Topology View Features (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology Filters</td>
<td>Allows you to filter and display devices and links.</td>
<td>Filter device types, LANE components, link types, and discrepancies in your network. For more details on filters, see Using Topology Filters.</td>
</tr>
<tr>
<td>Status Bar</td>
<td>Displays Topology Services system messages on the left and the Discovery Status button on the right.</td>
<td>This window displays Data Collection status. Click the color-coded Status to view the Data Collection statistics.</td>
</tr>
</tbody>
</table>

### Figure 7-3  Network Topology View

1. Menu
2. Toolbar
3. Topology Filters
4. Topology Map
Connecting Securely to Devices From Clients

You can connect securely to a device using SSH. To connect to a device from a client, Microsoft Windows clients must perform the SSH executable configuration.

To connect to the devices securely:

- Specify the SSH Client
- Connect to the device

This section explains:

- Specifying SSH Client
- Connecting to the Device

Specifying SSH Client

To specify the SSH Client:

Step 1  Create a file named campusmgr.properties.

The SSH Client is the default connection type.

If you select Putty as Client

a. Choose SSH as the Connection Type
b. Select Default Settings from the Saved Sessions list
c. Click Save to save the default settings.

To verify whether the default settings have been applied, close Putty and relaunch it.

Step 2  Write the following property in the file:

\texttt{CMSSH=SSH executable file name}

For example,

If you are using Secure Shell:

\texttt{CMSSH=C:\Progra~1\SSHCOM~1\SSHSEC~1\ssh2.exe}

If you are using Putty:

\texttt{CMSSH=C:\PROGRA~1\putty\putty.exe}

Step 3  Save the file in your home directory.

For example, your home directory can be D:\Documents and Settings\admin.
Connecting to the Device

Step 1  Select Monitor > Monitoring Tools > Topology Services.
Step 2  Go to a Network Topology View and right-click a device icon, and select SSH from the popup menu.
Or
Go to a Summary View and right-click a device entry, and select SSH from the popup menu.
The SSH dialog box opens.
Step 3  Enter the username in the User Name field.
Step 4  Click OK to connect or click Cancel to disconnect.
An SSH terminal window opens.

Displaying Network Views

A Network Topology View is a graphical representation of the devices in your network.
To access and display several network and domain views:

Step 1  Right-click a network view from the Tree View in the Topology Services Main Window.
A popup menu appears.
Step 2  Select Display View.
The Network Topology window opens, displaying the specified network or domain view. See Table 7-9 for more information.
Using Panner to View Topology Maps

**Figure 7-4** Panning the Topology Map

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Menu</td>
<td>4</td>
<td>Topology Map</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Toolbar</td>
<td>5</td>
<td>Navigator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Topology Filter</td>
<td>6</td>
<td>Panner Window</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Using Network Views

You can select a network view from the Tree View to display different segments of your network in a Network Topology window.

See Table 7-10 for a list of functions you can perform in Network Topology views.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN Edge View</td>
<td>Shows network connectivity between Layer 3 devices that have routing characteristics. Devices without Layer 3 connectivity are placed in Switch Cloud network views.</td>
<td>View: &lt;br&gt; - Device Attributes&lt;br&gt;- IPv6 Addresses.&lt;br&gt;- Port Attributes.&lt;br&gt;- Change Management IP&lt;br&gt;- Configure Inter-VLAN Routing&lt;br&gt;- Link Attributes&lt;br&gt;- Virtual Network Manager&lt;br&gt;- Aggregate Link Attributes&lt;br&gt;- Delete Links</td>
</tr>
<tr>
<td>Switch Cloud View</td>
<td>Displays the Layer 2 devices between two Layer 3 devices in your network.</td>
<td>View: &lt;br&gt; - Device Attributes&lt;br&gt;- IPv6 Addresses&lt;br&gt;- Port Attributes&lt;br&gt;- Service Attributes&lt;br&gt;- Change Management IP&lt;br&gt;- Configure Inter-VLAN Routing&lt;br&gt;- VLAN Report&lt;br&gt;- Link Attributes&lt;br&gt;- Configure EtherChannel&lt;br&gt;- Create Trunk&lt;br&gt;- Virtual Network Manager&lt;br&gt;- Trunk Attributes&lt;br&gt;- TDR Report&lt;br&gt;- Interface Reports&lt;br&gt;- IPSLA Reports</td>
</tr>
</tbody>
</table>
### Table 7-10  Network View Item Descriptions (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 View</td>
<td>Displays the Layer 2 information about your network, including LAN switches, routers, MLS devices, hubs, and switch probes.</td>
<td>View:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device Attributes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPv6 Addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Port Attributes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Service Attributes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Change Management IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure Inter-VLAN Routing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VLAN Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Link Attributes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure EtherChannel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create Trunk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Virtual Network Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Trunk Attributes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TDR Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Interface Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPSLA Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• End Host Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Switch Port Report</td>
</tr>
<tr>
<td>Unconnected Devices View</td>
<td>Displays devices for which connectivity information could not be obtained, including devices not supported by Topology Services.</td>
<td>View:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device Attributes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPv6 Addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Port Attributes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VLAN Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Virtual Network Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Change Management IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure Inter-VLAN Routing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Link Attributes</td>
</tr>
</tbody>
</table>
Table 7-10  Network View Item Descriptions (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>
| VTP Views     | Shows the devices that are participating in VTP domains. VTP Views also shows the non-VTP devices connected directly to the VTP domain. | View:  
  • Device Attributes  
  • Port Attributes  
  • Service Attributes  
  • VLAN Report  
  • Change Management IP  
  • Configure Inter-VLAN Routing  
  • Link Attributes  
  • Configure EtherChannel  
  • Create Trunk  
  • Virtual Network Manager  
  • Trunk Attributes  
  • TDR Report |

This section contains:
- Customizing Network Topology Views
- Changing Network Topology View Layouts
- Starting Cisco Prime LMS Features and Reports From Topology Views
- Modifying Network View Features

**Customizing Network Topology Views**

You can modify the Network Topology Views to change the location of device icons or links, save Network Topology Views, and remove devices from the Network Topology View.

This section contains:
- Saving Network Topology View Layouts
- Deleting Devices From Network View
- Rediscovering Devices from Topology Services
Saving Network Topology View Layouts

You can customize Network Topology Views by rearranging and dragging devices and links to different locations on the view. This allows multiple users to customize the way the Network Topology Views appear. To do this:

Step 1 Make any changes you want to the Network Topology View.
Step 2 Select File > Save Layout.

Deleting Devices From Network View

To delete devices from any Network Topology View.

Step 1 Select the device you want to delete from the Network Topology View.
Step 2 Select Edit > Delete Devices.
This step only removes the device from the LMS Server database. If the device still exists in your network and is discoverable by the LMS Server, it reappears during the next Data Collection.
If devices that you do not want to get displayed in Topology Services, continue to reappear on the Network Topology View, exclude the devices from Unified Device Manager (UDM) by setting up appropriate device management policies. This permanently deletes the device from LMS.
See Administration of Cisco Prime LAN Management Solution 4.2 for information on setting up device management policies.

Rediscovering Devices from Topology Services

To delete devices from any Network Topology View.

Step 1 Select the device you want to delete from the Network Topology View.
Step 2 Select Edit > Delete Devices.
This step only removes the device from the LMS Server database. If the device still exists in your network and is discoverable by the LMS Server, it reappears during the next Data Collection.
If devices that you do not want displayed in Topology Services continue to reappear on the Network Topology View, go to Inventory > Device Administration > Device Allocation Policy to configure the device allocation policy to delete the device from LMS.
Changing Network Topology View Layouts

To change the layout for each Network Topology View.

**Step 1**
Go to a Network Topology View window and select View > Relayout.

**Step 2**
Select a layout style. See Table 7-11.

### Table 7-11: Layout Style

<table>
<thead>
<tr>
<th>Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circular</td>
<td>Arranges devices in a circular pattern, resizes devices to fit in viewable area.</td>
</tr>
<tr>
<td>Hierarchical</td>
<td>Arranges devices in a hierarchical pattern, resizes devices to fit in viewable area.</td>
</tr>
<tr>
<td>Symmetric</td>
<td>Arranges devices in a compact pattern, resizes devices to fit in viewable area.</td>
</tr>
<tr>
<td>Orthogonal</td>
<td>Arranges devices in an angular pattern. Each link bends at right angles. Individual devices resize to show each link.</td>
</tr>
</tbody>
</table>

Starting Cisco Prime LMS Features and Reports From Topology Views

You can start some of the features or reports of Cisco Prime LAN Management Solution, from Topology maps.
Table 7-12 gives the list of applications that can be launched:

### Table 7-12 Applications Invoked from Topology Maps

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetConfig</td>
<td>Enables you to make configuration changes to all Configuration module supported network devices</td>
</tr>
<tr>
<td>Software Management</td>
<td>Software Management automates the steps associated with upgrade planning, scheduling, downloading software images, and monitoring your network.</td>
</tr>
<tr>
<td>Fault History Report</td>
<td>Fault History provides the history of LMS events.</td>
</tr>
<tr>
<td>Show Fault Monitor Alerts</td>
<td>Launces the LMS report which displays information on the faults and events that are associated with the device.</td>
</tr>
<tr>
<td>Create VRF</td>
<td>Allows you to create VRF on the devices and interfaces in an Enterprise network. For more information on creating VRF, see the Configuration Online help.</td>
</tr>
<tr>
<td>Edit VRF</td>
<td>Enables you to edit the VRF details configured on devices. For more information, see the Configuration Online help.</td>
</tr>
<tr>
<td>Extend VRF</td>
<td>Enables you to extend the VRF functionality to neighboring devices and interfaces. For more information, see the Configuration Online help.</td>
</tr>
<tr>
<td>Edge VLAN Configuration</td>
<td>Enables you to assign edge VLANs to a VRF instance. For more information, see the Configuration Online help.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Enables you to troubleshoot the end-to-end connectivity of devices participating in a VRF. You can troubleshoot using:</td>
</tr>
<tr>
<td></td>
<td>• Ping VRF. For more information on Ping, see Ping or Traceroute.</td>
</tr>
<tr>
<td></td>
<td>• Traceroute VRF. For more information on Traceroute, see Ping or Traceroute.</td>
</tr>
<tr>
<td></td>
<td>• Show Command VRF. For more information on Show Results, see Show Results.</td>
</tr>
<tr>
<td>Software Upgrade</td>
<td>Enables you to upgrade the software of the device to enhance its capability to participate in a VRF.</td>
</tr>
<tr>
<td>Create VLAN</td>
<td>Enables you to create VLAN for selected devices. For more information, see the Configuration Online help.</td>
</tr>
<tr>
<td>Device Dashboard</td>
<td>Launches Performance management device dashboard report</td>
</tr>
<tr>
<td>Create Collector</td>
<td>Allows you to create IPSLA collectors</td>
</tr>
<tr>
<td>Show Collectors</td>
<td>Allows you to list IPSLA collectors</td>
</tr>
<tr>
<td>NAM</td>
<td>Allows you to launch the NAM login page. See Launching NAM from Topology Services for more information.</td>
</tr>
</tbody>
</table>
Launching NAM from Topology Services

You can launch Network Analysis Module (NAM) from the shortcut menu of a NAM supported device managed in Topology Services.

The NAM supported device should be added to DCR to get displayed in the topology views.

To launch NAM from Topology services:

**Step 1**  Select **Monitor > Monitoring Tools > Topology Services**.

**Step 2**  Right-click a device icon from the topology views and select **NAM** from the shortcut menu.

The NAM dialog box opens.

If the device does not support NAM, the NAM menu item is not available in the shortcut menu.

**Step 3**  Select HTTP or HTTPS protocol to connect to the NAM server.

The default is HTTP.

**Step 4**  Enter the port number to connect to the NAM server in the Port Number field.

You can enter the port number value between 1 to 65535.

If you do not enter the port number, the default port number for the protocol selected will be used.

**Step 5**  Click **OK**.

Login page of NAM appears.

If you have already logged onto NAM server, the Overview page (NAM > Monitor > Overview) appears.

If the device has an unsupported version of NAM, then the device is considered as an unsupported device and no data will be fetched.
**Launching VRF-Lite Topology Map**

**Step 1**
Select any device from the map and right-click. You can select multiple devices.
To select multiple devices, press **Ctrl**.

**Step 2**
Select any of the following:

- **VRF Management > Create VRF**
  The Create VRF page with the selected devices is launched. You can create VRF on the selected device.

- **VRF Management > Edit VRF**
  The Edit VRF page appears with the selected devices and corresponding VRF details. You can Edit VRF on the selected device.

- **VRF Management > Extend VRF**
  The Extend VRF page appears with the selected devices and the VRF details of the selected devices is launched. You can extend VRF configuration details to the devices that are neighbors to the selected device.

- **VRF Management > Edge VLAN Configuration**
  The Edge VLAN Configuration workflow is used to access edge VLANs to a VRF instance. This provides an end-to-end virtualization. You can assign Edge VLAN to a VRF by associating it to a Switch Virtual Interface (SVI). You can assign VLANs to VRF at the edge, using the following options:
  - To perform Edge VLAN Configuration at the Distribution Layer, see **Edge VLAN Configuration at Distribution Layer**
  - To perform Edge VLAN Configuration at the Access Layer where Trunk exists on the selected device, see **Edge VLAN Configuration at Access Layer with Trunk**

- **VRF Management > Troubleshooting**
  The Ping or traceroute page is launched. You can troubleshoot the end-to-end connectivity of devices that participate in a VRF. You can troubleshoot using either Ping or Traceroute.
  - **VRF Management > Troubleshooting > Ping VRF**. For more information on Ping, see **Ping or Traceroute**.
  - **VRF Management > Troubleshooting > Traceroute VRF**. For more information on Ping, see **Ping or Traceroute**.
  You can view the results after VRF troubleshooting using **VRF Management > Troubleshooting > Show Results VRF**. For more information on Show Results, see **Show Results**.

- **VRF Management > Software Upgrade**.
  The Software Management page is launched and it displays the selected devices. You can upgrade the device software to make it a VRF capable device. If the device is already VRF Capable, the image can be upgraded to the next available higher version.

- **VRF Management > Create VLAN**
  Using Virtual Network Manager, you can create VLAN. The VLAN configuration page from LMS. The VLAN Configuration page guides you through the VLAN configuration process.
  For more information on Virtual Network Manager, see the Configuration Online help.
**Edge VLAN Configuration at Distribution Layer**

To achieve complete end-to-end VRF configuration, you must virtualize the Distribution Layer by using the Edge VLAN Configuration feature in Virtual Network Manager.

Here, Access VLANs are mapped to a VRF instance to allow the data from the devices in the Distribution layer to participate in a VRF. VLANs are associated to a VRF by associating them to an SVI.

---

**Step 1**
Launch Topology View
The Topology Services page appears.

**Step 2**
Expand the Network View tree and select **Layer 2 View**.

**Step 3**
Right-click the Layer 2 View and select **Display View**.
The Layer 2 View page appears.

**Step 4**
Select a VRF from the VRF filter under Topology Filters.
If you do not select a VRF, you can perform Edge VLAN Configuration on only one device.

**Step 5**
Select the devices from the Distribution Layer.

**Step 6**
Right-click the selected device and select **VRF Management > Edge VLAN Configuration**
If you directly select a device without selecting a VRF, you are prompted to select a VRF from the VRF Selector for the device window. The VRF selector displays a list of VRFs that are configured on the selected device.

The Edge VLAN Configuration: Select Devices page appears.
The Device Selector does not display pure L3 devices. The devices selected in the map view are already selected in the Select Devices page. In this page, you can select more devices to perform Edge VLAN Configuration.

For more information on the Edge VLAN Configuration, see the Configuration Online help.

---

**Edge VLAN Configuration at Access Layer with Trunk**

Consider a scenario where VLAN is not configured on the interface of the selected devices with Trunk configured on the selected devices.

To configure VLAN:

---

**Step 1**
Launch Topology View
The Layer 2 View page appears.

**Step 2**
In the Layer 2 View page, select the devices in the Access Layer.

**Step 3**
Right-click and select **Create VLAN**.
The VLAN Configuration page appears.
For more information on Creating VLAN, see the Configuration Online help.
If Trunk is not configured on the selected device, you can create Trunk by following Step 4 and Step 5.
**Step 4** Select a link connecting devices from the Distribution Layer to the Access Layer.

**Step 5** Right-click the link and select **Create Trunk**.

The Create Trunk page appears.

For more information on Creating Trunk, see the Configuration Online help.

---

**Modifying Fault Management Alert Settings**

After configuring the settings in the Admin page, the Topology maps show all the Critical Warning and Informational alerts, by default.

If you want to see only a certain type of alerts, you can change the settings as follows:

**Step 1** Select **Monitor > Monitoring Tools > Topology Services**.

**Step 2** Launch any Network Topology View.

**Step 3** Right click on the Topology map and choose **Show Fault Monitor Alert**.

Or

Click **View > Show Fault Monitor Alert** from the Topology Services menu.

The following settings are displayed:

- Critical
- Warning
- Informational

These settings are checked by default.

**Step 4** Uncheck the required setting, for which you do not want to display the information.

For example, if you want to display only Critical alerts, leave the Critical option checked and uncheck the other two options.

The Fault Monitor Alert settings is client specific. Therefore, the settings are applied only for your Topology maps and N-Hop View portlet. Other users connected to the same LMS server can choose their own settings.

**Step 5** Click **Apply** to save the settings.

The settings are saved to the server.

**Step 6** Close all Topology Windows and relaunch Topology Services for the change to take effect.
Modifying Network View Features

You can modify and customize various Network Topology View features to suit your operating environment. For example, you can change the display colors and view layout of the Network Topology View.

You can also customize the view features for individual user roles, or modify the default features for all users.

This section contains:
- Changing Network Topology View Properties for One User Role
- Changing Network Topology View Properties for All Users
- Setting Background Images for Topology Views

Changing Network Topology View Properties for One User Role

You can change client map properties for one user role without affecting the Network Topology View properties for other user roles. To do this:

**Step 1**
Go to a Network Topology View and select Edit > Map Preferences.
The Client Map Properties window opens.

**Step 2**
Change the properties as described in Table 7-13.

**Table 7-13**  
Client Network Topology View Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colors</td>
<td></td>
</tr>
<tr>
<td>Map Background</td>
<td>Color of the background in Network Topology Views</td>
</tr>
<tr>
<td>Map Foreground</td>
<td>Color of the foreground in Network Topology Views</td>
</tr>
<tr>
<td>Map Selection</td>
<td>Color of the outline for selected links and devices</td>
</tr>
<tr>
<td>Highlight Color</td>
<td>Color that links and devices are highlighted in</td>
</tr>
</tbody>
</table>
Table 7-13  Client Network Topology View Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Layout Style</strong></td>
<td></td>
</tr>
<tr>
<td>Hierarchical</td>
<td>Reveals precedence relations</td>
</tr>
<tr>
<td>Circular</td>
<td>Portrays interconnected ring and star topologies</td>
</tr>
<tr>
<td>Symmetrical</td>
<td>Produces representations of complex networks</td>
</tr>
<tr>
<td>Orthogonal</td>
<td>Produces graph layouts with edges running parallel to x and y axes</td>
</tr>
<tr>
<td><strong>Label Display Fallback Rule</strong></td>
<td></td>
</tr>
<tr>
<td>Fallback Rule</td>
<td>Allows you to set the order in which device labels appear in Network Topology Views</td>
</tr>
<tr>
<td>Edit Defaults</td>
<td>Allows you to edit the default properties for all users</td>
</tr>
<tr>
<td>Restore Defaults</td>
<td>Allows you to restore the default settings</td>
</tr>
</tbody>
</table>

Step 3  Click Apply to apply these changes based on your current user role.

Changing Network Topology View Properties for All Users

To change the Network Topology View properties for all users:

Step 1  Go to a Network Topology View and select Edit > Map Preferences.

Step 2  Click Edit Defaults.

The Client Default Properties window opens.

Step 3  Change the Network Topology View properties as described in Table 7-14.

Table 7-14  Default Network Topology View Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Colors</strong></td>
<td></td>
</tr>
<tr>
<td>Network Topology View Background</td>
<td>Color of the background in Network Topology Views</td>
</tr>
<tr>
<td>Network Topology View Foreground</td>
<td>Color of the foreground in Network Topology Views</td>
</tr>
<tr>
<td>Network Topology View Selection</td>
<td>Color of the outline for selected links and devices</td>
</tr>
<tr>
<td>Highlight Color</td>
<td>Color that links and devices are highlighted in</td>
</tr>
</tbody>
</table>
Using Network Views

To trim SysName based on Domain suffix, enable Trim Domain Suffix On Labels, specify Domain Suffix value and ensure that Trim SysName On Labels is not enabled.

Click Apply to change the Network Topology View preferences for all users.

### Setting Background Images for Topology Views

You can set an image as the background of the Network Topology Views in Topology Services. LMS allows you to upload images and set the image, where the image is in GIF, JPEG, or JPG image formats.

This section contains:

- **Uploading the Image**
- **Selecting the Image**
- **Deleting the Image**

To set the background image:

1. Upload the image.
2. Set the image as the background image.
Using Network Views

Chapter 7      Using Topology Services

Uploading the Image

To upload and set the background image:

Step 1  Right-click any Network View from the Tree View in the Topology Services Main Window.
Step 2  Select Display View from the pop up menu.
        The Network Topology window appears.
Step 3  Select Edit > Map Preferences from the menu.
        The Client Map Properties window appears.
Step 4  Click Upload Image, in the Map Background Image section.
Step 5  Select the file from the list in the Upload Map Background Image window, and click Open.

Selecting the Image

After you finish uploading the image, you can select and set the background for each network view.
To select an image for the background:

Step 1  Select Edit > Map Preferences from the menu in the Network Topology Display view.
        The Client Map Properties window appears.
        • Select an image from the drop-down menu for Background Image, in the Map Background Image section.
        • If you do not want to set an image, select the default None.
Step 2  Click Apply.
Step 3  Click OK.

Deleting the Image

To delete the image from the list of images that you have uploaded.

Step 1  Select Edit > Map Preferences from the menu from the Network Topology Display view.
        The Client Map Properties window appears.
Step 2  Select an image from the drop-down menu for Background Image, in the Map Background Image section.
Step 3  Click Delete Image.
Understanding Cluster Switches

LMS is now enhanced to discover Commander and member devices of a Switch Cluster. You can create and delete VLANs in these switches.

You can configure switch clusters to manage a set of switches using a single IP address. Switch cluster is a group of switches connected to each other, where one switch is designated as the Command switch and upto 15 switches can be designated as Member switches.

Communication to all these member switches is carried out through the command switch. The Command switch is the single point of contact for configuring, managing, and monitoring the cluster of switches. A member switch can not be a member of any other cluster at a point of time.

Clustering the switches allows you to:

- Manage a group of switches using a single IP address, especially when you have a limited number of IP addresses.
- Manage switches regardless of them being distributed across Layer 2 or Layer 3 networks. The member switches are connected to the Command switch through one common VLAN.
- Designate standby Command switch to avoid losing connectivity with the member switches.

Restrictions:

- Command switch cannot be a member or command switch of another cluster.
- Commander switches must connect to standby Command switches only through the management VLAN.

For information on displaying Cluster switches in Topology maps, see Displaying Cluster Switches.

Displaying Cluster Switches

LMS discovers and displays the switches participating in clustering and the devices connected to the cluster members.

To display the cluster members:

**Step 1**
Go to the Tree View in the Topology Services Main Window and right-click any Network View.

**Step 2**
Select Display View from the pop up menu.

The Network Topology window appears. The Map displays the Command switch using an icon, which you can see in Using Topology Services Legend.

The member switches of the cluster displays the IP address of the Command switch and the member number, in the following format: IP address-Member Number. For example, 10.77.210.211-2, where 10.77.210.211 is the IP address of the Command switch and 2 is the member number.

To display the IP address, select View > Display Labels > Show IP, from the Menu on Topology Map.
Using Topology Filters

You can filter devices, links, and networking services, and locate these items on the Network Topology Views. Many different filters are available, but the availability of specific filters varies among each of the different Network Topology Views.

You can use multiple filters at the same time to display more than one media type.

This section contains:

- Link Virtualization Status
- Enabling RMON to Measure Bandwidth Utilization
- Customizing Bandwidth Utilization Filters
- Highlighting Filtered Devices

To filter devices:

**Step 1** Select **Monitor > Monitoring Tools > Topology Services** from the menu. The Topology Services Main Window appears.

**Step 2** Go to the Tree View in the Topology Services Main Window, right-click the Network View you want and select **Display View** from the pop up menu. The Network Topology View appears.

**Step 3** Toggle any top-level item in the Topology Filters list to display additional options.

Table 7-15 describes various filters.

<table>
<thead>
<tr>
<th>Table 7-15</th>
<th>Topology Filters Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Types Filter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Device Types</td>
<td>Filters by individual device; for example, Catalyst 5000.</td>
</tr>
<tr>
<td>Link Types</td>
<td>Filters by type of link; for example, Ethernet100M.</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>—</td>
<td>Filters by Topology Groups in the Map. The filter displays the number of Groups displayed in the Map, in parentheses. For example, Topology Groups (3).</td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>—</td>
<td>Filters by the service running on the device. For example, Cisco CallManager.</td>
</tr>
<tr>
<td><strong>Device Status</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Reachable</td>
<td>Filters based on status of the device (reachable).</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Filters based on status of the device (unreachable).</td>
</tr>
<tr>
<td><strong>Internal Routers</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>—</td>
<td>Filters by the routers. For example, RSM/MSFC.</td>
</tr>
<tr>
<td><strong>Discrepancy</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Physical</td>
<td>Filters by physical discrepancy; for example, link speed.</td>
</tr>
</tbody>
</table>
Chapter 7      Using Topology Services

Using Topology Filters

<table>
<thead>
<tr>
<th>Network Address Filters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>Filters based on the protocols supported on the devices. For example, IPv6.</td>
</tr>
<tr>
<td>STP Inconsistency</td>
<td>Filters based on STP loop, PVID, device, or type inconsistencies.</td>
</tr>
</tbody>
</table>

Spanning Tree

| —                      | Filters based on the spanning tree details of devices. Selecting the filter will result in a view listing the VLANs applicable to all the switches in the selected switch cloud. |

PoE Devices

| PoE Capable Devices    | Filters based on the Power over Ethernet (PoE) capability of the device. Selecting the filter will highlight the devices that are PoE capable in the displayed network view. PoE is the ability of the LAN switching infrastructure to provide power over the ethernet copper wire to an endpoint (device). |

TDR

| TDR Links              | Filters by the TDR enabled links. |

VRF

<table>
<thead>
<tr>
<th>Readiness</th>
<th>Filters based on the readiness information of the following devices:</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF Capable Devices</td>
<td>Represents the devices with necessary hardware support.</td>
</tr>
<tr>
<td>VRF Supported Devices</td>
<td>Represents the VRF supported devices.</td>
</tr>
<tr>
<td></td>
<td>However, the software must be updated to configure VRF.</td>
</tr>
<tr>
<td></td>
<td>You can filter devices based on only one Readiness filter at a given time.</td>
</tr>
<tr>
<td>VRF List</td>
<td>Filters based on the list of VRFs present in the Network Enterprise.</td>
</tr>
<tr>
<td></td>
<td>The VRF Collection process collects the VRFs in your network. By default, the VRF collection process is scheduled to run after the Data Collection process has completed.</td>
</tr>
<tr>
<td></td>
<td>To get the latest VRFs under VRF Filters, you must relaunch the Display View.</td>
</tr>
<tr>
<td></td>
<td>When you select a VRF, the Map view displays the devices participating in the selected VRF along with the virtualization status of the links that connect two devices. You can view the following details based on the VRF filters:</td>
</tr>
<tr>
<td></td>
<td>Devices participating in a VRF</td>
</tr>
<tr>
<td></td>
<td>Link virtualization status of the link connecting any two devices in the Map view.</td>
</tr>
<tr>
<td></td>
<td>You can filter devices based on only one VRF at a given time.</td>
</tr>
</tbody>
</table>

VTP

| Trunk Encapsulation    | Filters based on the trunk encapsulation enabled on devices. |
| VTP Devices            | Filters based on the devices running VTP. |

Bandwidth Utilization

| Low                    | Filter for highlighting the links that are in the low utilization range. |
| Medium                 | Filter for highlighting the links that are in the medium bandwidth utilization range. |
| High                   | Filter for highlighting the links that are in the high bandwidth utilization range. |

Table 7-15 Topology Filters Description (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Address Filters</td>
<td>---</td>
</tr>
<tr>
<td>PoE Devices</td>
<td>---</td>
</tr>
<tr>
<td>VRF</td>
<td>---</td>
</tr>
<tr>
<td>VTP</td>
<td>---</td>
</tr>
<tr>
<td>Bandwidth Utilization</td>
<td>---</td>
</tr>
</tbody>
</table>
Link Virtualization Status

You can get the virtualization status by hovering the mouse over the links displayed in the Map view in Topology Services.

- Grey links have both From and To interfaces that do not participate in the selected VRF.

In the Figure 7-5, the Green VRF is selected. When you select the Green VRF, the Map view displays the number of devices and the interfaces participating in the Green VRF. The devices that are greyed out do not participate in the Green VRF. The devices participating in the Green VRF are highlighted in the Map view in Topology Services.

The interface in grey means that both the interfaces (Gi4/9 and Fa4/0) do not participate in Green VRF.

Figure 7-5  Grey Links - Neither Interfaces are a Part of VRF
- Cyan links have only one interface that participate in the selected VRF.
  In the Figure 7-6, the Blue VRF is selected. When you select the Blue VRF, it displays the status of the devices and interfaces participating in the Blue VRF. Here, two devices are a part of the Blue VRF. The devices that are not participating in Blue VRF are greyed out.
  The interface in Cyan means that only one interface (Fa0/1) is participating in the Blue VRF.

Figure 7-6    Cyan Links - Only One interface Part of VRF

- Black links represents the links with both from and to interfaces that participate in Green VRF.
  Black links have both From and To interfaces participating in the selected VRF.
  In the Figure 7-7, the Green VRF is selected. The selection of Green VRF displays the status of the devices and interfaces participating in the Green VRF. Here, four devices are a part of Green VRF. One device is greyed out because it is not participating in the Green VRF.
  The interface in Black means that both interfaces (Fa0/0 and Fa0/1) are participating in Green VRF.
You can filter devices based on only one VRF at a given time.

**Step 4** Select the check box next to any option to filter specific items.

- If you select multiple options from two different top-level filters (such as Types and VTP), your selection is an assumed Boolean AND expression.
  
  This requires that *all* criteria be met to highlight devices on the Network Topology View. Therefore, only those devices supporting active links of the selected type are displayed.

- If you select multiple options from the same top-level filter (such as Device and Link), your selection is an assumed Boolean OR expression.
  
  This requires that *any* criteria be met in order to highlight the selection on the Network Topology View. However, for discrepancy filters, selecting multiple options from the same top-level filter will assume an AND operation.

- If you choose to filter by a Service, the application servers that are configured to run that service, are highlighted on the map.
  
  However, you must complete the Displaying Service Attributes procedure to determine whether the specified Service (or any other Service) is currently active on the application server.

**Step 5** Select Edit > Highlight Filtered to highlight the filtered items.

To deselect items and check boxes that you have selected and return to the normal view, select Edit > Clear Highlighting.
This topic contains:

- Enabling RMON to Measure Bandwidth Utilization
- Customizing Bandwidth Utilization Filters
- Highlighting Filtered Devices

**Enabling RMON to Measure Bandwidth Utilization**

Bandwidth Utilization is the measure of traffic flowing across a link. LMS highlights bandwidth utilization across links, in the Topology maps. It computes the bandwidth utilization by taking the best estimate of the mean physical layer network utilization on the links, during the sampling time interval.

In Topology Map, LMS can differentiate the links using colors, based on the bandwidth utilized by them. You can customize the filters to display bandwidth utilization.

For more details, see Customizing Bandwidth Utilization Filters.

This section contains:

- Modifying the Parameters
- Enabling RMON on All Ports in Selected Devices
- Enabling RMON on Selected Ports in Selected Devices
- Disabling RMON

**Note**

LMS computes bandwidth utilization only on ethernet links, and not on any other type of link.

To compute bandwidth utilization in LMS, you must enable Remote Monitoring (RMON). Enabling RMON depends on two parameters.

**Parameters to Compute Bandwidth Utilization**

Enabling RMON depends on the following parameters:

- Bucket Size—Number of samples (incoming and outgoing packets) that will be examined for a given point of time.
- Interval—Duration for which samples are to be collected.

The default values for Bucket Size and Interval are 10 and 300 respectively. Though you cannot edit the values through the user interface of LMS, you can reconfigure these values through command line interface. For more details see Modifying the Parameters.

LMS computes bandwidth utilization only for those devices that have the same parametric values as configured and displayed in the RMON Settings page. This application allows you to configure only the same parametric values on all link ports. This is to avoid conflicts in computation.

**Enabling RMON on Ports**

LMS allows you to enable RMON on:

- All Ports in selected devices. For details, see Enabling RMON on All Ports in Selected Devices
- Selected Ports in selected devices, see Enabling RMON on Selected Ports in Selected Devices

LMS highlights links in the Topology Map even if the devices are managed by other applications such as Fault Management, HPOV, or CiscoView.
This topic contains:

- Modifying the Parameters
- Enabling RMON on All Ports in Selected Devices
- Enabling RMON on Selected Ports in Selected Devices
- Disabling RMON

### Modifying the Parameters

The default Bucket Size is 10 and the Interval is 300 seconds. LMS does not compute bandwidth utilization for the links whose ports have different Interval values.

You can configure new values for the parameters in the ANIServer.properties file. To reconfigure the values, you must restart the ANI server so that the file takes the new value.

For computing bandwidth utilization, LMS takes only the latest values in the ANIServer.properties file. You must reconfigure the link ports according to the values set in the properties file for Topology Map to highlight the links.

You must reconfigure the parametric values before you enable RMON on ports.

**Note**

You must configure the same value for Interval across the devices.

To reconfigure the values:

**Step 1**
Enter `pdtterm ANIServer` at the command line to stop the ANI server.

**Step 2**
Go to `NMSROOT/campus/etc/cwsi/ANIServer.properties`.

**Step 3**
Modify the values of the properties, `RMON.interval` for Interval and `RMON.bucketSize` for the Bucket Size.

The maximum value that you can enter for `RMON.interval` is 3600 seconds (One hour).

**Step 4**
Enter `pdexec ANIServer` at the command line to start the ANI server.

After modifying the bucket size and interval, enable RMON in devices as explained in Enabling RMON on All Ports in Selected Devices or Enabling RMON on Selected Ports in Selected Devices.

You can use `RMON.percentageTolerance` property in the ANIServer.properties file to provide a value for the Interval in a range. This is a hidden property that creates a range for the Interval value.

The property adds a value to the current interval that forms the upper limit and subtracts a value from the current interval that forms the lower limit of the range. The default hidden value is 10 percent of the interval.

For example, if the value provided in the ANIServer.properties file is 300, the range will be 270-330. Thus, the samples are collected for the range of 270 to 330 seconds.
If you want to change this default value, you must:

**Step 1**
Stop the ANI server.

**Step 2**
Enter `pdterm ANIServer` at the command line to stop the ANI server.

**Step 3**
Go to `NMSROOT/campus/etc/cwsi/ANIServer.properties`.

**Step 4**
Enter `RMON.percentageTolerance=value`.

**Step 5**
Start the ANI server.

**Step 6**
Enter `pdexec ANIServer` at the command line to start the ANI server.

---

**Enabling RMON on All Ports in Selected Devices**

To enable RMON on all ports in selected devices:

**Step 1**
Click **Admin > Network > Monitor / Troubleshoot > RMON Configuration**.

The Enable RMON dialog box appears. The Device Selector pane displays a list of all devices.

**Step 2**
Select the check box corresponding to the devices for which you want to enable RMON.

The RMON Settings area displays the default Bucket Size required as 10; and the Interval in seconds as 300.

For a Bucket Size of 10, and interval of 300 seconds, LMS collects 10 samples of bandwidth utilization across links over a period of 50 minutes, with an interval of 5 minutes (300 seconds).

To modify the Bucket Size and Interval, see **Modifying the Parameters**. If you modify the parameters, repeat all the steps listed in this section, for enabling RMON with the new parameters.

**Step 3**
Check the **Configure on all links** check box to configure all the ports of the selected devices in the Device Selector.

**Step 4**
Click **Configure** to enable RMON on all the ports in the selected devices.

The following command is configured on the selected ports:

```
rmon collection history integer owner ownername buckets bucket-number interval seconds
```

Example:

```
rmon collection history 4 owner campusmanager buckets 10 interval 300
```
Enabling RMON on Selected Ports in Selected Devices

To enable RMON on selected ports in selected devices:

**Step 1**  
Click **Admin > Network > Monitor / Troubleshoot > RMON Configuration**.  
The Enable RMON dialog box appears. The Device Selector pane displays the list of devices.

**Step 2**  
Select the check box corresponding to the devices for which you want to enable RMON.  
The RMON Settings area displays the default Bucket Size required as 10; and the Interval in seconds as 300.  
For a Bucket Size of 10, and interval of 300 seconds, LMS collects 10 samples of bandwidth utilization across links over a period of 50 minutes, with an interval of 300 seconds (5 minutes).  
To modify the Bucket Size and Interval, see **Modifying the Parameters**. If you modify the parameters, repeat all the steps listed in this section, for enabling RMON with the new parameters.

**Step 3**  
Uncheck the Configure on all Links check box since it is checked by default.

**Step 4**  
Click **Select links** to select the ports for which you want to enable RMON.  
It displays the list of ports in the selected devices. For details on the list displayed, see **Table 7-16**.  
The Select Links check box is enabled only when you uncheck the Configure on all links check box.

<table>
<thead>
<tr>
<th>Table 7-16</th>
<th>Select Links for RMON Configuration</th>
<th>Column Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Name of the port.</td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device where the port is connected.</td>
<td></td>
</tr>
<tr>
<td>Device Address</td>
<td>The IP address of the device.</td>
<td></td>
</tr>
<tr>
<td>isLink</td>
<td>True is displayed for link ports and False for a non-link port.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**  
Select check boxes corresponding to the ports for which you want to enable RMON.

**Step 6**  
Click **Configure** to enable RMON on the selected ports.  
The following command is configured on the selected ports:  
```
rmon collection history integer owner ownername buckets bucket-number interval seconds
```
Example:
```
rmon collection history 4 owner campusmanager buckets 10 interval 300
```
Disabling RMON

After you have enabled RMON on a device through LMS, you can disable it using Command Line Interface (CLI) only.

Commands to Disable RMON

For a device running Cisco IOS, enter the following command at the CLI prompt:

```
no rmon
```

For a device running Catalyst operating system, enter the following command at the CLI prompt

```
set snmp rmon disable
```

Customizing Bandwidth Utilization Filters

You can customize the three ranges of bandwidth utilization, which are low, medium, and high, provided in the Topology Filters. You can also customize the colors for the links in different ranges of bandwidth utilization.

To customize the range of utilization and the color for the ranges:

1. Select Monitor > Monitoring Tools > Topology Services from the menu. The Topology Services Main Window appears.
2. Select Edit > Bandwidth Filter Settings. The Bandwidth Filter Settings window appears.
3. Select the percent of utilization and color you want to specify for each range.
   For example, if you want to displays links with utilization between 0 to 40% in Yellow, set
   - **From %** to 0
   - **To %** to 40
   - **Color** to Yellow
4. Click Apply to save the changes.
   Now the links with 0 to 40% utilization will appear in yellow in all the topology maps.
Highlighting Filtered Devices

You can highlight the devices that you have filtered using the Topology filters. To do this:

**Step 1**  
Select the required Topology Filters from the Network Topology View.

**Step 2**  
Select **Edit > Highlight Filtered** from the menu.  
Or  
Right-click the topology map and select **Highlight Filtered** from the popup menu.  
The topology map highlights the devices that are being filtered.

**Step 3**  
To clear the highlight on the devices, select **Edit > Clear Highlighted** from the menu.

Using Find in Network Topology Views

You can locate specific devices in your network by searching for the device name or device address. You can do this by using the **Find** option. To do this:

**Step 1**  
Go to a Network Topology View and select **Edit > Find**.

**Step 2**  
Enter the required information as described in Table 7-17.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find Device By</td>
<td>Select search criteria:</td>
<td>Use the drop-down list box to find devices by device name or IP address.</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the desired search string</td>
<td>Use this field to narrow the number of matches by entering part or all of the device name or IP address.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists devices that match the specified criteria</td>
<td>Select the device from the list of matches.</td>
</tr>
<tr>
<td>Add to current Network Topology View selection</td>
<td>Selects the device without resetting the currently selected devices</td>
<td>Use this option if you are selecting several devices, and want to add this device to those selected.</td>
</tr>
</tbody>
</table>

To highlight the device in the Network Topology View window, click **Find**.
Understanding Summary View

You can use the Summary View to monitor the current configuration of your network and easily find devices in your network.

The Summary View allows you to obtain summary information about the managed domains, logical components, and physical topology of your network. See Interpreting Summary Information for details on summary information.

**Note**
You can select multiple rows from the table and display the context sensitive menus.

This topic contains:
- Highlighting Devices From Summary View
- Interpreting Summary Information
- Interpreting Network View Summary Information
- Interpreting Unconnected Device View Summary Information

Highlighting Devices From Summary View

You can select a device and choose to highlight the device in the Network View from the Summary View in the Topology Services Main Window. To do this:

**Step 1**
Select **Monitor > Monitoring Tools > Topology Services** from the menu.

The introduction page for Topology Services appears.

**Step 2**
Click **Launch Topology Services**.

The Topology Services Main Window appears.

**Step 3**
Select the device listed in the Summary View.

**Step 4**
Right-click the device and select **Highlight Device** from the popup menu.

The Topology Map appears with the highlighted device.

Interpreting Summary Information

To interpret summary information see the following sub-sections:
- Interpreting Network View Summary Information
- Interpreting Topology Groups Summary Information
Interpreting Network View Summary Information

To display summary information about items in the network views, click a Network View from the Tree View in Topology Services.

See Table 7-18 to interpret this information.

<table>
<thead>
<tr>
<th><strong>Table 7-18</strong></th>
<th><strong>Network View Field Descriptions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Devices</td>
<td>Number of devices displayed on the particular view.</td>
</tr>
<tr>
<td>Switches</td>
<td>Number of switches.</td>
</tr>
<tr>
<td>Routers</td>
<td>Number of routers.</td>
</tr>
</tbody>
</table>

**Device List**

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Product type.</td>
</tr>
<tr>
<td>State</td>
<td>Current status of device; that is, whether it is reachable or not.</td>
</tr>
</tbody>
</table>

Interpreting Unconnected Device View Summary Information

To display summary information about items in the unconnected device views, click Unconnected Devices View from the Tree View in Topology Services.

See Table 7-19 to interpret the fields in the Unconnected Devices View Summary.

<table>
<thead>
<tr>
<th><strong>Table 7-19</strong></th>
<th><strong>Device View Summary</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Devices</td>
<td>Number of devices displayed in the particular view.</td>
</tr>
<tr>
<td>Switches</td>
<td>Number of switches in the selected view.</td>
</tr>
<tr>
<td>Routers</td>
<td>Number of routers in the selected view.</td>
</tr>
</tbody>
</table>

**Device List**

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the device.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Product type.</td>
</tr>
<tr>
<td>State</td>
<td>Current status of the device; whether it is reachable or not.</td>
</tr>
<tr>
<td>Neighbors</td>
<td>Devices that are physically connected to the selected device.</td>
</tr>
</tbody>
</table>
Upgrading Network Topology Views

After an upgrade installation or manual data import from LMS 2.x, you may upgrade the Layer 2 View, LAN Edge View, or Unconnected Devices View that was saved in LMS 2.x to the new LMS format.

If this upgrade is not performed, you can directly use the default views, with enhanced features, generated by LMS Network Topology Functionality.

You can perform the following upgrade procedure more than once. To do this:

**Step 1**
Go to the Topology Services Main Window and select **File > Upgrade View layouts**.

The Upgrade Topology Views window appears.

**Step 2**
Select the views to upgrade.

**Step 3**
Click **Upgrade** to upgrade the views.

**Step 4**
Select the corresponding views from the side panel in the Topology Main Window.

**Step 5**
Select **Display View**.

---

**N-Hop View Portlet**

N-Hop View portlet is an HTML based light weight feature and is available as a part of Monitoring Dashboard. This is much faster than the regular Topology services.

This portlet displays a N-hop view from a specified device. It should be used to view a limited set of devices. See Configuring the Portlet for details on configuring this portlet.

N-Hop view displays only the devices your are authorized to view, if LMS is integrated with Local RBAC and the option Set Topology to RBAC mode is checked.

Using N-Hop view, even if more than 30 devices are present within the specified Hop Count of the root device, you can view a network of up to 30 devices only. You can view the other part of the network by randomly selecting a root device and specifying a Hop Count for the root device. To view the entire network, use Topology Services.

Using N-Hop View, you can:

- Select any device, right-click and choose **Software Management**
  
  It cross-launches to the Software Distribution page. This page enables you to distribute the images in your network.

- Select any device, right-click and choose **NetConfig**
  
  It cross-launches to the NetConfig page. This page enables you to manage NetConfig jobs. The page allows you to apply a set of commands (a task) on selected devices. You can create your own custom tasks that run on multiple devices.

- Select any device, right-click and choose **Troubleshoot**.
  
  The **Device Troubleshooting Report** page is launched. This page displays details about the device. In case of devices that are down, you can use these details to analyze why the device is unreachable.

- Select any device from the map and right-click and choose **Device Dashboard**.
  
  The Device Dashboard report is launched, which provides performance details for the device.
• Select any link from the Topology map and right-click and choose **Interface Report**. The Interface Report for that particular link is launched, displaying the last one hour data.

• Select any IPSLA capable device, right click and choose **Show Collector or Create Collector**. The corresponding Collector Management page is launched. You can create collectors only on devices which are IPSLA capable.

• Select any device, right-click and choose **Show Fault Monitor Alert**, to see the alerts associated with the device.

• Select any device, right-click and choose **Fault History Report**, to see the history of Fault Management events.

• Access a device using Telnet. To do so, choose a device, right click and choose **Telnet**.

• You can display the following information in the map:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>IP Address of the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>devicename</td>
<td>Name of the device</td>
</tr>
<tr>
<td>sysName</td>
<td>sysName</td>
</tr>
<tr>
<td>sysContact</td>
<td>Contact person for that device</td>
</tr>
<tr>
<td>sysLocation</td>
<td>Physical location of the device</td>
</tr>
<tr>
<td>sysOID</td>
<td>Value of the System Object Identifier MIB variable of the device</td>
</tr>
</tbody>
</table>

- To view information, right click anywhere in the map and select the required value. The selected information is displayed for all devices.

- To hide the displayed information, right click anywhere in the map and select **Show/Hide Labels**. Move the mouse over the label to display this relevant information.

• Drag the labels anywhere inside the map. To set it to its original position, right click in the map and choose **Reset Draggables**.

• Print the N-hop view by right-clicking anywhere in the map and choose **Print View**.

Before printing the N-hop view, we recommend that you provide the following browser settings:

For Internet Explorer:

1. Go to **Tools > Internet Options > Advanced Tab > Printing**

2. Check Print background colors and images under Printing
For Mozilla Firefox:

1. Go to File > Page Setup > Format & Options Tab
2. Check Print Background (Colors & Images) under Options

- You can view the details about a single device/link.
  - Click the link Show Properties at the top right corner (This link toggles between Show properties and Hide Properties).
  - Choose a device or link. Properties of the device or link are displayed as explained below:

### Device Details

<table>
<thead>
<tr>
<th>Devicename</th>
<th>Name of the device</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP Address of the device</td>
</tr>
<tr>
<td>status</td>
<td>Indicates if the device is up or down</td>
</tr>
<tr>
<td>imageVer</td>
<td>Version details of the image installed in the device</td>
</tr>
<tr>
<td>sysLocation</td>
<td>Physical location of the device</td>
</tr>
<tr>
<td>sysName</td>
<td>sysName</td>
</tr>
<tr>
<td>sysContact</td>
<td>Contact person for that device</td>
</tr>
<tr>
<td>sysOID</td>
<td>Value of the System Object Identifier MIB variable of the device</td>
</tr>
</tbody>
</table>

### Link Details

<table>
<thead>
<tr>
<th>Link Status</th>
<th>Indicates whether the link is up or down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device IP</td>
<td>IP Address of the device. Shown for both devices between which the link is configured.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface in the device. Shown for both devices between which the link is configured.</td>
</tr>
</tbody>
</table>

### Configuring the Portlet

To configure the N-Hop View portlet:

**Step 1** Select Monitor > Dashboards > Monitoring from the menu and locate the N-Hop view portlet.

**Step 2** Move the mouse over the top right corner of the N-Hop View portlet and choose Configuration.

The configuration screen is displayed.

**Step 3** Enter the IP address or the Device name of the root device.

If the device you specify is not managed by LMS, it will display an error message.

**Step 4** Enter the number of hops in the Hop count field.

The Network Topology map is drawn for the specified number of hops.

**Step 5** Add the device to the critical device poller by checking the Poll devices check-box.

LMS polls the network periodically. If you need to monitor the status of a certain device more frequently, add it to the critical device poller.

This device is removed from the critical device poller list when you close the N-Hop View portlet window.
To display Fault Management alerts in N-Hop view, choose Show Fault Monitor Alerts.

- To display Critical alerts, choose Critical.
- To display Warning alerts, choose Warning.
- To display Informational alerts, choose Information.

For the above feature to work, the Fault Monitor poller should be enabled. For details on this, see Administration of Cisco Prime LAN Management Solution 4.2.

**Step 6** Select the time interval from the Refresh Every drop-down list. This interval can be in minutes or hours. By default, the portlet refreshes the Topology map every 5 minutes. If you set the time interval, it refreshes accordingly. For every refresh, the data is fetched from the last polling cycle of the critical device poller.

**Step 7** Click Save.

**Step 8** Click the back arrow to view the Topology map for the configured device.

---

### Using Microsoft Visio With Topology Views

You can export the network clouds, aggregate links, device nodes, links, buses, and all associated labels into a Visio drawing.

You can export Network Topology Views to Visio 2003 as an XML file. For more details, see Exporting Network Topology Views to Visio. Visio 2003 does not support CSV file format.

To export Network Views to Microsoft Visio 2002 or previous versions, there are two options:

1. Export to .CSV file. To do so,
   - Download the Cisco stencil file (cm_cisco.vss).
     - This file stores images of Cisco devices that Visio uses to create the drawing. For more details, see Downloading the Cisco Visio Stencil File.
   - Export Network Topology Views to Visio.
     - For more details, see Exporting Network Topology Views to Visio.

2. Export to an XML file.
   - For more details, see Exporting Network Topology Views to Visio.
Download the Cisco Visio Stencil File

You must download the Cisco stencil file if you want to export Network Topology views to Visio 2002 or previous versions. See Exporting Network Topology Views to Visio for more details. To do this:

Step 1 Select File > Download Visio Stencil from a Network Topology View.
Step 2 Navigate to the Solutions directory where Visio is installed.
The directory path is usually Visio\Solutions

Caution Do not change the default filename.
Step 3 Click Save.

Exporting Network Topology Views to Visio

To export Network Topology views to Visio:

Step 1 Select the devices you want to export from a Network Topology view.
Step 2 Select File > Export ToVisio.
Step 3 Select either of the following options:
  • Export To csv...
    Saves the Network Topology view as a .CSV file, which you can open in Visio 2002 or previous versions and convert into a Visio drawing. When you open the saved text file in Visio, select comma as the delimiter to use. See the Visio manual on how to create drawings from external data.
Or
  • Export To xml...
    Saves the Network Topology view as a .VDX file, which you can open in Visio 2003. Proceed to Step 5.
Step 4 Navigate to the directory where you saved the Cisco stencil file (cm_cisco.vss).
Step 5 Accept the default or enter a filename.
Step 6 Click Save.

Note When you try to export more than 50 nodes from the Topology view, there will be loss of clarity in the exported Visio diagram.
Working With Links

You can use Network Topology Views to display information about links between discovered devices and the type of link connecting the devices. This section explains:

- Interpreting Link Tooltips
- Displaying Link Attributes
- Displaying Aggregate Link Attributes

Interpreting Link Tooltips

Link tooltips provide detailed information about links. They appear as popup windows as you move the cursor over different items in the discovered network.

Some network types display additional information in the tooltips. Use Table 7-20 to help you interpret the tooltips that appear.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Links</td>
<td>Connecting switch name or IP address:slot/port (media type, media speed)</td>
<td>172.18.2.25:2/4 - 172.18.2.2:1/3 (Ethernet 100M)</td>
</tr>
<tr>
<td>Buses</td>
<td>Media type</td>
<td>Ethernet bus, FDDI</td>
</tr>
</tbody>
</table>

Displaying Link Attributes

You can display information about the links between devices in your network.

From a Network Topology View, right-click a link and select Link Attributes from the popup menu, or select Reports > Link Attributes.

The Link Attributes window opens. See Interpreting Link Attributes for more information.
Chapter 7      Using Topology Services

Section: Working With Links

Interpreting Link Attributes

See Table 7-21 to interpret the fields shown in the Link Attributes window.

### Table 7-21   Link Attribute Window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Device from which link originates</td>
</tr>
<tr>
<td>To</td>
<td>Device at which link ends</td>
</tr>
<tr>
<td>Device</td>
<td>Device name</td>
</tr>
<tr>
<td>Interface</td>
<td>Port to which link is connected on the originating and ending devices</td>
</tr>
<tr>
<td>Type</td>
<td>Media type of the link, such as Ethernet</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed of the link, such as 10Mbps, which is 10 megabits per second, or 100Mbps, which is 100 megabits per second.</td>
</tr>
</tbody>
</table>

Displaying Aggregate Link Attributes

The aggregation of multiple physical Ethernet links into a single, virtual link allows network managers to speed the flow of traffic through their networks, reaching speeds that would not be possible otherwise.

For example, if you have no access to links any faster than 100 Mbps, you might aggregate four separate channels of 100 Mbps each into a single 400 Mbps channel.

If there are any aggregate links between devices in your network, you can use Topology Services to display information about those aggregate links.

To display information about the aggregate links:

- Right-click a link from a Network Topology View and select **Aggregate Link Attributes** from the popup menu.

Or

- Select **Reports > Aggregate Link Attributes**.

The Aggregate Link Attributes window opens. See **Interpreting Aggregate Link Attributes** for more information.
Interpreting Aggregate Link Attributes

See Table 7-22 to interpret the fields shown in the Aggregate Link Attributes window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Domain from which link originates</td>
</tr>
<tr>
<td>To</td>
<td>Domain at which link ends</td>
</tr>
<tr>
<td>Device</td>
<td>Device name</td>
</tr>
<tr>
<td>Interface</td>
<td>Port to which link is connected on the originating and ending devices</td>
</tr>
<tr>
<td>Type</td>
<td>Media type of the link, such as Ethernet</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed of the link, such as 10 Mbps</td>
</tr>
</tbody>
</table>

Time Domain Reflectometry Reports

Time Domain Reflectometry (TDR) is used to detect faults in a cable. TDR checks and locates open circuits, short circuits, sharp bends, crimps, kinks, impedance mismatches, and other such defects.

Time Domain Reflectometry is required when the application cannot establish a link, or if the link does not perform as expected.

This usually occurs if you:
- Replace a cable.
- Migrate from Fast Ethernet to Gigabit switch.
- Develop new cable plants.

In such cases, the nature of the defect in the cables are important. To detect the defects, you can perform a TDR test on the link. The TDR test checks the various aspects of the performance of physical links and its reliability, and reports status and failure.

This topic contains:
- Understanding Time Domain Reflectometry
- Using Time Domain Reflectometry Reports

Understanding Time Domain Reflectometry

Time Domain Reflectometry detects the defects by sending a signal through a cable, and reflecting it from the end of the cable. Open circuits, short circuits, sharp bends and other defects in the cable, reflects the signal back, at different amplitudes, depending on the severity of the defect.

The TDR measures the time taken by the signal to reflect back and thus calculates the distance to the defect in the cable. When the signal reaches the end of the cable, it reflects at a very low amplitude.
Using Time Domain Reflectometry Reports

LMS supports TDR Cable Diagnostic Test and generates a report listing the results of the test on Cisco Catalyst 6000 switches.

This topic contains:
- Running TDR Test for a Link
- Running TDR Test For a Port

Running TDR Test for a Link

To run the TDR test for a link:

Step 1  Select Monitor > Monitoring Tools > Topology Services from the menu.
Step 2  Select a view that contains the device for which you want to run TDR Test. This view in the Tree View in the Topology Services Main Window.
Step 3  Right-click the view and select Display View.
The Network Topology window for the selected view appears.
Step 4  Select the link for which you want generate TDR Report.
Step 5  Right-click the link.
Step 6  Select TDR Report from the pop up menu.
A message appears:
Running TDR Report may affect data traffic in the link. Do you like to run the TDR Test.
Step 7  Click Yes.
The TDR Report window appears. See Table 7-23 for details on the report.
After you generate the TDR Report you can:

- Print the TDR report. To do so select **File > Print** from the menu.
- Export the report to your machine. To do so select **File > Export** from the menu.

To view the links that support TDR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select <strong>Monitor &gt; Monitoring Tools &gt; Topology Services</strong> from the menu.</td>
</tr>
</tbody>
</table>
| Step 2 | Select a view that contains the device, for which you want to run TDR Test.  
This view is in the Tree View in the Topology Services Main Window. |
| Step 3 | Right-click the view and select **Display View**.  
The Network Topology window for the selected view appears.  
The Topology Filters pane has a filter, TDR. |
| Step 4 | Click **TDR**. |
| Step 5 | Check the check box for TDR Links.  
The supported links are highlighted. |

### Table 7-23 Field Description for TDR Report on Links

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Device</td>
<td>Name of the local device.</td>
</tr>
<tr>
<td>Local Port</td>
<td>Port of the local device.</td>
</tr>
<tr>
<td>Pair</td>
<td>Pair name corresponding to the local port.</td>
</tr>
<tr>
<td>Local Pair Length</td>
<td>Length of the cable from the local device.</td>
</tr>
<tr>
<td>Local Pair Status</td>
<td>Status of the local pair.</td>
</tr>
<tr>
<td>Local Distance To Fault</td>
<td>Distance to the defect on the cable pair, from the local port.</td>
</tr>
<tr>
<td>Local Channel</td>
<td>Channel to which the cable pair is connected.</td>
</tr>
<tr>
<td>Remote Device</td>
<td>Remote device connected to the local device.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Remote port on the remote device.</td>
</tr>
<tr>
<td>Remote Pair</td>
<td>Remote pair connected to the local pair.</td>
</tr>
<tr>
<td>Remote Pair Length</td>
<td>Length of the cable from the remote device.</td>
</tr>
<tr>
<td>Remote Pair Status</td>
<td>Status of the remote pair.</td>
</tr>
<tr>
<td>Remote Distance to Fault</td>
<td>Distance to the defect on the cable pair, from the remote port.</td>
</tr>
<tr>
<td>Remote Channel</td>
<td>Channel to which the cable pair is connected.</td>
</tr>
</tbody>
</table>
Running TDR Test For a Port

**Step 1** Select **Monitor > Monitoring Tools > Topology Services** from the menu.

**Step 2** Select a view that contains the device that has the port for which you want to run TDR Test. This view is in the Tree View in the Topology Services Main Window.

**Step 3** Select the device that has the port for which you want to run TDR Test.

**Step 4** Right-click the device and select **Port Attributes** from the pop up menu.

The Port Attributes window for the device appears.

**Step 5** Select the port for which you want to run TDR Test.

**Step 6** Select **View > TDR Report** from the menu.

A message appears:

Running TDR Report may affect data traffic in the link. Do you like to run the TDR Test.

**Step 7** Click **Yes**.

The TDR report window appears.

See **Table 8-24** for more details on the TDR report.

### Table 7-24 TDR Report on Ports Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Port</td>
<td>Name of the port.</td>
</tr>
<tr>
<td>Pair</td>
<td>Pair name corresponding to the port.</td>
</tr>
<tr>
<td>Pair Length</td>
<td>Cable length from the device.</td>
</tr>
<tr>
<td>Pair Status</td>
<td>Status of the pair.</td>
</tr>
</tbody>
</table>

After you generate the TDR report you can:

- Print the TDR report. To do so, select **File > Print** from the menu.
- Export the report to your machine. To do so, select **File > Export** from the menu.
Working With Devices

You can use a Network Topology View to display information about the routers and switches in your network. This section contains:

- Performing Data Collection for Devices
- Interpreting Device Tooltips
- Displaying Device Labels
- Displaying Device Attributes
- Viewing End Host Report
- Viewing Switch Port Report
- Displaying Port Attributes
- Setting Preferred Management Addresses
- Starting CiscoView
- Starting Telnet
- Starting Device Center
- Working With MLS Devices
- Working With Application Servers
- Displaying Device Service Modules
- Displaying Service Attributes

Performing Data Collection for Devices

You can perform data collection for each device or a group of devices from Topology Services.

**Step 1** Select **Monitor > Monitoring Tools > Topology Services** from the menu.

**Step 2** Select the device entry in Summary View, for which you want to perform the data collection.

**Step 3** Right-click the device entry and select **Perform Data Collection** from the popup menu. 
Or
Select the device from the topology map.

**Step 4** Select **Edit > Perform Data Collection**, or right-click the device and select **Perform Data Collection** from the popup menu.

The status bar displays the message:

```
Request data collection for n device(s) accepted by ANI.
```

The discovery status button on the status bar shows the status as Running.

After the data collection is complete, the status bar displays a message:

```
Data Collection done.
```

The discovery status on the status bar shows the status as Idle.
Interpreting Device Tooltips

A tooltip is a text message that clarifies the purpose or meaning of a user interface element such as a button, a line, or an icon.

Generally, tooltips appear whenever your pointer rests on any user interface element for which a tooltip has been defined. Tooltip messages are displayed against a colored background (typically yellow or lavender) in a rectangle that hovers above the user interface element being described.

Tooltips in Topology Services provide detailed information about devices and links in Network Topology Views.

Some device types display additional information in the tooltips. Tooltip for a device, for example, 172.18.2.11(C3900), contains the device name or the IP address, and the device type in parentheses.

Displaying Device Labels

To display device information labels in Network Topology Views. To do this:

Step 1 Select **View > Display Labels** from the Network Topology View.

Step 2 Select either IP address, device name, or SysName to be displayed.

This topic contains:

- Interpreting Device Labels
- Clearing Device Labels

Interpreting Device Labels

The device labels are then displayed. See **Table 7-25**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the device.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>SysName</td>
<td>SysName of the device.</td>
</tr>
</tbody>
</table>

Clearing Device Labels

To clear device information labels in the Network Topology Views.

From a Network Topology View, select **View > Display Labels > Clear Labels**. The device labels are hidden.
Displaying Device Attributes

To display information about a specific device:

- Right-click a device icon from a Network Topology View, and select **Device Attributes** from the popup menu

Or

- Select **Reports > Device Attributes**.

The Device Attributes window opens. See **Interpreting Device Attributes** for more information.

Viewing End Host Report

To view End Host Report for a specific device:

- Right-click a device icon from a Network Topology View, and select **End Host Report** from the popup menu

Or

- Select **Reports > End Host Report**.

The Quick Report page appears. See the Reports Online help for more information.

Viewing Switch Port Report

To view Switch Port Report for a specific device:

- Right-click a device icon from a Network Topology View, and select **Switch Port Report** from the popup menu

Or

- Select **Reports > Report Generator > Switch Port Report**.

The Device Attributes window opens. See **Interpreting Device Attributes** for more information.

Interpreting Device Attributes

See **Table 7-26** to interpret the fields shown in the Device Attributes window.

<table>
<thead>
<tr>
<th>Table 7-26</th>
<th>Device Attributes Column Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device.</td>
</tr>
<tr>
<td>Type</td>
<td>Cisco product name for the device, such as 7505 or 5500.</td>
</tr>
<tr>
<td>Module</td>
<td>Module type; set to default for devices without modules.</td>
</tr>
<tr>
<td>ID</td>
<td>Module identification (such as slot number for Cisco Catalyst 5000 series switches or switch number for Cisco Catalyst 3000 series switches).</td>
</tr>
<tr>
<td>SubID</td>
<td>Sub is the slot number and the ID is the box number for stackable devices, such as Catalyst 3000 series switches.</td>
</tr>
</tbody>
</table>
Displaying Port Attributes

To display information about the status of the ports in your network.

- Right-click a device icon from a Network Topology View and select Port Attributes from the popup menu
  
  Or

- Select Reports > Port Attributes.

The Port Attributes window opens. See Interpreting Port Attributes for more information.

Interpreting Port Attributes

See Table 7-27 to interpret the columns shown in the Port Attributes Report window.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Device IP</td>
<td>IP address of the device.</td>
</tr>
<tr>
<td>Port</td>
<td>Name of the port.</td>
</tr>
<tr>
<td>Port Description</td>
<td>Description of the port that you have entered.</td>
</tr>
<tr>
<td>Type</td>
<td>Media type, such as Ethernet.</td>
</tr>
<tr>
<td>AdminStatus</td>
<td>Whether port has been brought down intentionally.</td>
</tr>
<tr>
<td>OperStatus</td>
<td>Whether port is active or inactive.</td>
</tr>
<tr>
<td>isLink</td>
<td>If checked, the port is linked to a switch.</td>
</tr>
<tr>
<td>isTrunk</td>
<td>If checked, the port is participating in a VLAN trunk.</td>
</tr>
</tbody>
</table>

| Table 7-26 Device Attributes Column Description (continued) |

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#NumPorts</td>
<td>Total number of ports that the LMS Server has discovered on the device or module.</td>
</tr>
<tr>
<td>Versions</td>
<td>Model-specific string that varies by device type. For example, Cisco Catalyst 5000 series switches display hardware (hw), software (sw), and firmware (fw) versions. However, only the hardware version is displayed for the Cisco Catalyst 3000 series switches.</td>
</tr>
<tr>
<td>Status</td>
<td>Device-specific status string. For example, the Cisco Catalyst 5000 series switches display faulty, no module, stopped, and running. The Cisco Catalyst 3000 series switches display Other, OK, Minor fault, and Major fault.</td>
</tr>
<tr>
<td>Daughter Card</td>
<td>Daughter cards added to modules (for example, the NetFlow Feature Card or the Uplink module for the Supervisor III engine on Cisco Catalyst 5000 series switches).</td>
</tr>
</tbody>
</table>
To see the list of unused ports, select **View > Unused Ports** from the menu.

To see the complete list of ports, deselect **View > Unused Ports** to view the complete list of ports. You can also save or print the lists.

### Setting Preferred Management Addresses

Some devices, such as routers, can have multiple IP addresses. You can set a preferred management address to be used by LMS using either of the following procedures.

**Note**

When you set an IP address as preferred management address, the IP address in the Device and Credential Repository also changes accordingly.

To navigate from Topology Services Main Window:

**Step 1**

Select a view that contains the device, for which you want to set the IP.

This view is in the Tree View in Topology Services Main Window.

**Step 2**

Select a device from the device list in any one of the summary tables.

**Step 3**

Right-click and select **Change Management IP** from the popup menu.

The Select Management IP Address window containing the multiple IP addresses of the selected device appears.
**Starting CiscoView**

You can display specific device configuration and diagnostic information by starting CiscoView. CiscoView is a graphical user interface (GUI) based device management software application that provides dynamic status, statistics, and comprehensive configuration information for Cisco internetworking devices.

CiscoView allows you to configure and monitor the port level information.

To start CiscoView:

**Step 1** Start **Monitor > Monitoring Tools > Topology Services** from the menu.

**Step 2** Select the VTP domain and enter appropriate search criteria, if necessary.

**Step 3** Select the row that contains the device from the VTP Domain table. In the VTP Domain table, select the row that contains the device.

**Step 4** Right-click the selected row.

**Step 5** Select CiscoView from the popup menu.

CiscoView page launches for the selected device.
Starting Telnet

You can initiate a remote terminal connection with the Cisco Systems Console on a device that supports Telnet and that appears in the Topology map.

To do this:

Step 1
Select Monitor > Monitoring Tools > Topology Services from the menu.
The Topology Services Main Window appears.

Step 2
Select the port of the device from the Summary View.

Step 3
Right-click the row and select Telnet from the popup menu.
A Telnet session window opens.

If you are using Internet Explorer 8.0, change the following settings to use Telnet:

Step 1
Go to Start > Run.

Step 2
Enter regedit in the textbox and click OK.
The Registry Editor opens.

Step 3
Click the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl, from the list displayed.

Step 4
Go to the Edit menu and choose New > Key.

Step 5
Enter FEATURE_DISABLE_TELNET_PROTOCOL as the name of the new Key.

Step 6
Choose the above key, right click and choose REG_DWORD.

Step 7
Enter iexplore.exe as the value of the REG_DWORD property.

Step 8
Enter the Data as 0.

Step 9
Restart the browser.
Starting Device Center

Device Center provides the summary of details for a device. The application launches troubleshooting tools, management tasks, and reports for the selected device.

Since the application is based on a device-centric navigation paradigm, Device Center helps you to focus on device-centric features and information from one location.

After launching Device Center, you can change the device attributes, update inventory, and initiate telnet with a device that is selected from the Device Center Window.

To launch Device Center from Topology Services:

---

**Step 1**
Select Monitor > Monitoring Tools > Topology Services from the menu.

The Topology Services Main Window appears.

**Step 2**
Right-click a device entry from a Summary View, and select Device Center from the popup menu,

Or,

Right-click a device icon from a Network Topology View, and select Device Center from the popup menu.

Device Center launches for that device.

---

To launch Device Center from VLAN Port Assignment:

---

**Step 1**
Start Configuration > Workflows > VLAN > Configure Port Assignment from the menu.

The VLAN Port Assignment window appears.

**Step 2**
Select the VTP Domain and click Show All Ports or Get Ports.

The VTP Domain table lists the ports that are in the selected VTP domain.

**Step 3**
Right-click the device and select Device Center from the popup menu.

Device Center launches for that device.

---

Working With MLS Devices

If you are using Multilayer Switching (MLS) in your network, LMS displays MLS switches and routers in the network view.

MLS provides high-performance Layer 3 switching for Cisco routers and switches. MLS switches IP data packets between subnets while using standard routing protocols for route determination.

MLS also provides traffic statistics as part of its switching function. These statistics are used for identifying traffic characteristics for administration, planning, and troubleshooting.

This topic contains:

- Displaying MLS Reports
- Interpreting MLS Reports
Displaying MLS Reports

You can obtain information about devices in your network that are participating in multilayer switching.

**Step 1**

Go to a Network Topology View and click two or more multilayer switching (MLS) devices.

If you do not know which devices are MLS devices, select **Edit > Find**.

**Step 2**

Select **Reports > Multi-Layer Switching > Route Processors** to display the relationship between Layer 3 route processing devices in your network.

Or,

Select **Reports > Multi-Layer Switching > Switch Engines** to display the relationship between Layer 3 switching and forwarding devices in your network.

Interpreting MLS Reports

You can use MLS reports to display the relationships among multilayer switching (MLS) devices in your network.

The Route Processors Report displays information about the routers in your network that support multilayer switching, and their relationship with the MLS switches.

The Switching Engines Report displays information about the switches in your network that support Layer 3 switching (MLS), and their relationship with the MLS routers. This report also provides information about how the flow is Layer 3 switched.

This topic contains:

- Interpreting the Route Processors Report
- Interpreting Switching Engines Report

Interpreting the Route Processors Report

See Table 7-28 to interpret information shown in the Route Processors report.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLS Routers</td>
<td>Lists the Multilayer Switching Route Processors that participate in MLS. The Route Processors are listed either by IP address or device name.</td>
</tr>
<tr>
<td>MLS Switches</td>
<td>Lists the Multilayer Switching Engines that perform Layer 3 switching for the routers listed in the MLS Routers field. The Switching Engines are listed either by IP address or device name.</td>
</tr>
</tbody>
</table>
Interpreting Switching Engines Report

See Table 7-29 to interpret information displayed in the Switching Engines report.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLS Switches</td>
<td>Lists the Switching Engines that perform Layer 3 switching (MLS) for the routers listed in the MLS Routers field. The Switching Engines are listed either by IP address or device name.</td>
</tr>
<tr>
<td>MLS Routers</td>
<td>Lists Route Processors that participate in MLS. Route Processors are listed either by IP address or device name.</td>
</tr>
</tbody>
</table>
| Flow Mask      | • Destination-IP (DST)—Switching Engine maintains one MLS entry for every destination IP address. All flows to the destination IP address use this MLS entry. This mode is used if there are no access lists on any of the MLS interfaces.  
                  • Source-Destination-IP (SRC, DST)—Switching Engine maintains one MLS entry for every source and destination IP address pair. All flows between the source and destination use this MLS entry regardless of the IP protocol ports (such as FTP). This mode is used if there is a standard access list on any of the MLS interfaces.  
                  • IP-flow (SRC, DST, PORT)—Switching Engine maintains one MLS entry for every IP-flow. A separate MLS entry is created for every flow in IP-flow mode. The IP-flow includes source IP address, destination IP address, protocol, and protocol ports. This mode is used if there is an extended access list on any MLS interface. |

Note About Unified Icon

Network Topology View displays a single icon for Cisco Catalyst 6000 with MSFC and Cisco Catalyst 5000 with RSM devices. The unified icon is Layer 2 and Layer 3 Switch Router icon.

In previous versions of LMS the these devices were represented using different icons.

Working With Application Servers

Application servers are high-availability workflow systems that provide categories of service on a network, such as Cisco AVVID (Architecture for Voice, Video and Integrated Data) services.

For example, a Media Convergence Server (MCS) is an application server providing such AVVID-related applications as Cisco CallManager.

Cisco CallManager provides signaling and call control services to Cisco integrated multimedia applications as well as third-party applications. Cisco CallManager services can be distributed and clustered over an IP network, thereby allowing scale to 10,000 users and triple call processing redundancy.
The LMS Server component of Cisco Prime LMS manages application servers, and Topology Services displays them in the Layer 2 view.

You can access application servers and start Cisco CallManager from Topology Services.

Topology Services cannot distinguish a Windows server (NT and 2000) from an application server running Cisco CallManager.

Topology Services always displays a Windows server or a Media Convergence Server as an application server.

To start an application server:

**Step 1** Right-click an application server icon from a Network Topology View and select **Service Attributes** from the popup menu.

See **Displaying Service Attributes** for more details on the Service Attributes.

Or

Right-click an application server entry from a Summary View and select **Service Attributes** from the popup menu.

The Service Attributes window opens.

**Step 2** Click **Launch** in the Launch column of the Service Attributes window.

The application server starts. See the documentation included with the application server for more information.

---

### Displaying Device Service Modules

To view the details on service modules for the devices:

**Step 1** Select **Monitor > Monitoring Tools > Topology Services** from the menu.

The Topology Services Main Window appears.

**Step 2** Select a Cisco Catalyst 6000 device from the Switch Cloud in the LANEdge View.

**Step 3** Right-click the Cisco Catalyst 6000 device and select **Service Modules** from the pop up menu.

The Service Modules window appears.

**Table 7-30** describes the fields shown in the Service Modules window.
To print Service Modules information, select File > Print from the menu. To save the details to a text file, select File > Export from the menu.

### Displaying Service Attributes

Services are server processes on the application servers in your network. Examples might include Cisco CallManager, Cisco Application Engine, and Cisco Trivial File Transfer Protocol (TFTP) Server.

You can use Topology Services to display information about the available services in your network. To do this:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select a view or a domain from the Tree View in the Topology Services Main Window.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select View &gt; Display View. The Network Topology Window opens.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Double-click Services in the Topology Filters list to expand the list of available services in the specified view or domain, and select a service from the list. Device icons in the network topology map become dimmed, except for those devices configured to run the specified service. The icons that are not dimmed in the map are highlighted.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click a highlighted device, and select Service Attributes from the menu. The Software Service Attributes window appears.</td>
</tr>
</tbody>
</table>
Interpreting Service Attributes

See Table 7-31 to interpret the fields shown in the Software Service Attributes window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the device.</td>
</tr>
<tr>
<td>Application Name</td>
<td>Name of the service.</td>
</tr>
<tr>
<td>Application Version</td>
<td>Release number of the service.</td>
</tr>
<tr>
<td>Installed on</td>
<td>Installation date.</td>
</tr>
<tr>
<td>Started at</td>
<td>Time stamp.</td>
</tr>
<tr>
<td>Status</td>
<td>Current operational status.</td>
</tr>
<tr>
<td>Launch</td>
<td>Button that allows you to start the administration screen of the service.</td>
</tr>
</tbody>
</table>

Displaying Network Topology and Layer-2 Services Reports

LMS allows you to generate the following reports:

- Discrepancies.
- Best Practice Deviations.
- Port Attributes.
- Device Attributes.
- VLAN.

To see these reports:

**Step 1** Select Monitor > Monitoring Tools > Topology Services from the menu.
The Topology Services Main Window appears.

**Step 2** Select a view that contains the device, switch cloud, or the VTP Domain for which you want to view the report. This view is in the Tree View in the Topology Services Main Window.

**Step 3** Select Reports > Technology Reports and/or Reports > Fault/Event Reports from the menu.
The LMS Report Generator dialog box appears.

**Step 4** Select the following reports you want to view:

- Best Practices Deviations
- Device Attributes
- Discrepancies
- Port Attributes
- VLAN Reports

**Step 5** Select the devices or the device groups from the Device Selector area.
Step 6  Select the run type from the drop down menu, in the Scheduling area to schedule the report generator. You can schedule it for generating the report immediately, once, daily, weekly, or monthly. If you choose to generate the report immediately, go to Step 11.

Step 7  Set the date and time for generating the report, in the Scheduling area.

Step 8  Enter a description to identify this job, in the Job Description field, of the Job Info area.

Step 9  Enter a valid e-mail ID in the Email field of the Job Info area, to receive the report through mail.

Step 10  Click Submit to generate the report or click Reset to modify the values that you have entered. The report window for the report you selected, appears.

Monitoring Protocol Filter by Port

You can monitor protocol filtering by each port on devices that support this feature and have NetFlow Feature Cards installed.

This section contains:

- Understanding Protocol Filtering
- Displaying Protocol Filter Information

Understanding Protocol Filtering

On Cisco Catalyst 5000 series switches with NetFlow Feature Cards installed, you can filter broadcast traffic by protocol on a port-by-port basis.

You can display relevant ports on these switches and their protocol filtering status. This can help you troubleshoot end-user host connectivity problems based on mismatched protocols.

Displaying Protocol Filter Information

You can display protocol filter information for each port on switches with NetFlow Feature Cards. Protocol filtering is supported on Ethernet VLANs only, and the ports must be non-trunking; trunking ports are members of all protocol groups. Verify that the port for which you want to display filter information is a non-trunking port.

To display protocol filter information:

Step 1  Go to a Network Topology View and click a device with a NetFlow feature card installed.

Step 2  Select Reports > Port Attributes or right-click the device icon and select Port Attributes from the popup menu.

Step 3  Compare the information in the Protocols Enabled and Protocols Seen fields. A mismatch between these fields implies connectivity problems.
Viewing Data Collection Metrics

To view a tabular report containing statistics for the last \( n \) Data Collection cycles.

From the Topology Services main window, select **Reports > Data Collection Report**. The Data Collection Metrics window opens. See Table 7-32 for information displayed in the Data Collection Metrics window.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>StartTime</td>
<td>Time at which the most recent Data Collection cycle began.</td>
</tr>
<tr>
<td>PercentComplete</td>
<td>Percentage of Data Collection that has completed so far in the current Data Collection cycle.</td>
</tr>
<tr>
<td>EndTime</td>
<td>Time at which the most recent Data Collection cycle completed.</td>
</tr>
<tr>
<td>TotalTime</td>
<td>Total time taken for the most recent Data Collection.</td>
</tr>
<tr>
<td>Total Devices</td>
<td>Total number of managed devices.</td>
</tr>
<tr>
<td>New Devices</td>
<td>Number of newly managed devices, not seen in the previous Data Collection cycle.</td>
</tr>
<tr>
<td>Devices Deleted</td>
<td>Number of devices that were seen in the previous Data Collection cycle, but not in the most recent Data Collection.</td>
</tr>
<tr>
<td>Devices PerHour</td>
<td>Number of devices managed per hour.</td>
</tr>
<tr>
<td>Objects PerHour</td>
<td>Number of objects managed per hour.</td>
</tr>
</tbody>
</table>

Topology Groups

The Topology Groups feature in IPM allows you to create customized views of the network, in which devices are grouped according to various criteria. A view may be considered as a group of devices or device elements.

You can define the criteria (called a rule) that will determine the settings of your custom view. The rule will determine the group of devices to be displayed in the view.

These groups are subsets of Layer 2 maps, the members being defined by a set of rule expressions. In a network with a large number of devices, a Topology Group helps you to perform operations in a subset of the large network.

You can use Topology Groups Administration to manage the Topology Groups in your system.

The following topics provide information about:

- Understanding Topology Groups
- Interpreting Topology Groups Summary Information
- Hierarchical Maps
Understanding Topology Groups

A Topology Group can be thought of as a convenience view that allows you to view a subset of the entire network based on the group rule defined while creating the view.

These views, which are subsets of the Layer 2 views, can be accessed by a user or a set of users. These custom views are generated using a LMS feature called Grouping Services, which helps manage groups of devices.

Grouping Services determines the membership of a group by interpreting and applying the rule associated with the group.

Hence, Topology Groups provides multiple benefits:

- Provides a channel to identify, and view a set of objects corresponding to a view.
- Facilitates the creation and management of views.
- Provides you with a way to define convenience views which are a subset of the Layer 2 map.

Interpreting Topology Groups Summary Information

You can display summary information about devices in Topology Groups. To do this:

Step 1: Go to the Tree view in Topology Services, click a Topology Groups view.

See Table 7-33 to interpret Topology Groups summary information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>Number of devices displayed in the particular view.</td>
</tr>
<tr>
<td>Routers</td>
<td>Number of routers.</td>
</tr>
<tr>
<td>Device List</td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the Device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the device.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Product Type.</td>
</tr>
<tr>
<td>State</td>
<td>Current status of the device, whether it is reachable or not.</td>
</tr>
</tbody>
</table>

Hierarchical Maps

Hierarchical maps are the Network Topology Views that display the devices listed under Topology Groups in a hierarchical organization. Each map displays the selected group as a cloud of devices.

This section contains:

- Understanding Hierarchical Maps
- Viewing Hierarchical Maps
Understanding Hierarchical Maps

Hierarchical Maps provide a hierarchical view for the devices under the Topology Groups.

These Maps display each Topology Group as a cloud. If a Topology Group contains a sub-group, the Network Topology View of the parent group displays a cloud icon to represent the sub-group.

Similarly, each sub-group is displayed inside the corresponding parent group as a cloud icon.

The Network Topology View for the parent topology Group displays an aggregate link for all the links from the sub-group to the devices in the parent group.

- If one or more devices in the sub-group of the Topology Group, are connected to the devices in the parent Topology Group, the hierarchical map of the parent group displays an aggregate link for all the links from the sub-group to the devices.
- If you double-click the sub-group cloud, you can view the Hierarchical map for the child group inside the parent group. Thus, hierarchical maps display the devices hierarchically till the last child group.

Viewing Hierarchical Maps

To view Hierarchical maps from the Topology Services window:

**Step 1** Select **Topology Services > Topology Groups** from the LMS Main Window.

**Step 2** Select the Group that you want to view.

**Step 3** Select **View > Display View** from the menu.

The Network Topology View window displays the hierarchical map for the selected group. If there are sub-groups, the Network Topology View displays each sub-group as a Cloud icon in the map represents the sub-group.

**Step 4** Right-click the Cloud icon in the Network Topology View and select **Open**.

Or

Double-click the cloud to view the sub-group.

The Network Topology View window for the sub-group appears.

Displaying the Device Label

To display the name of the Cloud icon or the sub-group in the Network Topology View:

Select the Cloud icon, select **View > Display Labels**, and select either **IP address**, **Device name**, or **SysName**.

The Network Topology View displays the sub-group device category names.

Filters for Topology Groups

Filters are provided for the Topology Groups, in Network Topology Views. You can use these filters to filter the clouds, that are the sub-groups. For more details, see **Using Topology Filters**.
Displaying Aggregate Links in Hierarchical Maps

You can view the aggregate links between the clouds. The network view displays the aggregate links if a device in a cloud is linked to another cloud or the sub-group. Aggregate links may contain one or more links.

For more details, see Displaying Aggregate Link Attributes.

To view the aggregate links between the clouds, right-click the Cloud icon and select Show Aggregate Links.

To clear the display of aggregate links, right click the Cloud icon and select Clear Aggregate Links.

Notes:

- The Groups under Admin > System > Groups Management > Devices and under Topology Services > Topology Groups follow the same hierarchy.
- In Topology Groups, when you use the Find option using the device name or device IP address, the Find on Map window displays only the devices in the respective selected group, and does not display the devices in other sub-groups.
  For more details, see Using Find in Network Topology Views.
- After you create a Group through Admin > System > Groups Management > Devices, you must reopen the Topology Services to view the changes. For more details, see the Admin Online help.

Topology Services Menu Reference

See the command references for understanding the Topology Services windows.

This section contains:

- Topology Services Main Window Menu Reference
- Network Topology View Menu Reference

Topology Services Main Window Menu Reference

<table>
<thead>
<tr>
<th>Table 7-34</th>
<th>Topology Services Main Window Menu Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu</td>
<td>Command</td>
</tr>
<tr>
<td>File</td>
<td>Print</td>
</tr>
<tr>
<td>Export</td>
<td>None</td>
</tr>
<tr>
<td>Upgrade View Layouts</td>
<td>None</td>
</tr>
<tr>
<td>Exit</td>
<td>None</td>
</tr>
</tbody>
</table>
### Table 7-34  Topology Services Main Window Menu Descriptions (continued)

<table>
<thead>
<tr>
<th>Menu</th>
<th>Command</th>
<th>Toolbar Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Rename</td>
<td>None</td>
<td>Renames a switch cloud.</td>
</tr>
<tr>
<td>Copy</td>
<td>None</td>
<td></td>
<td>Copies selected text to the clipboard.</td>
</tr>
<tr>
<td>Find</td>
<td></td>
<td></td>
<td>Opens Find window to enable searching for items in the Tree View and Summary View.</td>
</tr>
<tr>
<td>Find Next</td>
<td>None</td>
<td></td>
<td>Uses Find to search for next item that matches previously entered search criteria.</td>
</tr>
<tr>
<td>Bandwidth Filter Settings</td>
<td>None</td>
<td></td>
<td>You can set the ranges of bandwidth utilization and color for the links to be highlighted in the Map. For more details, see <a href="#">Customizing Bandwidth Utilization Filters</a>.</td>
</tr>
<tr>
<td>View</td>
<td>Show Toolbar</td>
<td>None</td>
<td>Shows or hides the toolbar.</td>
</tr>
<tr>
<td></td>
<td>Reload</td>
<td>None</td>
<td>Refreshes Tree View contents.</td>
</tr>
<tr>
<td></td>
<td>Refresh Summary</td>
<td></td>
<td>Updates information in Summary View.</td>
</tr>
<tr>
<td></td>
<td>Expand All</td>
<td>None</td>
<td>Expands selected folder in Tree View.</td>
</tr>
<tr>
<td></td>
<td>Collapse All</td>
<td>None</td>
<td>Closes selected folder in Tree View.</td>
</tr>
<tr>
<td></td>
<td>Display View</td>
<td>None</td>
<td>Opens Network Topology View for selected item in Tree View.</td>
</tr>
</tbody>
</table>
### Table 7-34  Topology Services Main Window Menu Descriptions (continued)

<table>
<thead>
<tr>
<th>Menu</th>
<th>Command</th>
<th>Toolbar Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports</td>
<td>Discrepancies</td>
<td>None</td>
<td>Displays discrepancies or anomalies in the discovered network. You can generate a report on the discrepancies. For more details, see the Reports Online help.</td>
</tr>
<tr>
<td></td>
<td>Best Practices Deviations</td>
<td>None</td>
<td>Displays Best Practices Deviations page in Report Generator, where you can generate a report of Best Practices Deviations. For more details, see the Reports Online help.</td>
</tr>
<tr>
<td></td>
<td>Data Collection Report</td>
<td>None</td>
<td>Opens the Data Collection Metrics window. For more details, see the Reports Online help.</td>
</tr>
<tr>
<td></td>
<td>Campus Reports</td>
<td>None</td>
<td>Displays the Report Generator page from where you can generate any of the five reports on: best practices deviations, device attributes, discrepancies, port attributes, or VLANs for VTP domain or the switch cloud. For more details, see the Reports Online help.</td>
</tr>
<tr>
<td></td>
<td>VLAN Report</td>
<td>None</td>
<td>Displays VLAN reports for devices, switch clouds, or VTP domains. You must select a VTP domain or a switch cloud for generating the report.</td>
</tr>
<tr>
<td></td>
<td>Spanning Tree Configuration</td>
<td>None</td>
<td>Allows to generate reports and configure Spanning Trees on the network.</td>
</tr>
<tr>
<td>Tools</td>
<td>VLAN Management &gt; Create</td>
<td><img src="image" alt="Create VLAN" /></td>
<td>Creates an Ethernet VLAN. This function can be performed only by users logged in as Network Administrators or System Administrators.</td>
</tr>
<tr>
<td></td>
<td>VLAN Management &gt; Delete</td>
<td><img src="image" alt="Delete VLAN" /></td>
<td>Deletes the selected VLAN. This function can be performed only by users logged in as Network Administrators or System Administrators.</td>
</tr>
<tr>
<td></td>
<td>PVLAN Management &gt; Create</td>
<td>None</td>
<td>Creates Private VLAN.</td>
</tr>
<tr>
<td></td>
<td>PVLAN Management &gt; Delete</td>
<td>None</td>
<td>Deletes Private VLANs.</td>
</tr>
<tr>
<td></td>
<td>VLAN Port Assignment</td>
<td><img src="image" alt="VLAN Port Assignment" /></td>
<td>Moves ports between VLANs in the same VTP domain.</td>
</tr>
<tr>
<td>Window</td>
<td>None</td>
<td>None</td>
<td>Switches between all open Topology Services windows.</td>
</tr>
</tbody>
</table>
Table 7-35  Network Topology View Menu Descriptions

<table>
<thead>
<tr>
<th>Menu</th>
<th>Command</th>
<th>Toolbar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>Save Layout</td>
<td>![Icon]</td>
<td>Saves any changes you make to the Network Topology View (applies only to your user ID).</td>
</tr>
<tr>
<td>Print &gt; Print All</td>
<td></td>
<td>![Icon]</td>
<td>Prints the entire Network Topology View, at the normal viewing level. Each page will have a corresponding column and row number with grid marks to align the pages.</td>
</tr>
<tr>
<td>Print &gt; Print Visible</td>
<td></td>
<td>![Icon]</td>
<td>Prints what is visible the current screen, shrinking it to fit on one page.</td>
</tr>
<tr>
<td>Export To Visio &gt; Export To csv</td>
<td>None</td>
<td>![Icon]</td>
<td>Allows you to export the network map as a Visio drawing and save it in .csv format.</td>
</tr>
<tr>
<td>Export To Visio &gt; Export To xml</td>
<td>None</td>
<td>![Icon]</td>
<td>Allows you to export the network map as a Visio drawing and save it in XML format.</td>
</tr>
<tr>
<td>Download Visio Stencil</td>
<td>None</td>
<td>![Icon]</td>
<td>Opens new browser window with a link for downloading the cm_cisco.vss stencil file.</td>
</tr>
<tr>
<td>Close</td>
<td>None</td>
<td>![Icon]</td>
<td>Exits Network Topology View.</td>
</tr>
<tr>
<td>Edit</td>
<td>Undo</td>
<td>None</td>
<td>Reverses the last operation.</td>
</tr>
<tr>
<td></td>
<td>Redo</td>
<td>None</td>
<td>Repeats the last operation.</td>
</tr>
<tr>
<td>Find</td>
<td></td>
<td>![Icon]</td>
<td>Finds devices by name or IP address.</td>
</tr>
<tr>
<td>Select &gt; All Devices</td>
<td>None</td>
<td>![Icon]</td>
<td>Selects all devices on the current Network Topology View.</td>
</tr>
<tr>
<td></td>
<td>Select &gt; All Links</td>
<td>None</td>
<td>Selects all links on the current Network Topology View.</td>
</tr>
<tr>
<td>Menu</td>
<td>Command</td>
<td>Toolbar Button</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Edit (Contd.)</td>
<td>Select &gt; All Highlighted Objects</td>
<td>None</td>
<td>Selects all highlighted devices on the current Network Topology View.</td>
</tr>
<tr>
<td></td>
<td>Select &gt; All Filtered Objects</td>
<td>None</td>
<td>Selects all filtered objects on the current Network Topology View.</td>
</tr>
<tr>
<td></td>
<td>Highlight Filtered</td>
<td>None</td>
<td>Highlights devices that conform to selected filters.</td>
</tr>
<tr>
<td></td>
<td>Clear Highlighted</td>
<td>None</td>
<td>Clears highlighting from Network Topology View.</td>
</tr>
<tr>
<td></td>
<td>Perform Data Collection</td>
<td>![Image]</td>
<td>RedisCOVERS a selected device or a group of devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This function can be performed only by users logged in as System Administrators.</td>
</tr>
<tr>
<td></td>
<td>Delete Device(s)</td>
<td>None</td>
<td>Removes devices from the Network Topology View.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Devices still in your network and manageable by LMS will reappear on the Network Topology View after the next Campus Data Collection cycle.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This function can be performed only by users logged in as Network Administrators or System Administrators.</td>
</tr>
<tr>
<td></td>
<td>Delete Link(s)</td>
<td>None</td>
<td>Removes a link from the Network Topology View.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This function can be performed only by users logged in as Network Administrators or System Administrators.</td>
</tr>
<tr>
<td></td>
<td>Map Preferences</td>
<td>None</td>
<td>Edit Network Topology View settings such as color and layout style.</td>
</tr>
<tr>
<td>View</td>
<td>Show Toolbar</td>
<td>None</td>
<td>Shows or hides the toolbar.</td>
</tr>
<tr>
<td></td>
<td>Show Grid</td>
<td>None</td>
<td>Shows or hides the grid. When moving devices with the grid on, the devices snap to the grid.</td>
</tr>
<tr>
<td></td>
<td>Panner</td>
<td>None</td>
<td>Displays compact view of entire Network Topology View.</td>
</tr>
<tr>
<td></td>
<td>Zoom In</td>
<td>![Image]</td>
<td>Focuses on a specific Network Topology View area.</td>
</tr>
</tbody>
</table>
### Table 7-35  Network Topology View Menu Descriptions (continued)

<table>
<thead>
<tr>
<th>Menu</th>
<th>Command</th>
<th>Toolbar Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View (Contd.)</td>
<td>Zoom Out</td>
<td></td>
<td>Expands the focus to a larger area.</td>
</tr>
<tr>
<td></td>
<td>Zoom to Selected Devices</td>
<td></td>
<td>Focuses on selected devices. Fits selected devices in a Network Topology View window at the maximum size possible.</td>
</tr>
<tr>
<td></td>
<td>Normal</td>
<td></td>
<td>Returns to the default view.</td>
</tr>
<tr>
<td></td>
<td>Fit in Window</td>
<td></td>
<td>View all discovered devices.</td>
</tr>
<tr>
<td></td>
<td>Display Labels &gt; Show IP</td>
<td>None</td>
<td>Displays device IP addresses.</td>
</tr>
<tr>
<td></td>
<td>Display Labels &gt; Show Device Name</td>
<td>None</td>
<td>Displays device names.</td>
</tr>
<tr>
<td></td>
<td>Display Labels &gt; Show Sysname</td>
<td>None</td>
<td>Displays device sysNames.</td>
</tr>
<tr>
<td></td>
<td>Display Labels &gt; Clear Labels</td>
<td>None</td>
<td>Clears labels from Network Topology View.</td>
</tr>
<tr>
<td></td>
<td>Relayout &gt; Circular</td>
<td>None</td>
<td>Portrays interconnected ring and star topologies.</td>
</tr>
<tr>
<td></td>
<td>Relayout &gt; Hierarchical</td>
<td>None</td>
<td>Reveals precedence relations.</td>
</tr>
<tr>
<td></td>
<td>Relayout &gt; Symmetric</td>
<td>None</td>
<td>Provides representations of complex networks.</td>
</tr>
<tr>
<td></td>
<td>Relayout &gt; Orthogonal</td>
<td>None</td>
<td>Provides graph layouts with edges running parallel to x and y axes.</td>
</tr>
<tr>
<td>View (Contd.)</td>
<td>Refresh Map</td>
<td>None</td>
<td>Refreshes the display.</td>
</tr>
<tr>
<td></td>
<td>Fault Monitor Alert Settings</td>
<td>None</td>
<td>Launches Fault Monitor Alert Settings Page.</td>
</tr>
</tbody>
</table>
### Table 7-35  Network Topology View Menu Descriptions (continued)

<table>
<thead>
<tr>
<th>Menu</th>
<th>Command</th>
<th>Toolbar Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports</td>
<td>Discrepancies</td>
<td>None</td>
<td>Displays discrepancies or anomalies in the discovered network. You can generate a report on the discrepancies. For more details, see the Reports Online help.</td>
</tr>
<tr>
<td>Best Practices</td>
<td>Deviations</td>
<td>None</td>
<td>Displays Best Practices Deviations page in Report Generator, where you can generate a report of Best Practices Deviations. For more details, see the Reports Online help.</td>
</tr>
<tr>
<td>Data Collection</td>
<td>Report</td>
<td>None</td>
<td>Displays Data Collection Metrics report. For more details, see the Reports Online help.</td>
</tr>
<tr>
<td>Device Attributes</td>
<td></td>
<td>None</td>
<td>Displays descriptive information about the selected device or devices.</td>
</tr>
<tr>
<td>IPv6 Addresses</td>
<td></td>
<td>None</td>
<td>Displays the IPv6 Addresses report.</td>
</tr>
<tr>
<td>Service Attributes</td>
<td></td>
<td>None</td>
<td>Displays descriptive information about any application servers that are running on the selected device or devices.</td>
</tr>
<tr>
<td>Port Attributes</td>
<td></td>
<td>None</td>
<td>Displays descriptive information about ports belonging to the selected device.</td>
</tr>
<tr>
<td>Link Attributes</td>
<td></td>
<td>None</td>
<td>Displays descriptive information about the selected link or links.</td>
</tr>
<tr>
<td>VLAN Report</td>
<td></td>
<td>None</td>
<td>Displays the VLAN Report for the selected devices in the Topology Map or for all devices in the Map. For more details, see the Reports Online help.</td>
</tr>
<tr>
<td>Multi-Layer Switching</td>
<td>&gt; Switching Engines</td>
<td>None</td>
<td>Displays relationship between Layer 3 route processing devices in network.</td>
</tr>
<tr>
<td>Multi-Layer Switching</td>
<td>&gt; Route Processors</td>
<td>None</td>
<td>Displays relationship between Layer 3 switching and forwarding devices in your network.</td>
</tr>
</tbody>
</table>
Supported Protocols

The following concepts are important for understanding how to use Topology Services:

- Inter-Switch Link (ISL) Protocol
- IEEE 802.1Q

You must make sure that the applicable protocols are implemented correctly in your network; otherwise, the information gathered might be incomplete.

Inter-Switch Link (ISL) Protocol

Inter-Switch Link (ISL) is a Cisco-proprietary protocol that allows VLAN trunking by maintaining VLAN information as traffic flows between switches and routers.

You can pass VLAN information between devices by configuring links between the switches. If you want a link to carry more than one VLAN, you must use ISL. To use ISL, you must configure the ports on both sides of the link as trunk ports.

When two VTP domains are interconnected using an ISL trunk between two LAN switches, by default, no VLAN traffic is forwarded. However, you can configure the ports on each switch to receive and forward specific VLANs.
To configure the ports, the VLANs on either side of the ISL trunk must be identical and share the same VLAN characteristics such as VLAN names, VLAN indexes, and so on.

### IEEE 802.1Q

IEEE 802.1Q is the industry-standard for trunking. A standard for encapsulation protocol to carry traffic for multiple VLANs over a single link. You can use this standard when you want to interconnect a Cisco device with a trunk link to a non-Cisco device.

You can use the encapsulation dot1q command on Cisco IOS version 12.0.1(t) or higher for the Cisco routers.

### Support for IPv6 in Topology Services

This section contains the Internet Protocol version 6 (IPv6) support provided in Topology Services. It contains the following:

- **Topology Changes**
- **Viewing IPv6 Addresses Report**
- **Intrepreting IPv6 Addresses Report**

#### Topology Changes

Topology Services provides the following for IPv6 support:

- IPv6 filter that lets you highlight the IPv6 devices
- Find option for IPv6 devices
- Table for devices running IPv6
- Change Management IP Address displays IPv6 address, if the device is enabled with IPv6 option.

**Note**

IPv6 support for the following STP options has not been tested: Per VLAN STP Recommendations, Cisco MISTP Recommendations, and IEEE 802.1s Recommendations.

#### Viewing IPv6 Addresses Report

You can view IPv6 addresses report for IPv6 enabled devices.

To view this report:

**Step 1**
Right-click the LAN Edge View or Layer 2 View from Network Views in the Topology Services window.

**Step 2**
Click Display View.

The Network Topology window appears.
Step 3    Select an IPv6 enabled device.
Step 4    Right-click the device then select IPv6 Addresses, or choose Reports > IPv6 Addresses.
          The IPv6 Addresses report appears.

## Interpreting IPv6 Addresses Report

See the table below for interpreting the fields in the IPv6 Addresses Report.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Name of the IPv6 address interface.</td>
</tr>
</tbody>
</table>
| IPv6 Address  | IPv6 address of the device. An IPv6 address typically has four groups of 8 bits each.  
|               | Example: 2001:5:A:3:0:0:0:2                                                 |
|               | You can sort the records in the report based on IPv6 Addresses.              |
| Prefix Length | Length of the prefix. This is a decimal value representing how many of the left-most contiguous bits of the address comprise the prefix. |
| Prefix Address| Prefix portion of the IPv6 address. This is similar to CIDR in IPv4 and is written in CIDR notation. An IPv6 address prefix is represented by the notation: IPv6-address/prefix-length.  
|               | You can sort the records in the report based on Prefix Address.             |
| Address Type  | Type of IPv6 address. Network Topology, User Tracking and Layer 2 Services supports unicast addresses. The Address Type can be global, link-local, or site-local.  
|               | Global addresses are identified by the Format Prefix of 001. Addresses of this type are designed to be aggregated or summarized to produce an efficient routing infrastructure.  
|               | Link-local addresses are used to communicate between hosts on the link with no router.  
|               | Site-local addresses are used between nodes that communicate with other nodes in the same site. Site-local addresses are identified by the Format Prefix of 1111 1110 11. |
Managing Network Spanning Trees

This chapter describes the IEEE 802.1d Spanning Tree Protocol (STP), and how to use and configure Cisco’s proprietary spanning-tree protocols, Per VLAN Spanning Tree (PVST), Multiple Spanning Tree (MSTP), and Multi-Instance Spanning Tree Protocol (MISTP) in a LMS network. It contains the following sections:

- Understanding Spanning Tree Protocol
- Spanning Tree Recommendation Reports
- Spanning Tree Reports: STP Visualizer
- Generating Reports and Configuring STP on the Network
- Spanning Tree Filters

Understanding Spanning Tree Protocol

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network. Hence, STP is a loop-prevention protocol.

It is a technology that allows Bridges to communicate with each other to discover physical loops in the network. The protocol then specifies an algorithm that Bridges can use to create a loop-free logical topology.

In other words, STP creates a tree structure of loop-free leaves and branches that spans the entire Layer 2 network.

To provide path redundancy STP spans all switches in an extended network. STP forces certain redundant data paths into a standby (blocked) state.

This section describes the specific functions available to you when you use spanning-tree protocols. STP uses a distributed algorithm that selects one Bridge of a redundantly connected network as the root of a Spanning Tree-connected active topology.

STP assigns roles to each port depending on what the port’s function is in the active topology. Port roles are:

- Root—Forwarding port that is elected for the spanning-tree topology
- Designated—Forwarding port that is elected for every switched LAN segment
- Alternate—Blocked port providing an alternate path to the root port in the Spanning Tree
- Backup—Blocked port in a loopback configuration

Designated, Alternate, and Backup states are specific to MST.
Understanding Spanning Tree Protocol

The switches that have ports with these assigned roles are called the root or designated switches. In Ethernet networks, only one active path may exist between any two stations. Multiple active paths between stations can cause loops in the network.

When loops occur, some switches recognize the same stations on more than one side of the switch. This situation causes the forwarding algorithm to malfunction allowing the duplicate frames to be forwarded.

The Spanning Tree algorithms provide path redundancy by defining a tree that spans all of the switches in an extended network and then forces certain redundant data paths into a standby (blocked) state.

At regular intervals, the switches in the network send and receive Spanning Tree BPDUs that they use to identify the path.

If one network segment becomes unreachable, or if the Spanning Tree costs change, the Spanning Tree algorithm reconfigures the Spanning Tree topology and reestablishes the link by activating the standby path.

The Spanning Tree operation is transparent to end stations, which do not detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

STP provides these advantages:

- Detection and elimination of loops
- Capability to automatically detect failed active paths and to utilize alternate paths
- User-configurable parameters that enable a network administrator to fine-tune the algorithm’s performance

These sections describe the following Spanning Tree Protocols in brief:

- Per VLAN Spanning Tree Protocol
- Multiple Spanning Tree Protocol
- Multiple Instance Spanning Tree Protocol

**Per VLAN Spanning Tree Protocol**

Per VLAN Spanning Tree Protocol maintains a separate instance of STP for each individual VLAN configured in the network.

It 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). It does this by forwarding some VLANs on one trunk and other VLANs on another trunk without causing a Spanning Tree loop.

**Multiple Spanning Tree Protocol**

Multiple Spanning Tree uses IEEE’s RSTP as base Spanning Tree Protocol. MST uses only one BPU for all instances.

A disadvantage of PVST is that it adds a lot of overhead to your switching equipment. If a switch is configured to use MST, it must ascertain which of its neighbors are using which type of STP.

It does this by configuring switches into common MST regions, where every switch in a region runs MST with compatible parameters. You can map a group of VLANs to instance.
In most networks, a single MST region is sufficient, although you can configure more than one region. Within the region, all switches must run the instance of MST that is defined by the following attributes:
- MST configuration name (32 characters)
- MST configuration revision number (0 to 65535)
- MST instance-to-VLAN mapping table (4096 entries)

**Multiple Instance Spanning Tree Protocol**

Multiple Instance Spanning Tree Protocol (MISTP) allows you to group multiple VLANs under a single instance of Spanning Tree (an MISTP instance).

An MISTP instance is a virtual logical topology that is defined by a set of bridge and port parameters. When you map VLANs to an MISTP instance, this virtual logical topology becomes a physical topology.

Each MISTP instance has its own root switch and a different set of forwarding links, that is, different bridge and port parameters.

Each MISTP instance root switch propagates the information that is associated with it to all other switches in the network. This process maintains the network topology. This is because it ensures that each switch has the same information about the network.

MISTP builds MISTP instances by exchanging MISTP BPDU s with peer entities in the network. MISTP uses one BPDU for each MISTP instance.

An MISTP instance can have any number of VLANs that are mapped to it, but a VLAN can be mapped only to a single MISTP instance.

You can move a VLAN (or VLANs) in an MISTP instance to another MISTP instance if it has converged.

**Spanning Tree Recommendation Reports**

LMS Recommendation Reports aid deployment of Spanning Trees in the network. The following reports are available:
- **Spanning Tree Reports: Optimal Root Recommendation Report**
- **Spanning Tree Reports: Number of Instances Recommendation Report**
- **Spanning Tree Reports: Instance Reduction Recommendation Report**
- **Spanning Tree Reports: VLAN to Instance Mapping Recommendation Report**
Spanning Tree Reports: Optimal Root Recommendation Report

The Optimal Root Recommendation Report allows you to compute the optimal root in a switch cloud running Per VLAN STP, Cisco MISTP, or IEEE 802.1s.

**Step 1**
Invoke Switch Cloud Map View from Topology Services.

**Step 2**
Select any of the following:
- Reports > Per VLAN STP Recommendations > Optimal Root Recommendation
- Reports > Cisco MISTP Recommendations > Optimal Root Recommendation
- Reports > IEEE 802.1s Recommendations > Optimal Root Recommendation

The Optimal Root Recommendation window appears.

**Step 3**
In the Computation Criteria, select a computation type.

*Table 8-1* lists three computation types and their description.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Least Depth</td>
<td>Computes depth from each node in the switch cloud. Chooses the root in such a manner that the resulting Spanning Tree has minimum depth.</td>
</tr>
<tr>
<td>Least Cost</td>
<td>Computes cost for each node in the switch cloud. Computes maximum edge node cost for all the nodes by assuming current node as the root node. The node with minimum value for maximum edge node cost is considered as the optimal root.</td>
</tr>
<tr>
<td>Traffic Data</td>
<td>Computes a Spanning Tree, which provides optimal path for given percentage of traffic or selected nodes.</td>
</tr>
</tbody>
</table>

If you select Traffic Data, go to **Step 4**, else go to **Step 5**.

**Step 4**
Select a traffic data source from the Traffic Details (*Table 8-2*).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Source</td>
<td>Select either of the following network traffic data sources:</td>
</tr>
<tr>
<td></td>
<td>• NAM—Select this option if you use Cisco Network Analysis Modules to collect data.</td>
</tr>
<tr>
<td></td>
<td>• Netflow Collector 3.6—Select this option if you use NetFlow FlowCollector to collect data.</td>
</tr>
<tr>
<td>Traffic File Name</td>
<td>Enter the NAM or NetFlow traffic data filename.</td>
</tr>
</tbody>
</table>

**Step 5**
Click *Compute*.

The Recommended Roots table lists the optimal root devices.
Interpreting Optimal Root Recommendation

The optimal root recommendation report helps you to select the best root for your network using any of the three methods:

- **Least Depth**
  
  Use this method to compute better overall convergence. Convergence time is based on the distance to the boundary nodes. The node with the least path cost to boundary nodes is recommended as optimal root.

  A device farther from the boundary nodes takes longer to propagate the topology change that has occurred than another node that is near the boundary nodes in the same switched environment.

  This directly affects the convergence time of the switched or bridged network. After this root is selected, you can make suitable adjustments to forward the delay timer of Spanning Tree protocol to take advantage of faster convergence.

- **Least Cost**
  
  The node with the least cumulative cost to all other nodes is recommended as root according to this method. When Spanning Tree root is computed based on this method it provides a better path between nodes in the switched environment assuming equal traffic distributions.

  In case of unbalanced switched environment where core switch A is connected to 10 other distribution switches and another core switch B is connected to only 5 of the distribution switches, this algorithm will suggest A as root as compared to B.

  Five switches that are not directly connected to B should take a longer path to other nodes if B is selected as root. If A is selected as root this problem could be avoided.

- **Traffic Data**
  
  In a switched or bridged network environment, when Spanning Tree is computed the primary aim is to eliminate loops and it may not provide shortest possible path between every node to every other node.

  Based on the traffic pattern a particular device may provide optimal path for a greater percentage of traffic than another.

  For example, a switched network containing nodes—A, B, C, D, and E. Overall traffic is 95% localized between a set of nodes {A, B, and C}. A node which when selected as root, provides the shortest path between A, B, and C would be the ideal choice. This is regardless of whether it provides shortest path from D or E to any other nodes.

  In some cases you may not be able to get the shortest path between A, B, and C when trying to find the optimal root. In such cases, a root that provides most optimal path between A, B, and C is chosen.
Spanning Tree Reports: Number of Instances Recommendation Report

The Number of Instances Recommendation Report allows you to compute the number of instances in a switch cloud running Cisco MISTP or IEEE 802.1s.

**Step 1** Invoke Switch Cloud Map View from Topology Services.

**Step 2** Select either of the following:
- Reports > Cisco MISTP Recommendations > Instance Recommendation
- Reports > IEEE 802.1s Recommendations > Instance Recommendation

The Number of Instance Recommendation window appears.

**Step 3** In the Computation Techniques area, select a computation type.

**Table 8-3** lists two computation techniques and their description.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max instances for better link utilization</td>
<td>Computes the optimal number of Spanning Tree instances that can be run on the given switched network for optimizing network link resources</td>
</tr>
<tr>
<td>Min instances for better CPU utilization</td>
<td>Computes the optimal number of Spanning Tree instances that can be run on the given switched network for optimizing device CPU resources.</td>
</tr>
</tbody>
</table>

**Step 4** Click **Compute**.

The Recommended Number of Instances appears in the Results area.

**Step 5** Select a value from the Select Instance drop-down list.

**Step 6** Click **Highlight in Map** to highlight the device icon in Switch Cloud Map.

**Step 7** Click **Close** to close the Number of Instances Recommendation window.

**Interpreting Number of Instances Recommendation**

The number of instance recommendation is made based on two methods:

- Max instances for better link utilization method
  - Use this method to compute better balanced link utilization.
  - We recommend that you use the number of instances that is the least common multiplier of all the independent redundant paths, as the maximum number of instances.

- Min instances for better CPU utilization
  - Use this method to compute a minimum number of instances so that CPU utilization is minimum.
  - We recommend that the number of instances, which results in the maximum number of independent redundant paths is recommended.
Spanning Tree Reports: Instance Reduction Recommendation Report

The Instances Reduction Recommendation Report allows you to compute the number of instances in a switch cloud running Cisco MISTP or IEEE 802.1s.

**Step 1** Invoke Switch Cloud Map View from Topology Services.

**Step 2** Select either of the following:
- Reports > Cisco MISTP Recommendations > Instance Reduction Recommendation
- Reports > IEEE 802.1s Recommendations > Instance Reduction Recommendation

The Instance Reduction Recommendation window appears.

**Step 3** In the Computation Techniques area, select a computation type.
Table 8-4 lists two computation techniques and their description.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub-tree Reduction</td>
<td>Determine if one or more Spanning Tree instances are mergeable if the instances have a supertree–subtree relationship.</td>
</tr>
<tr>
<td>Conditional Reduction</td>
<td>Determines the Spanning Tree instances that can be merged based on the forwarding topology of the network.</td>
</tr>
</tbody>
</table>

**Step 4** Click Compute.

The Recommended Number of Instances in displayed in the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Instance ID.</td>
</tr>
<tr>
<td>Mergeable Instances</td>
<td>Comma separated list of instance IDs which can be merged.</td>
</tr>
</tbody>
</table>

**Step 5** Select a row, and click **Highlight in Map** to highlight the instances in Switch Cloud Map.

**Step 6** Click **Close** to close the Instance Reduction Recommendation window.
Interpreting Instance Reduction Recommendation

You can use the Instance Reduction Recommendations if your network contains multiple Spanning Tree instances that share the same forwarding topology.

The Recommendation report allows you to determine Spanning Tree instances. These instances can be merged into a shared instance without any impact on convergence or operation.

Fewer instances help you to optimize the utilization of memory and CPU resources of the switches. Instance reduction recommendation is made based on two methods:

- **Sub tree reduction method**
  
  Use this method to determine Spanning Tree instances, which can be merged when the switched network has an instance that spans across different sets of switches as compared to another instance.
  
  For example, instance A is considered a sub-tree of instance B if all the forwarding and blocking paths of instance A are in the same state in instance B. Instance A is a sub-tree of instance B if the forwarding and blocking paths of instance A exactly matches that of instance B.
  
  If the above case is satisfied, the report recommends merging of the two STP instances.

- **Conditional reduction method**
  
  Use this method to determine the Spanning Tree instances, which can be merged when the switched network has instances that share forwarding paths and root.

Spanning Tree Reports: VLAN to Instance Mapping Recommendation Report

The Number of Instances Recommendation Report allows you to compute the optimum number of VLANs to instances in a switch cloud running Cisco MISTP or IEEE 802.1s.

**Step 1**
Invoke Switch Cloud Map View from Topology Services.

**Step 2**
Select either of the following:

- Reports > Cisco MISTP Recommendations > VLAN to Instance Mapping Recommendation.
- Reports > IEEE 802.1s Recommendations > VLAN to Instance Mapping Recommendation.

The VLAN to Instance Mapping Recommendation window appears.

**Step 3**
In the Computation Metrics area, select a metric type. Table 8-6 lists the four computation techniques and their description.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of VLANs</td>
<td>Select a device (reference device), Spanning Tree instance that has least number of VLANs mapped to it.</td>
</tr>
<tr>
<td>Optimal path for select devices</td>
<td>Select multiple devices to find the Spanning Tree instance with least sub-optimality.</td>
</tr>
<tr>
<td>Least instance load</td>
<td>Select only one device (reference device). It recommends the Spanning Tree with the least load.</td>
</tr>
<tr>
<td>Least instance load for selected devices</td>
<td>Select multiple devices. It will recommend the Spanning Tree instance with the least traffic.</td>
</tr>
</tbody>
</table>
If you select Least instance load or Least instance load for selected devices, go to Step 4, else go to Step 5.

**Step 4**  
Select a traffic data source from the Traffic Type drop-down list in the Traffic Details area. Table 8-7 lists the two types of data sources supported.

**Table 8-7  Traffic Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Type</td>
<td>Select either of the following network traffic data sources:</td>
</tr>
<tr>
<td></td>
<td>• NAM—Select this option if you use Cisco Network Analysis Modules</td>
</tr>
<tr>
<td></td>
<td>to collect data.</td>
</tr>
<tr>
<td></td>
<td>• Netflow Collector 3.6—Select this option if you use NetFlow Collector</td>
</tr>
<tr>
<td></td>
<td>to collect data.</td>
</tr>
<tr>
<td>File</td>
<td>Enter the NAM or NetFlow traffic data filename.</td>
</tr>
</tbody>
</table>

**Step 5**  
Click **Compute**.

The Recommended Instance ID is displayed in the VLAN Instance Recommendation area.

**Step 6**  
Select a device, and click **Highlight in Map** to highlight the device icon in Switch Cloud Map.

**Step 7**  
Click **Close** to close the VLAN Instance Mapping Recommendation window.

**Interpreting VLAN to Instance Mapping Recommendation**

The number of instance recommendation is made based on four methods:

- **Number of VLANs**
  
  Use this method when the traffic or load on each of the VLANs is almost the same. This method assumes that an instance with least number of VLANs is optimal for mapping to a new VLAN. Hence, the Spanning Tree instances with the least number of VLANs mapped to it will be recommended.

- **Optimal path for select devices**
  
  You can provide the information on devices, which will be part of the new VLAN to be created. This method determines the optimal path for various available instances for the selected devices.

- **Least instance load**
  
  The projected traffic of the new VLAN you selected is used, and the instance which has least overall traffic is recommended.

- **Least instance load for selected devices**
  
  This method assumes that the devices you selected will be part of the new VLAN. Based on this information, the instance with the least load that is spread across the devices you selected is recommended.
Spanning Tree Reports: STP Visualizer

The STP Visualizer allows you to test changes to STP settings before you enforce them on a network. This section explains:

- Interpreting STP Visualizer
- STP Visualizer Notes

To view the STP Visualizer:

**Step 1**
Invoke Switch Cloud Map View from Topology Services.

**Step 2**
Select Reports > STP Visualizer.

The Spanning Tree Visualizer window appears.

**Step 3**
From the Select Instance ID field, click Select.

Depending on the Spanning Tree Protocol the device is running, one of the following appears:

- If the device is running PVST, the Select Instance dialog box appears. Go to **Step 4**.
- If the device is running MST, the Select Region dialog box appears. Go to **Step 5**.
- If the device is running MISTP, the Select Instance dialog box appears. Go to **Step 6**.

**Step 4**
Enter the required information as described in Table 8-8.

To view the devices in the VLAN Region, click Select. The ID of the selected Spanning Tree instance is displayed in the Selected Instance ID field.

### Table 8-8 Selecting PVST or VLAN in Switch Clouds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select instance by type</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the VLAN Name or VLAN ID field, click the drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>• VLAN Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VLAN ID</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of the VLAN Name or VLAN ID.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists VLANs that match the specified criteria.</td>
<td>Select the VLAN from the list of matches.</td>
</tr>
</tbody>
</table>

To view the devices in the VLAN Region, click Select. The ID of the selected Spanning Tree instance is displayed in the Selected Instance ID field.
**Step 5**  
Enter the required information as described in Table 8-9.

<table>
<thead>
<tr>
<th>Table 8-9</th>
<th>Selecting MST in Switch Clouds</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>
| Select instance by region | Select either of the following criteria:  
• All Regions  
• Region Name | To view the valid values for the region field, click the drop-down arrow. |
| What | Enter the string | Use this field to narrow the number of matches by entering the region name (partially or fully). |
| Matches | Lists instances that match the specified criteria. | Select the STP instance from the list of matches. |

To view the Spanning Tree details of an MST Instance in the Network Topology View window, click **Select**. The ID of the selected Spanning Tree instance is displayed in the Selected Instance ID field.

**Step 6**  
Enter the required information as described in Table 8-10.

<table>
<thead>
<tr>
<th>Table 8-10</th>
<th>Selecting MISTP Instances in Switch Clouds</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>
| Select instance by region | Select either of the following criteria:  
• All Instances  
• Instance Name | To view the valid values for the instance field, click the drop-down arrow. |
| What | Enter the string | Use this field to narrow the number of matches by entering part or all of the instance name. |
| Matches | Lists instances that match the specified criteria. | Select the instance from the list of matches. |

To view the Spanning Tree details of an MISTP Instance in the Network Topology View window, click **Select**. The ID of the selected Spanning Tree instance is displayed in the Selected Instance ID field.

The devices in the VLAN instance appear in a table. Table 8-11 lists the fields in the table, their description, and usage notes for editable fields.

<table>
<thead>
<tr>
<th>Table 8-11</th>
<th>Port Details</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the IP address of the device.</td>
<td>This field is not configurable.</td>
</tr>
</tbody>
</table>
| Port | Displays the port name. | This field is not configurable.  
In case of device priority, this field displays NA. |
Interpreting STP Visualizer

The STP Visualizer allows you to:

- Try different Spanning Tree settings offline before you configure them on the network.
- Change settings and highlight devices on the Topology Map.

STP Visualizer Notes

STP Visualizer cannot suggest the correct configuration in the following scenarios:

- If any of the devices in the switch cloud does not support the required MIB (for example CISCO-STP-EXTENSIONS-MIB). In this case you may need to upgrade some of the device images to solve this issue.
- There are device families such as Cisco Catalyst 2900XL and Catalyst 3500XL, which do not support the CISCO-STP-EXTENSIONS-MIB. An error may be displayed, if these devices are present in the switch cloud.
- If there are SNMP request timeouts during discovery of devices, STP Visualizer may not be able to proceed with the computation because of incomplete information about the devices. To resolve the problem, In this case you may need to select these devices and rediscover.
If you are using SNMPv3, not all devices running SNMPv3 support context names for getting required Spanning Tree information from the devices. Only a few later images of Catalyst 6500 series devices support this feature. You may need to use SNMPv2 or SNMPv1 to resolve this problem.

Generating Reports and Configuring STP on the Network

You can generate reports and configure STP on switch clouds for the following:

- Reporting and Configuring PVST Port
- Reporting and Configuring MST Port
- Reporting and Configuring MISTP Port
- Reporting and Configuring PVST Device
- Reporting and Configuring MST Device
- Reporting and Configuring MISTP Device
- Reporting and Configuring MST Instance
- Reporting and Configuring MISTP Instance
- Reporting and Configuring PVST Trunk
- Reporting and Configuring MST Trunk
- Reporting and Configuring MISTP Trunk

Reporting and Configuring PVST Port

To configure PVST port on a switch cloud:

**Step 1** From the Summary View, select **Reports > Spanning Tree Configuration**.

The Spanning Tree Configuration page appears.

**Step 2** Select the **Port** tab.

The Spanning Tree Port Configuration page appears.

**Step 3** Select **PVST** from the Spanning Tree Type drop-down list.

**Step 4** From the Spanning Tree Instance field, click **Select**.

The Select Instance dialog box appears.

**Step 5** Enter the required information as described in the **Table 8-12**.
Step 6  
Click Select to view the devices in the VLAN Instance.

The devices in the VLAN instance appear in a table. Table 8-13 lists the fields in the table, their description, and usage notes for editable fields.

Table 8-12  
**Selecting Spanning Tree Instances in Switch Clouds**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select instance by type</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the VLAN Name or VLAN ID field, click the</td>
</tr>
<tr>
<td></td>
<td>• VLAN Name</td>
<td>drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>• VLAN ID</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the VLAN Name or VLAN ID.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists VLANs that match the specified criteria.</td>
<td>Select the VLAN from the list of matches.</td>
</tr>
</tbody>
</table>

Table 8-13  
**PVST Port Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number used for bridge forwarding.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>IsLink</td>
<td>Displays a check mark if the port is a link port.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>State</td>
<td>State of the port. The possible states are:</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td></td>
<td>• Blocking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Forwarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
</tr>
</tbody>
</table>
### Table 8-13 PVST Port Details (continued)

<table>
<thead>
<tr>
<th>Field1</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>
| Cost*  | Port cost value. | The STP port path cost default value is derived from the media speed of a LAN interface.  
- If there are redundant paths, STP considers port cost when selecting a LAN interface to place that into a forwarding state.  
You can assign lower cost values to LAN interfaces that you want STP to maintain in a forwarding state.  
- If all LAN interfaces have the same cost value, STP puts the LAN interface with the lowest LAN interface number in the forwarding state and blocks other LAN interfaces.  
The possible cost range is 0 through 65535 (the default is media specific).  
STP uses the port cost value when the LAN interface is configured as an access port and uses VLAN port cost values when the LAN interface is configured as a trunk port. |
| Priority* | Port priority. | The STP port path cost default value is derived from the media speed of a LAN interface.  
- If there are redundant paths, STP considers port priority when selecting a LAN port to put into the forwarding state.  
Priority is taken into account after examining cost and sending bridge ID. That is, if the cost and bridge ID is the same, priority is considered.  
- If all LAN ports have the same priority value, STP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports.  
- Values are multiples of 16 ranging from 0-240. The lower the number, the higher the priority. |
| Designated Bridge | Bridge ID for the designated bridge.  
The Designated Bridge provides the minimum root path cost on a LAN.  
Also, it is the only bridge allowed to forward frames to and from the LAN for which it is the designated bridge. | This field is not configurable. |
| Designated Port | ID of the port that connects a LAN to the designated bridge. | This field is not configurable. |
### Table 8-13 PVST Port Details (continued)

<table>
<thead>
<tr>
<th>Field(^1)</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PortFast(^*)</td>
<td>State of the PortFast Interface Configuration feature: Enable or Disable.</td>
<td>Select a value from the drop-down list. When enabled, PortFast causes a switch or trunk port interface to enter the Spanning Tree forwarding state immediately, bypassing the listening and learning states.</td>
</tr>
<tr>
<td>Loop Guard(^*)</td>
<td>State of the Loop Guard feature: Enable or Disable.</td>
<td>Select a value from the drop-down list. When enabled, Loop Guard works on non-designated ports and does not allow the port to become designated via max_age expiry.</td>
</tr>
<tr>
<td>BPDU Guard(^*)</td>
<td>State of the BPDU Guard feature: Enabled, Disabled or Default.</td>
<td>Select a value from the drop-down list. When enabled, BPDU Guard feature prevents loops by moving a nontrunking port into an errdisable state when a BPDU is received on that port. When the BPDU guard feature is enabled on the switch, Spanning Tree shuts down PortFast-configured interfaces that receive BPDUs, instead of putting them into the Spanning Tree blocking state.</td>
</tr>
<tr>
<td>BPDU Filter(^*)</td>
<td>State of the BPDU filter feature: Enabled, Disabled or Default.</td>
<td>Select a value from the drop-down list. When enabled, BPDU filtering allows you to avoid transmitting BPDUs on a port, usually connected to an end system. When you enable PortFast on the switch, Spanning Tree places ports in the forwarding state immediately, instead of going through the listening, learning, and forwarding states.</td>
</tr>
<tr>
<td>Root Guard(^*)</td>
<td>State of the Root Guard feature: Enable or Disable.</td>
<td>Select a value from the drop-down list. When enabled, Root Guard does not allow the port to become non-designated.</td>
</tr>
</tbody>
</table>

1. Fields marked with asterisk are editable.
To edit values of fields marked with an asterisk:

- Select rows, and uncheck Read-only. The selected rows are highlighted in the Edit Here section.

- To change the value of a field, do either of the following:
  - Double click the current value, and enter a new value or
  - Select a value from the drop-down list.

The new values are displayed, highlighted in pink.

**Step 7** Click **Configure** to make changes to the devices. Or Click **Reset** to return to the previous values without making any changes.

---

### Reporting and Configuring MST Port

To configure MST port on a switch cloud:

**Step 1** From the Summary View, select **Reports > Spanning Tree Configuration**.

The Spanning Tree Configuration page appears.

**Step 2** Select the **Port** tab.

The Spanning Tree Port Configuration page appears.

**Step 3** Select **MST** from the Spanning Tree Type drop-down list.

**Step 4** From the Spanning Tree Instance field, click **Select**.

The Select Instance dialog box appears.

**Step 5** Enter the required information as described in the Table 8-14.

**Table 8-14 Selecting Spanning Tree Instances in Switch Clouds**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select instance by region</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the region field, click the drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>• All Regions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Region Name</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the region name.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists instances that match the specified criteria</td>
<td>Select the STP instance from the list of matches.</td>
</tr>
</tbody>
</table>

- To view the devices in the VLAN Region, click **Select**.

The devices running the selected MST instance appear in a table. Table 8-15 lists the fields in the table, their description, and usage notes for editable fields.
### Table 8-15  MST Port Details

<table>
<thead>
<tr>
<th>Field^1</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number used for bridge forwarding</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>isLink</td>
<td>Displays a check mark if the port is a link port</td>
<td>This field is not configurable.</td>
</tr>
</tbody>
</table>
| LinkType | Link type of the port. The possible link types are:  
  • Point-to-point link  
  • Shared medium  
By default, the switch derives the link type of a port from the duplex mode.  
A full-duplex port is considered as a point-to-point link while a half-duplex configuration is assumed to be on a shared link. | This field is not configurable. |
| Cost* | Port cost value | The STP port path cost default value is derived from the media speed of a LAN interface.  
• If a loop occurs, STP considers port cost when selecting a LAN interface to place that into the forwarding state.  
You can assign lower cost values to LAN interfaces that you want STP to select first and higher cost values to LAN interfaces that you want STP to select last.  
• If all LAN interfaces have the same cost value, STP puts the LAN interface with the lowest LAN interface number in the forwarding state and blocks other LAN interfaces.  
The possible cost range is 0 through 65535 (the default is media specific).  
STP uses the port cost value when the LAN interface is configured as an access port and uses VLAN port cost values when the LAN interface is configured as a trunk port. |
### Table 8-15  MST Port Details (continued)

<table>
<thead>
<tr>
<th>Field¹</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>
| Priority² | Port priority | • If a loop occurs, STP considers port priority when selecting a LAN port to put into the forwarding state.  
You can assign higher priority values to LAN ports that you want STP to select first and lower priority values to LAN ports that you want STP to select last.  
• If all LAN ports have the same priority value, STP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports.  
• Values are multiples of 16 ranging from 0-240. The lower the number, the higher the priority. |
| State | State of the port. The possible states are:  
• Blocking  
• Forwarding  
• Disabled | This field is not configurable. |
| Status | Indicates if the port lies in the boundary of an MST region.  
If yes, the status is shown as Boundary.  
If not, the field is left blank. | In generic terms, a port is at the boundary of a region:  
If the designated bridge on its segment is in a different region  
Or  
If it receives legacy 802.1d BPDUs. |
| Role | Role of the port. The possible roles are:  
• Root  
• Designated  
• Alternate  
• Backup  
• Disabled  
MST assigns port roles as follows:  
• Root port or designated port role includes the port in the active topology.  
• Alternate port or backup port role excludes the port from the active topology. | This field is not configurable. |
### Table 8-15 MST Port Details (continued)

<table>
<thead>
<tr>
<th>Field1</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designated Bridge</td>
<td>Bridge ID for the designated bridge. The Designated Bridge provides the minimum root path cost on a LAN. Also, it is the only bridge allowed to forward frames to and from the LAN for which it is the designated bridge.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Designated Port</td>
<td>Displays the ID of the port that connects a LAN to the designated bridge</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>PortFast*</td>
<td>Displays the state of the PortFast Interface Configuration feature: Enabled or Disabled</td>
<td>Select a value from the drop-down list. When enabled, PortFast causes a switch or trunk port interface to enter the Spanning Tree forwarding state immediately, bypassing the listening and learning states.</td>
</tr>
<tr>
<td>Loop Guard*</td>
<td>Displays the state of the Loop Guard feature: Enable or Disable.</td>
<td>Select a value from the drop-down list. When enabled, Loop guard works on non-designated ports and does not allow the port to become designated via max_age expiry.</td>
</tr>
<tr>
<td>BPDU Guard*</td>
<td>Displays the state of the BPDU Guard feature: Enabled, Disabled or Default.</td>
<td>Select a value from the drop-down list. When enabled, BPDU Guard feature prevents loops by moving a nontrunking port into an enable state when a BPDU is received on that port. When the BPDU Guard feature is enabled on the switch, Spanning Tree shuts down PortFast-configured interfaces that receive BPDUs, instead of putting them into the Spanning Tree blocking state.</td>
</tr>
</tbody>
</table>
Chapter 8  Managing Network Spanning Trees

Generating Reports and Configuring STP on the Network

To edit values of fields marked with an asterisk, select rows, and uncheck Read-only. The selected rows are highlighted in the Edit Here section.

- To change the value of a field, do either of the following:
  - Double click the current value, and enter a new value,
  or
  - Select a value from the drop-down list.
  The new values appear, highlighted in pink.

Step 6
Click Configure to make changes to the devices.
Or
Click Reset to return to the previous values without making any changes.

Reporting and Configuring MISTP Port

To configure MISTP port on a switch cloud:

Step 1
From the Summary View, select Reports > Spanning Tree Configuration.
The Spanning Tree Configuration page appears.

Step 2
Select the Port tab.
The Spanning Tree Port Configuration page appears.

Step 3
Select MISTP from the Spanning Tree Type drop-down list.
Step 4  From the Spanning Tree Instance field, click **Select**.
The Select Instance dialog box appears.

Step 5  Enter the required information as described in the Table 8-16.

### Table 8-16  Selecting Spanning Tree Instances in Switch Clouds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select device by instance</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the instance field, click the drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>• All Instances</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Instance Name</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of the instance name.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists instances that match the specified criteria.</td>
<td>Select the instance from the list of matches.</td>
</tr>
</tbody>
</table>

To view the devices in the VLAN Instance, click **Select**.
The devices running the selected MIST instance appear in a table. Table 8-17 lists the fields in the table, their description, and usage notes for editable fields.

### Table 8-17  MISTP Port Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number used for bridge forwarding</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>isLink</td>
<td>Displays a check mark if the port is a link port</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>State</td>
<td>State of the port. The possible states are:</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td></td>
<td>• Blocking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Forwarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
</tr>
</tbody>
</table>
**Table 8-17 MISTP Port Details (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost*</td>
<td>Port cost value</td>
<td>The STP port path cost default value is derived from the media speed of a LAN interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If a loop occurs, STP considers port cost when selecting a LAN interface to place that into the forwarding state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can assign lower cost values to LAN interfaces that you want STP to select first and higher cost values to LAN interfaces that you want STP to select last.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If all LAN interfaces have the same cost value, STP puts the LAN interface with the lowest LAN interface number in the forwarding state and blocks other LAN interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The possible cost range is 0 through 65535 (the default is media specific).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>STP uses the port cost value when the LAN interface is configured as an access port and uses VLAN port cost values when the LAN interface is configured as a trunk port.</td>
</tr>
<tr>
<td>Priority*</td>
<td>Port priority</td>
<td>• If a loop occurs, STP considers port priority when selecting a LAN port to put into the forwarding state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can assign higher priority values to LAN ports that you want STP to select first and lower priority values to LAN ports that you want STP to select last.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If all LAN ports have the same priority value, STP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Values are multiples of 16 ranging from 0-240. The lower the number, the higher the priority.</td>
</tr>
<tr>
<td>Designated</td>
<td>Bridge ID for the designated</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Bridge</td>
<td>bridge.</td>
<td>The Designated Bridge provides the minimum root path cost on a LAN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Also, it is the only bridge allowed to forward frames to and from the LAN for which it is the designated bridge.</td>
</tr>
<tr>
<td>Designated</td>
<td>ID of the port that connects a</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Port</td>
<td>LAN to the designated bridge.</td>
<td></td>
</tr>
</tbody>
</table>
To edit values of fields marked with an asterisk, select rows, and uncheck **Read-only**. The selected rows are highlighted in the Edit Here section.

To change the value of a field, do either of the following:
- Double click the current value, and enter a new value,
  or
- Select a value from the drop-down list.

The new values appear, highlighted in pink.

**Step 6**  
Click **Configure** to make changes to the devices. Or  
Click **Reset** to return to the previous values without making any changes.

### Table 8-17 MISTP Port Details (continued)

<table>
<thead>
<tr>
<th>Field†</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>

| PortFast* | State of the PortFast Interface Configuration feature:  
Enabled or Disabled. | Select a value from the drop-down list.  
When enabled, PortFast causes a switch or trunk port interface to enter the Spanning Tree forwarding state immediately, bypassing the listening and learning states. |

| Loop Guard* | State of the loop guard feature:  
Enable or Disable. | Select a value from the drop-down list.  
When enabled, Loop Guard works on non-designated ports and does not allow the port to become designated via max_age expiry. |

| BPDU Guard† | State of the BPDU guard feature:  
Enabled, Disabled or Default. | Select a value from the drop-down list.  
When enabled, BPDU Guard feature prevents loops by moving a nontrunking port into an errdisable state when a BPDU is received on that port.  
When the BPDU Guard feature is enabled on the switch, Spanning Tree shuts down PortFast-configured interfaces that receive BPDUs, instead of putting them into the Spanning Tree blocking state. |

| BPDU Filter* | State of the BPDU filter feature:  
Enabled, Disabled or Default. | Select a value from the drop-down list.  
When enabled, BPDU filtering allows you to avoid transmitting BPDUs on a port, usually connected to an end system.  
When you enable PortFast on the switch, Spanning Tree places ports in the forwarding state immediately, instead of going through the listening, learning, and forwarding states. |

| Root Guard* | State of the Root guard feature:  
Enable or Disabled. | Select a value from the drop-down list.  
When enabled, Root Guard does not allow the port to become non-designated. |

1. Fields marked with asterisk are editable.
Reporting and Configuring PVST Device

To configure PVST device on a switch cloud:

**Step 1** From the Summary View, select **Reports > Spanning Tree Configuration**. The Spanning Tree Configuration page appears.

**Step 2** Select the Device tab. The Spanning Tree Device Configuration page appears.

**Step 3** Select **PVST** from the Spanning Tree Type drop-down list. PVST details appear in text boxes. Table 8-18 lists the displayed fields and descriptions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Bridge</td>
<td>IP address of the switch.</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>Forward Delay timer. This determines how long each of the listening and learning states last</td>
</tr>
<tr>
<td></td>
<td>before the port begins forwarding.</td>
</tr>
<tr>
<td>HelloTime</td>
<td>Hello timer. This is the number of seconds between STP configuration messages. The HelloTime</td>
</tr>
<tr>
<td></td>
<td>determines how often the network device broadcasts hello messages to other network devices.</td>
</tr>
<tr>
<td>Max Age</td>
<td>Maximum age timer. This determines the amount of time protocol information received on a port</td>
</tr>
<tr>
<td></td>
<td>is stored by the network device.</td>
</tr>
</tbody>
</table>

**Step 4** From the Spanning Tree Instance field, click **Select**. The Select Instance dialog box appears.

**Step 5** Enter the required information as described in the Table 8-19.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select instance by</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the VLAN Name or VLAN ID field, click the</td>
</tr>
<tr>
<td>type</td>
<td>VLAN Name, VLAN ID</td>
<td>drop-down arrow.</td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the VLAN Name or VLAN ID.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists VLANs that match the specified criteria.</td>
<td>Select the VLAN from the list of matches.</td>
</tr>
</tbody>
</table>

- To view the devices in the VLAN Instance, click **Select**. The devices in the VLAN instance appear in a table. Table 8-20 lists the fields in the table, their description, and usage notes for editable fields.
### Table 8-20 PVST Device Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Root ID</td>
<td>ID of the bridge assumed to be root. On initialization, each bridge assumes itself as root.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Root Port</td>
<td>ID of the port, which is closest to the root.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Cost Mode</td>
<td>Type of Spanning Tree path cost mode configured on the device.</td>
<td>Applies to all STP instances running on the device.</td>
</tr>
<tr>
<td></td>
<td>When you change, the path cost of all ports are reassigned to the default path cost values based on the new Spanning Tree path cost mode and ports' speed. The possible values are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Short—Short cost is specified by 802.1d</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Long—Long cost is specified by 802.1t</td>
<td></td>
</tr>
<tr>
<td>Root Cost</td>
<td>Cost of the root.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Extended SysID*</td>
<td>State of the extended system ID feature on the switch:</td>
<td>Select a value from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>Enable, Disabled, or Unknown</td>
<td>STP uses the VLAN ID as the extended system ID. It uses the extended system ID plus a MAC address to make the bridge ID unique for each VLAN.</td>
</tr>
<tr>
<td>Priority*</td>
<td>Bridge priority</td>
<td>The device with the lowest bridge identifier is considered the highest priority bridge and becomes the root bridge. By default, the bridge priority is set to 32768.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the bridge priority command to set the priority that the bridge Spanning Tree uses to choose the root bridge in the network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bridge priority can range from 0 to 65535. But if you have enabled MAC address reduction, the root bridge priority becomes a multiple of 4096 plus the VLAN ID.</td>
</tr>
<tr>
<td>Backbone Fast*</td>
<td>State of the Backbonefast feature:</td>
<td>Select a value from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>Enabled or Disabled.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 8-20 PVST Device Details (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uplink Fast*</td>
<td>State of the Uplinkfast feature: Enabled or Disabled.</td>
<td>Select a value from the drop-down list. When enabled, UplinkFast feature dramatically decreases the convergence time of the STP in the event of the failure of an uplink on an access switch.</td>
</tr>
<tr>
<td>Loop Guard*</td>
<td>State of the Loop Guard feature: Enable or Disable.</td>
<td>Select a value from the drop-down list. When enabled, Loop Guard works on non-designated ports and does not allow the port to become designated via max_age expiry.</td>
</tr>
<tr>
<td>PortFast Global*</td>
<td>State of the PortFast Global Configuration feature: Enabled or Disabled.</td>
<td>Select a value from the drop-down list. When enabled, PortFast causes a switch or trunk port to enter the Spanning Tree forwarding state immediately, bypassing the listening and learning states. If you configure the default on each port, this setting applies to interfaces.</td>
</tr>
<tr>
<td>BPDU Filter*</td>
<td>State of the BPDU Filter feature: Enabled, Disabled or Default.</td>
<td>Select a value from the drop-down list. When enabled, BPDU filtering allows you to avoid transmitting BPDUs on a port, usually connected to an end system. When you enable PortFast on the switch, Spanning Tree places ports in the forwarding state immediately, instead of going through the listening, learning, and forwarding states.</td>
</tr>
<tr>
<td>BPDU Guard*</td>
<td>State of the BPDU Guard feature: Enabled, Disabled or Default.</td>
<td>Select a value from the drop-down list. When enabled, BPDU Guard feature prevents loops by moving a nontrunking port into an errdisable state when a BPDU is received on that port. When the BPDU Guard feature is enabled on the switch, Spanning Tree shuts down PortFast-configured interfaces that receive BPDUs, instead of putting them into the Spanning Tree blocking state.</td>
</tr>
</tbody>
</table>

1. Fields marked with asterisk are editable.
To edit values of fields marked with an asterisk, select rows, and uncheck **Read-only**. The selected rows are highlighted in the Edit Here section.

To change the value of a field, do either of the following:

- Double click the current value, and enter a new value,
- Select a value from the drop-down list.

The new values are displayed, highlighted in pink.

**Step 6**

Click **Configure** to make changes to the devices.

Or

Click **Reset** to return to the previous values without making any changes.

---

## Reporting and Configuring MST Device

To configure MST port on a switch cloud:

**Step 1**

From the Summary View, select **Reports > Spanning Tree Configuration**.

The Spanning Tree Configuration page appears.

**Step 2**

Select the Device tab.

The Spanning Tree Device Configuration page appears.

**Step 3**

Select **MST** from the Spanning Tree Type drop-down list.

MST details appear in text boxes. Table 8-21 lists the displayed fields and descriptions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Bridge</td>
<td>IP address of the switch.</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>Forward delay timer. This determines how long each of the listening and learning states last before the port begins forwarding.</td>
</tr>
<tr>
<td>HelloTime</td>
<td>Hello timer. This is the number of seconds between STP configuration messages. The HelloTime determines how often the network device broadcasts hello messages to other network devices.</td>
</tr>
<tr>
<td>Max Age</td>
<td>Maximum age timer. This determines the amount of time protocol information received on a port is stored by the network device.</td>
</tr>
</tbody>
</table>

**Step 4**

From the Spanning Tree Instance field, click **Select**.

The Select Instance dialog box appears.
**Step 5** Enter the required information as described in Table 8-22.

**Table 8-22** Selecting Spanning Tree Instances in Switch Clouds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select instance by region</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the region field, click the drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>• All Regions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Region Name</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of the region name.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists instances that match the specified criteria</td>
<td>Select the STP instance from the list of matches.</td>
</tr>
</tbody>
</table>

- To view the devices in the Instance, click Select.

The devices in the instance appear in a table.

Table 8-23 lists the fields in the table, their description, and usage notes for editable fields.
### Table 8-23  
**MST Device Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Root ID</td>
<td>ID of the bridge assumed to be root. Upon initialization, the bridge assumes that it is root.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Root Port</td>
<td>Port ID of the port, which is closest to the root.</td>
<td>This field is not configurable.</td>
</tr>
</tbody>
</table>
| Cost Mode      | Type of Spanning Tree path cost mode configured on the device. Applies to all STP instances running on the device. When you change the value, the path cost of all ports are reassigned to the default path cost values based on the new Spanning Tree path cost mode and ports' speed. The possible values are:  
  - Short—Short cost is specified by 802.1d  
  - Long—Long cost is specified by 802.1t | This field is not configurable.                                           |
| Root Cost      | Cost of the root.                                                           | This field is not configurable.                                           |
| Extended SysID*| State of the extended system ID feature on the switch: Enable, Disabled, or Unknown | Select a value from the drop-down list.                                   |
| Priority*      | Bridge priority                                                             | The device with the lowest bridge identifier is considered the highest priority bridge and becomes the root bridge. By default, the bridge priority is set to 32768. Use the bridge priority command to set the priority that the bridge Spanning Tree uses to choose the root bridge in the network. The range for bridge priority is 0 to 65535. The value should be a multiple of 4096. |
| Region Name*   | Alphanumeric configuration name assigned to the MST region that the switch is part of. | Enter a new name in the field to change the region name. For two or more switches to be in the same MST region, they must have the same VLAN-to-instance map, the same configuration revision number, and the same configuration name. |
### Table 8-23 MST Device Details (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region Revision*</td>
<td>MST configuration revision number (0 to 65535).</td>
<td>Enter a new value in the field to change the revision number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For two or more switches to be in the same MST region, they must have the same VLAN-to-instance map, the same configuration revision number, and the same configuration name.</td>
</tr>
<tr>
<td>Max. Hop Count</td>
<td>Number of hops in an MST region after which a BPDU is discarded, and the information held for a port is aged. (1 to 40; default is 20).</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>VLANs</td>
<td>List of VLANs that form part of the MST region.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Loop Guard*</td>
<td>State of the Loop Guard feature: Enable or Disable.</td>
<td>Select a value from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When enabled, loop guard works on non-designated ports and does not allow the port to become designated via max_age expiry.</td>
</tr>
<tr>
<td>PortFast Global*</td>
<td>State of the PortFast Global Configuration feature: Enabled or Disabled.</td>
<td>Select a value from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When enabled, PortFast causes a switch or trunk port to enter the Spanning Tree forwarding state immediately, bypassing the listening and learning states.</td>
</tr>
<tr>
<td>BPDU Filter*</td>
<td>State of the BPDU filter feature: Enabled, Disabled or Default.</td>
<td>Select a value from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When enabled, BPDU filtering allows you to avoid transmitting BPDUs on a port, usually connected to an end system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When you enable PortFast on the switch, Spanning Tree places ports in the forwarding state immediately, instead of going through the listening, learning, and forwarding states.</td>
</tr>
<tr>
<td>BPDU Guard*</td>
<td>State of the BPDU Guard feature: Enabled, Disabled or Default.</td>
<td>Select a value from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When enabled, BPDU Guard feature prevents loops by moving a nontrunking port into an errdisable state when a BPDU is received on that port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When the BPDU Guard feature is enabled on the switch, Spanning Tree shuts down PortFast-configured interfaces that receive BPDUs, instead of putting them into the Spanning Tree blocking state.</td>
</tr>
</tbody>
</table>

1. Fields marked with asterisk are editable.
To edit values of fields marked with an asterisk, select rows, and uncheck Read-only. The selected rows are highlighted in the Edit Here section.

To change the value of a field, do either of the following:
- Double click the current value, and enter a new value,
or
- Select a value from the drop-down list.
The new values appear, highlighted in pink.

**Step 6**
Click **Configure** to make changes to the devices.
Or
Click **Reset** to return to the previous values without making any changes.

---

### Reporting and Configuring MISTP Device

To configure MISTP port on a switch cloud:

**Step 1**
From the Summary View, select **Reports > Spanning Tree Configuration**.
The Spanning Tree Configuration page appears.

**Step 2**
Select the Device tab.
The Spanning Tree Device Configuration page appears.

**Step 3**
Select **MISTP** from the Spanning Tree Type drop-down list.
MISTP details appear in text boxes. Table 8-24 lists the displayed fields and descriptions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Bridge</td>
<td>IP address of the switch.</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>Forward Delay timer. This determines how long each of the listening and learning states last before the port begins forwarding.</td>
</tr>
<tr>
<td>HelloTime</td>
<td>Hello timer. This is the number of seconds between STP configuration messages. The HelloTime determines how often the network device broadcasts hello messages to other network devices.</td>
</tr>
<tr>
<td>Max Age</td>
<td>Maximum age timer. This determines the amount of time protocol information received on a port is stored by the network device.</td>
</tr>
</tbody>
</table>

**Step 4**
From the Spanning Tree Instance field, click **Select**.
The Select Instance dialog box appears.
Step 5 Enter the required information as described in the Table 8-25.

Table 8-25 Selecting Spanning Tree Instances in Switch Clouds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select device by instance</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the instance field, click the drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>• All Instances</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Instance Name</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of the instance name.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists instances that match the specified criteria.</td>
<td>Select the instance from the list of matches.</td>
</tr>
</tbody>
</table>

- To view the devices in the MISTP instance, click Select.

The devices in the instance appear in a table. Table 8-26 lists the fields in the table, their description, and usage notes for editable fields.

Table 8-26 MISTP Device Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Root ID</td>
<td>ID of the bridge assumed to be root. Upon initialization, the bridge assumes that it is root.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Root Port</td>
<td>Port ID of the port, which is closest to the root.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Cost Mode</td>
<td>Type of Spanning Tree path cost mode configured on the device. Applies to all STP instances running on the device. When you change the value, the path cost of all ports will be reassigned to the default path cost values based on the new Spanning Tree path cost mode and ports’ speed. The possible values are: • Short—Short cost is specified by 802.1d • Long—Long cost is specified by 802.1t</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Root Cost</td>
<td>Cost of the root.</td>
<td>This field is not configurable.</td>
</tr>
</tbody>
</table>
### Table 8-26  MISTP Device Details (continued)

<table>
<thead>
<tr>
<th>Field(^\d)</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended SysID(^*)</td>
<td>State of the extended system ID feature on the switch: Enable, Disabled, or Unknown</td>
<td>Select a value from the drop-down list.</td>
</tr>
<tr>
<td>Priority(^*)</td>
<td>Bridge priority</td>
<td>The device with the lowest bridge identifier is considered the highest priority bridge and becomes the root bridge. By default, the bridge priority is set to 32768. Use the bridge priority command to set the priority that the bridge Spanning Tree uses to choose the root bridge in the network. The range for bridge priority is 0 to 65535. The value should be a multiple of 4096.</td>
</tr>
<tr>
<td>Backbone Fast(^*)</td>
<td>State of the Backbonefast feature: Enabled or Disabled.</td>
<td>Select a value from the drop-down list.</td>
</tr>
<tr>
<td>Uplink Fast(^*)</td>
<td>State of the Uplinkfast feature: Enabled or Disabled.</td>
<td>Select a value from the drop-down list. When enabled, UplinkFast feature dramatically decreases the convergence time of the STP in the event of the failure of an uplink on an access switch.</td>
</tr>
<tr>
<td>Loop Guard(^*)</td>
<td>State of the Loop Guard feature: Enable or Disable.</td>
<td>Select a value from the drop-down list. When enabled, loop guard works on non-designated ports and does not allow the port to become designated via max_age expiry.</td>
</tr>
<tr>
<td>PortFast Global(^*)</td>
<td>State of the PortFast Global Configuration feature: Enabled or Disabled.</td>
<td>Select a value from the drop-down list. When enabled, PortFast causes a switch or trunk port to enter the Spanning Tree forwarding state immediately, bypassing the listening and learning states.</td>
</tr>
</tbody>
</table>
To edit values of fields marked with an asterisk, select rows, and uncheck Read-only. The selected rows are highlighted in the Edit Here section.

To change the value of a field, do either of the following:
- Double click the current value, and enter a new value,
or
- Select a value from the drop-down list.
The new values appear, highlighted in pink.

Step 6 Click Configure to make changes to the devices.

Or

Click Reset to return to the previous values without making any changes.

Table 8-26 MISTP Device Details (continued)

<table>
<thead>
<tr>
<th>Field¹</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPDU Filter*</td>
<td>State of the BPDU Filter feature: Enabled, Disabled or Default.</td>
<td>Select a value from the drop-down list. When enabled, BPDU filtering allows you to avoid transmitting BPDUs on a port, usually connected to an end system. When you enable PortFast on the switch, Spanning Tree places ports in the forwarding state immediately, instead of going through the listening, learning, and forwarding states.</td>
</tr>
<tr>
<td>BPDU Guard*</td>
<td>State of the BPDU Guard feature: Enabled, Disabled or Default.</td>
<td>Select a value from the drop-down list. When enabled, BPDU Guard feature prevents loops by moving a nontrunking port into an errdisable state when a BPDU is received on that port. When the BPDU Guard feature is enabled on the switch, Spanning Tree shuts down PortFast-configured interfaces that receive BPDUs, instead of putting them into the Spanning Tree blocking state.</td>
</tr>
</tbody>
</table>

¹. Fields marked with asterisk are editable.

Note Preferred VLANs are available only on Cisco Catalyst switches running Catalyst operating system.
Reporting and Configuring MST Instance

To configure MST instance on a switch cloud:

**Step 1**
From the Summary View, select Reports > Spanning Tree Configuration. The Spanning Tree Configuration page appears.

**Step 2**
Select the Instance tab. The Spanning Tree Port Instance Configuration page appears.

**Step 3**
Select MST from the Spanning Tree Type drop-down list.

**Step 4**
From the Device field, click Select. The Select Device dialog box appears.

**Step 5**
Enter the required information as described in the Table 8-27.

### Table 8-27 Selecting Devices in Switch Clouds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select device by filter</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the filter field, click the drop-down arrow.</td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of the name, IP address or system name.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists devices that match the specified criteria.</td>
<td>Select the device from the list of matches.</td>
</tr>
</tbody>
</table>

- To view the MST instances that are running on the device, click Select.
  The instance and VLAN appear in a table. Table 8-28 lists the fields in the table, their description, and usage notes for editable fields.

### Table 8-28 MST Instance Details

<table>
<thead>
<tr>
<th>Field¹</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>MST instance that the device is part of.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>VLANS *</td>
<td>VLANs that are mapped to the instance.</td>
<td>Select a value from the drop-down list.</td>
</tr>
</tbody>
</table>

1. Fields marked with asterisk are editable.
• To edit the instance to VLAN mapping, select the particular instance, and uncheck Read-only. The selected rows are highlighted in the Edit Here section.
• To change the value of a field, do either of the following:
  - Double click the current value, and enter a new value,
  Or
  - Select a value from the drop-down list.
The new values are displayed, highlighted in pink.

**Step 6**
Click **Configure** to make changes to the devices.
Or
Click **Reset** to return to the previous values without making any changes.

---

### Reporting and Configuring MISTP Instance

To configure MISTP instance on a switch cloud:

**Step 1**
From the Summary View, select **Reports > Spanning Tree Configuration**.
The Spanning Tree Configuration page appears.

**Step 2**
Select the Instance tab.
The Spanning Tree Port Instance Configuration page appears.

**Step 3**
Select **MISTP** from the Spanning Tree Type drop-down list.

**Step 4**
From the Device field, click **Select**.
The Select Device dialog box appears.

**Step 5**
Enter the required information as described in **Table 8-29**.

---

### Table 8-29  Selecting Devices in Switch Clouds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select device by filter</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the filter field, click the drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Device IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SysName</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of the name, IP address or system name.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists devices that match the specified criteria.</td>
<td>Select the device from the list of matches.</td>
</tr>
</tbody>
</table>
Step 6  To view the MST instances that are running on the device, click Select.
The instance and VLAN appear in a table. Table 8-30 lists the fields in the table, their description, and usage notes for editable fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>MISTP instance that the device is part of.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>VLANS*</td>
<td>VLANs that the device is part of.</td>
<td>Select a value from the drop-down list.</td>
</tr>
</tbody>
</table>

1. Fields marked with asterisk are editable.

- To edit the instance to VLAN mapping, select the particular instance, and uncheck Read-only. The selected rows are highlighted in the Edit Here section.
- To change the value of a field, do either of the following:
  - Double click the current value, and enter a new value, or
  - Select a value from the drop-down list.

  The new values are displayed, highlighted in pink.

Step 7  Click Configure to make changes to the devices.
Or
Click Reset to return to the previous values without making any changes.

Reporting and Configuring PVST Trunk

To configure PVST trunk on a switch cloud:

Step 1  From the Summary View, select Reports > Spanning Tree Configuration.
The Spanning Tree Configuration page appears.

Step 2  Select the Trunk tab.
The Spanning Tree Port Trunk Configuration page appears.

Step 3  Select PVST from the Spanning Tree Type drop-down list.

Step 4  From the Device field, click Select.
The Select Device dialog box appears.
Enter the required information as described in the Table 8-31.

**Table 8-31  **Selecting Devices in Switch Clouds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select device by filter</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the filter field, click the drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Device IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SysName</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of the name, IP address or system name.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists devices that match the specified criteria.</td>
<td>Select the device from the list of matches.</td>
</tr>
</tbody>
</table>

The instance and VLAN appear in a table. Table 8-32 lists the fields in the table, their description, and usage notes for editable fields.

**Table 8-32  PVST Trunk Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Port</td>
<td>Trunk port on the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>isTrunk</td>
<td>Displays a check mark if the port is a trunk port.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Preferred VLANs *</td>
<td>Preferred VLANs the trunk port is configured for.</td>
<td>Preferred VLANs are VLANs you prefer to keep in forwarding mode on a trunk link. You can do this by setting the port instance cost of these VLANs to be lower than the other VLANs. When port instance cost is lowered these instances are made forwarding on the trunk as against the other. You can load balance VLAN traffic across multiple trunk links. For example, if you want to have some VLANs to use only a particular trunk link, then you can lower their STP cost so that they are preferred over that link.</td>
</tr>
</tbody>
</table>

1. Fields marked with asterisk are editable.
• Uncheck Read-only, and select the trunk port.
  The selected rows are highlighted in the Edit Here section.
• Select the trunk port, and enter the VLANs that have to be preferred in the Edit Here section.
• To change the value of a field, do either of the following:
  – Double click the current value, and enter a new value,
  or
  – Select a value from the drop-down list.
  The new values appear, highlighted in pink.

Step 6 Click Configure to make changes to the devices.
Or
Click Reset to return to the previous values without making any changes.

---

Note Preferred VLANs are available only on Cisco Catalyst switches running Catalyst operating system.

### Reporting and Configuring MST Trunk

To configure MST trunk on a switch cloud:

---

**Step 1** From the Summary View, select Reports > Spanning Tree Configuration.
The Spanning Tree Configuration page appears.

**Step 2** Select the Trunk tab.
The Spanning Tree Port Trunk Configuration page appears.

**Step 3** Select MST from the Spanning Tree Type drop-down list.

**Step 4** From the Device field, click Select.
The Select Device dialog box appears.
Step 5  Enter the required information as described in Table 8-33.

Table 8-33  Selecting Devices in Switch Clouds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select device by filter</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the filter field, click the drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>- Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Device IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SysName</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the name, IP address or system name.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists devices that match the specified criteria.</td>
<td>Select the device from the list of matches.</td>
</tr>
</tbody>
</table>

The instance and VLAN appear in a table. Table 8-34 lists the fields in the table, their description, and usage notes for editable fields.

Table 8-34  MST Trunk Details

<table>
<thead>
<tr>
<th>Field1</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number used for bridge forwarding.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>isTrunk</td>
<td>Displays a check mark if the port is a trunk port.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Preferred Instance *</td>
<td>Preferred instances the trunk port is configured for.</td>
<td>Preferred VLANs are VLANs you prefer to keep in forwarding mode on a trunk link. You can do this by setting the port instance cost of these VLANs to be lower than the other VLANs. When port instance cost is lowered, these instances are made forwarding on the trunk as against the other. You can load balance VLAN traffic across multiple trunk links. For example, if you want to have some VLANs to use only a particular trunk link, then you can lower their STP cost so that they are preferred over that link.</td>
</tr>
</tbody>
</table>

1. Fields marked with asterisk are editable.

- Uncheck Read-only, and select the trunk port.
  The selected rows are highlighted in the Edit Here section.
- Select the trunk port, and enter the VLANs that have to be preferred in the Edit Here section.
To change the value of a field, do either of the following:
- Double click the current value, and enter a new value,
or
- Select a value from the drop-down list.
The new values appear, highlighted in pink.

**Step 6**
Click **Configure** to make changes to the devices.
Or
Click **Reset** to return to the previous values without making any changes.

---

**Note**
Preferred VLANs are available only on Cisco Catalyst switches running Catalyst operating system.

---

**Reporting and Configuring MISTP Trunk**

To configure MISTP trunk on a switch cloud:

**Step 1**
From the Summary View, select **Reports > Spanning Tree Configuration**.
The Spanning Tree Configuration page appears.

**Step 2**
Select the Trunk tab.
The Spanning Tree Port Trunk Configuration page appears.

**Step 3**
Select **MST** from the Spanning Tree Type drop-down list.

**Step 4**
From the Device field, click **Select**.
The Select Device dialog box appears.

**Step 5**
Enter the required information as described in Table 8-35.

### Table 8-35  Selecting Devices in Switch Clouds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select device by filter</td>
<td>Select desired criteria:</td>
<td>To view the valid values for the filter field, click the drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Device IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SysName</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the desired string</td>
<td>Use this field to narrow the number of matches by entering part or all of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the name, IP address or system name.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists devices that match the specified criteria.</td>
<td>Select the desired device from the list of matches.</td>
</tr>
</tbody>
</table>

The instance and VLAN appear in a table. Table 8-36 lists the fields in the table, their description, and usage notes for editable fields.
Table 8-36  MST Trunk Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number used for bridge forwarding.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>isTrunk</td>
<td>Displays a check mark if the port is a trunk port.</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Preferred Instance *</td>
<td>Preferred instances the trunk port is configured for.</td>
<td>Preferred VLANs are VLANs you prefer to keep in forwarding mode on a trunk link. You can do this by setting the port instance cost of these VLANs to be lower than the other VLANs. When port instance cost is lowered these instances are made forwarding on the trunk as against the other. You can load balance VLAN traffic across multiple trunk links. For example, if you want to have some VLANs to use only a particular trunk link, then you can lower their STP cost so that they are preferred over that link.</td>
</tr>
</tbody>
</table>

1. Fields marked with asterisk are editable.

- Uncheck Read-only, and select the trunk port.
  The selected rows are highlighted in the Edit Here section.
- Select the trunk port, and enter the VLANs that have to be preferred in the Edit Here section.
- To change the value of a field, do either of the following:
  - Double click the current value, and enter a new value,
  or
  - Select a value from the drop-down list.
  The new values appear, highlighted in pink.

**Step 6**

Click Configure to make changes to the devices.
Or
Click Reset to return to the previous values without making any changes.

**Note**

Preferred VLANs are available only on Cisco Catalyst switches running Catalyst operating system.
Spanning Tree Filters

Topology Map provides two filters for STP enabled devices or links. These filters are available in the topology maps for Switch Clouds under LAN Edge View.

- STP Inconsistency
- STP Filters in Switch Cloud View
- Viewing STP Loop Inconsistency

STP Inconsistency

If your network has incorrect configurations, STP stops functioning and you may lose connectivity. STP Inconsistency detects these incorrect configurations in your network and changes the state to inconsistent for corresponding ports, thus preventing the ports from affecting the network.

When you select the filter, Topology View highlights the link and device associated with that specific STP inconsistency.

STP inconsistencies are computed during each data collection. Devices in the switched clouds are polled when the filter is applied.

Topology Map provides four filters under STP Inconsistency:

- Loop (Viewing STP Loop Inconsistency)
- PVID (Viewing STP PVID Inconsistency)
- Root (Viewing STP Root Inconsistency)
- Type (Viewing STP Type Inconsistency)

Spanning Tree

These filters are based on the Spanning Tree details of devices. When you select the filter, topology map lists the Spanning Tree Instances applicable to all the switches in the selected switch cloud. Topology Map provides three filters under Spanning Tree:

- IEEE 802.1s Instance (Viewing Spanning Tree per IEEE 802.1s Instance)
- Cisco MIST Instance (Viewing Spanning Tree per Cisco MISTP Instances)
- VLAN (Viewing VLANs in Switch Clouds)

Viewing STP Loop Inconsistency

To view STP loop inconsistencies in switch clouds:

1. **Step 1**
   Invoke Switch Cloud Map View from Topology Services.

2. **Step 2**
   Select **Topology Filters > STP Inconsistency > Loop**.

The link and devices with loop inconsistencies appear.
Viewing STP PVID Inconsistency

To view STP PVID inconsistencies in switch clouds:

- **Step 1** Invoke Switch Cloud Map View from Topology Services.
- **Step 2** Select Topology Filters > STP Inconsistency > PVID.

The link and devices with PVID inconsistencies appear.

Viewing STP Root Inconsistency

To view STP root inconsistencies in switch clouds:

- **Step 1** Invoke Switch Cloud Map View from Topology Services.
- **Step 2** Select Topology Filters > STP Inconsistency > Root.

The link and devices with root inconsistencies are displayed.

Viewing STP Type Inconsistency

To view STP type inconsistencies in switch clouds:

- **Step 1** Invoke Switch Cloud Map View from Topology Services.
- **Step 2** Select Topology Filters > STP Inconsistency > Type.

The link and devices with type inconsistencies are displayed.

STP Filters in Switch Cloud View

Spanning Tree Filter is available in Switch Cloud Maps in Topology Services. Spanning Tree information in a switch cloud provides a better picture of the Spanning Tree than displaying Spanning Tree information in the VTP domain map.

Sometimes, the Spanning Tree root might not be part of VTP domain. The availability of STP Filters on Switch Cloud View resolves this problem. When you select the filter, it displays the list of Spanning Tree Instances that are applicable to all switches in the switch cloud, in a popup dialog box.

The following information is provided for the selected Spanning Tree Instance in the Topology Map:
- Port states (forwarding or blocking) of Switches
- Highlighted Root Bridge.
Spanning Tree

These filters are based on the Spanning Tree details of devices. When you select the filter, the Topology map lists the Spanning Tree Instances applicable to all switches in the selected switch cloud. Topology Map provides three filters under Spanning Tree:

- IEEE 802.1s Instance (Viewing Spanning Tree per IEEE 802.1s Instance)
- Cisco MIST Instance (Viewing Spanning Tree per Cisco MISTP Instances)
- VLAN (Viewing VLANs in Switch Clouds)

Viewing Spanning Tree per IEEE 802.1s Instance

You can specify the IEEE 802.1s instances by searching for the instance number. To do this:

Step 1  
From a Network Topology View, select Topology Filters &gt; Spanning Tree &gt; IEEE 802.1s Instance. The Select Instance window appears.

Step 2  
Enter the required information as described in Table 8-37.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select instance by region</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the region field, click the drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>- All Regions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Region Name</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of the region name.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists instances that match the specified criteria.</td>
<td>Select the STP instance from the list of matches.</td>
</tr>
</tbody>
</table>

To view the Spanning Tree details of an IEEE 802.1s Instance in the Network Topology View window, click Select.

Viewing Spanning Tree per Cisco MISTP Instances

You can specify the MISTP instances by searching for the instance name. To do this:

Step 1  
From a network topology view, select Topology Filters &gt; Spanning Tree &gt; Cisco MISTP Instance. The Select Instance window appears.

Step 2  
Enter the required information as described in Table 8-38.
Table 8-38  Selecting Cisco MIST Instances in Switch Clouds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select device by instance</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the instance field, click the drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>• All Instances</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Instance Name</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of the instance name.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists instances that match the specified criteria.</td>
<td>Select the instance from the list of matches.</td>
</tr>
</tbody>
</table>

To view the Spanning Tree details of an MISTP Instance in the Network Topology View window, click Select.

Viewing VLANs in Switch Clouds

You can specify VLANs by searching for the instance name.

**Step 1**
From a Network Topology View, select Topology Filters > Spanning Tree > VLAN. The Select VLAN window appears.

**Step 2**
Enter the required information as described in Table 8-39.

Table 8-39  Selecting VLANs in Switch Clouds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select VLAN</td>
<td>Select either of the following criteria:</td>
<td>To view the valid values for the VLAN field, click the drop-down arrow.</td>
</tr>
<tr>
<td></td>
<td>• VLAN Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VLAN ID</td>
<td></td>
</tr>
<tr>
<td>What</td>
<td>Enter the string</td>
<td>Use this field to narrow the number of matches by entering part or all of the VLAN name or ID.</td>
</tr>
<tr>
<td>Matches</td>
<td>Lists the VLANs that match the specified criteria.</td>
<td>Select the name or ID from the list of matches.</td>
</tr>
</tbody>
</table>

To view the Spanning Tree details of the VLAN in the Network Topology View window, click Select.
Fault Monitor

LMS Fault Monitor is a centralized browser, where you can view the information on faults, system events, and performance management events of devices in a single place.

A fault refers to a problem in the device or in the network. Examples for faults include Device Down, Link Down, and High Utilization.

An event refers to the activities or changes happening in the network. Examples for events are Config Change, user login, and user logout.

Fault Monitor collects information on faults and events from all devices in real-time and display the information for a selected group of devices. It allows you to own the faults or clear them. You can also annotate the devices.

Fault Monitor has two tabs: Device Fault Summary View and Fault View. It provides a launch point for Event Monitor, and allows you to view event forensic data collected.

While previous releases monitored alerts as well as events, the concept of alerts has been removed in this release to allow for quicker access to event information and troubleshooting tools.

These topics describe the use of Fault Monitor:

- Starting Fault Monitor
- Understanding Fault Monitor
- Using Fault Monitor
- Event Forensics
- Using Event Monitor

Starting Fault Monitor

Select Monitor > Monitoring Tools > Fault Monitor to launch Fault Monitor.

When Fault Monitor is launched for the first time, it displays the data based on all devices in LMS and their faults. After you select a group, it displays devices and faults for the selected device group.
Understanding Fault Monitor

Fault Monitor consists of three main parts:

- Group selector, which lists the following groups in LMS to provide easy access to devices:
  - System-defined groups
  - User-defined groups
  - Unreachable Devices group
  - Unmanaged Devices group
  - Suspended Devices group

**Note**
If group selector has more than 2000 nodes, it takes some time to expand the group nodes. While expanding the nodes, a stop script popup may appear. You can ignore the stop script error and view the data. To view the data, click No from the popup window if you are using IE. If you are using Firefox, click Continue. This stop script popup may occur for two or three times. Each time when the popup appears, you have to click No or Continue depending upon your browser.

- Device Fault Summary view, which contains the Devices and Faults sub-panes. Devices sub-pane provides a summary of devices selected from the group selector located on the right pane. If a device is selected, its faults are displayed in the Faults table.

- Faults view, which provides fault details. When Fault Monitor is launched for the first time, it displays the details of all devices and for the subsequent times, it displays the focused device group faults based on user selections.
Understanding the Layout of Fault Monitor and Events Displays

These topics provide details about the information in the Fault Monitor.

- **Group Selector**
- **Device Fault Summary Tab**
- **Faults Tab**
- **Window Tools Area**
- **Action Button Area on the Device Fault Summary and Fault Tabs**

**Group Selector**

The group selector shows all system and user-defined groups in LMS in a tree-based format.

The group selector pane is updated every two minutes or when user refreshes.

**Device Fault Summary Tab**

The Device Fault Summary tab contains two subpanes: Devices and Faults.

The initial display includes All Devices. After you select a group in the group selector, the Devices pane refreshes with devices belonging to that group.

The faults that correspond to the selections display in the Fault subpane.

Devices and events are sorted based on time, and not on severity. The most recent activity displays first. This pane is refreshed every 60 seconds. For an explanation of all of the items in the tabular display, see Table 9-1.

The tabular display pane is scrollable and can store up to 1,000 records. For a description of the Device Fault Summary tab, see Table 9-1.

**Table 9-1 Device Fault Summary Tab Contents**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Devices Panel</strong></td>
<td></td>
</tr>
<tr>
<td>Radio button</td>
<td>Allows you to select a device to perform device-level operations.</td>
</tr>
<tr>
<td>Severity icon</td>
<td>Fault status icon. Indicates the highest severity event on this device.</td>
</tr>
<tr>
<td>Annotation icon</td>
<td>Indicates whether annotation is added to device or not.</td>
</tr>
<tr>
<td>Annotation</td>
<td>Annotation is a convenient tool for making sure that all users see event information. You can add an annotation by clicking the Annotation button. Adding an annotation is described in Annotating an Event—Using the Fault Monitor Events Tab</td>
</tr>
<tr>
<td>Device Name</td>
<td>Device name or IP address. Displays a device details window on mouse over.</td>
</tr>
<tr>
<td>Device IP</td>
<td>IP Address of the device.</td>
</tr>
<tr>
<td>Type</td>
<td>Device type. Example: Routers, Interfaces and Modules, and Switches.</td>
</tr>
<tr>
<td>Status columns</td>
<td>Critical icon</td>
</tr>
<tr>
<td></td>
<td>Warning icon</td>
</tr>
<tr>
<td></td>
<td>Information icon</td>
</tr>
</tbody>
</table>
Understanding Fault Monitor

Faults Tab

The contents of the Fault tab in the Fault Monitor page is described in Table 9-2.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Updated Time</td>
<td>Time and date of event update (indicates activity, such as an event recurrence, event acknowledgement, the addition of a note, and so forth). Events are grouped by severity, and within severities, events with the latest change are listed first.</td>
</tr>
</tbody>
</table>

Faults Panel

<table>
<thead>
<tr>
<th>Selection box</th>
<th>Allows you to select single or multiple faults on which to take action.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity icon</td>
<td>Fault status icon. Indicates the highest severity event on this device.</td>
</tr>
<tr>
<td>Status icon</td>
<td>Indicates whether the fault is owned or yet to taken with an action.</td>
</tr>
<tr>
<td>Annotation icon</td>
<td>Indicates this fault has user notations. Only fault-level annotation is supported. Annotation is a convenient tool for making sure that all users see event information. You can add an annotation by clicking the Annotation button. Adding an annotation is described in Annotating Faults—Using the Device Fault Summary Tab.</td>
</tr>
</tbody>
</table>

Event Name      | Identifies event name. Events are sorted based on the time of the most recent event status changes.                                                                                                           |
| Device Name     | Device name or IP address. Clicking link accesses Device Details window.                                                                                                                                 |
| Component Name  | Device component name.                                                                                                                                                                                        |
| Creation Time   | Date and time event appeared.                                                                                                                                                                                |

Window Tools Area

The top-right corner of the Fault Monitor display contains available tools buttons. All buttons are described in Getting Started with Cisco Prime LAN Management Solution 4.1.
Action Button Area on the Device Fault Summary and Fault Tabs

The action buttons on the Devices Faults subpane provides you ways to respond to faults. See Using Fault Monitor for more details on how to use this.

The following icons are available in the Device Fault Summary and Fault Tabs:

- **Refresh** — Allows you to refresh the page and see the latest contents.
- **Print** — Allows you to print the device or event details.
- **Export** — Allows you to export the device or event details to a PDF or CSV file.
- **Settings** — Allows you to choose the columns you want to display and customize the view of the tabs.

### Table 3  Events Display—Command Buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Own it</td>
<td>Allows to own or re-own the faults by the users.</td>
</tr>
<tr>
<td>Clear</td>
<td>Clears the faults.</td>
</tr>
<tr>
<td>Event Monitor</td>
<td>Launches Event Monitor.</td>
</tr>
<tr>
<td>Annotate</td>
<td>User entered information acknowledging device or fault status. Available only for events.</td>
</tr>
<tr>
<td>Notify</td>
<td>Send e-mail to specified user about the selected faults.</td>
</tr>
<tr>
<td>Filter</td>
<td>Sets the filters on the selected display.</td>
</tr>
<tr>
<td>Clear Filter</td>
<td>Clears the filters set to display the selected devices.</td>
</tr>
</tbody>
</table>

Using Fault Monitor

The following topics discuss how to use Fault Monitor:

- Accessing Device and Event Details Windows from within Fault Monitor Tabs
- Viewing Device Data using Device Fault Summary Tab
- Viewing Data Using Faults Tab

Accessing Device and Event Details Windows from within Fault Monitor Tabs

You can see the device details and event details by hovering the device name and event names respectively, listed in Fault Monitor Windows.

**Accessing Device Details Windows From Fault Monitor**

You can see the device details by hovering over the device name listed in the Device Fault Summary tab for several seconds. The mouse hover popup window for Devices displays:

- Device details such as Device Name, IP Address, Device Type, OS Type, Version, and so on.
- Cross-launch points for various tools and tasks such as Device Center, CiscoView, Ping, Traceroute, Telnet/SSH, Search Communities, Open TAC Case links and so on.
Accessing Event Details Windows From Fault Monitor

From the Faults tab in Fault Monitor, you can see the details of event by hovering the events name for several seconds.

The mouse hover popup window for Events displays:

- Details such as Event Description, Device IP, Device Type, Fault Last Updated At, Component, Component Class, Component Event Code, Event Category, Event Source, and so on.
- Cross-launch points for various tools and tasks such as Fault History, Polling Parameters, Fault Threshold Settings, Forensics Data, Search Communities, Open TAC Case link and so on.

Viewing Device Data using Device Fault Summary Tab

To view device data and take action on specific device faults using the Device Fault Summary tab, use the following topics:

- Owning Faults—Using the Device Fault Summary Tab
- Clearing Events—Using the Device Fault Summary Tab
- Annotating Faults—Using the Device Fault Summary Tab
- Sending E-Mail in Response to an Event—Using the Device Fault Summary Tab

Owning Faults—Using the Device Fault Summary Tab

Acknowledging active faults signals to other users that you are aware of the fault. When you own an event, this status change is populated to all events displays.

You can also re-assign the faults assigned to other owner.

Use this procedure to own one or more device faults from the Fault Monitor tab.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From Fault Monitor, select a device from the Devices pane. The Faults sub-pane refreshes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select one or more faults in the Faults sub-pane by selecting check boxes for them.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Own it. A confirmation dialog box appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter your username.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select Annotate if you want to insert text and type the desired annotation.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Yes. The events display refreshes and the Status column displays acknowledged for the selected devices.</td>
</tr>
</tbody>
</table>

Clearing Events—Using the Device Fault Summary Tab

Clearing an event moves the event to the Cleared state. Cleared events are displayed for 20 minutes in the events display.

The event is purged from database. As a result, when the next event is raised for the same device, a new event ID is generated.
When you clear an event, this status change is populated to all events displays. Once an event is cleared, the status cannot be changed back. To get the existing state of the events for that device, you must manually delete and re-add the device to LMS. If any new event on the device recurs, the status reverts to active.

Note
The cleared event is removed from the Events display after LMS performs its normal polling and determines that the alarm has been in the cleared state for 30 minutes or longer (from the time of polling). The maximum time that a cleared event can be seen in the Events display is 60 minutes.

Use this procedure to clear one or more device events from the Fault Monitor tab.

**Step 1**
From Fault Monitor, select a device from the Devices pane.
The Faults sub-pane refreshes.

**Step 2**
Select one or more faults in the Events sub-pane by selecting check boxes for them.

**Step 3**
Click **Clear**.
A confirmation dialog box appears.

**Step 4**
Enter your initials.

**Step 5**
Click **OK**.
LMS clears the selected events and refreshes the display.

**Annotating Faults—Using the Device Fault Summary Tab**

You can annotate an event by clicking the **Annotate** button. An editable Annotation dialog box opens wherein you can enter up to 255 characters. Any number of annotations can be entered. An annotation is shown whenever other users view the event from an Event Details page.

**Step 1**
From Fault Monitor, select a device from the Devices pane.
The Faults sub-pane refreshes.

**Step 2**
Select one or more events in the Faults sub-pane by selecting check boxes for them and click **Annotate**.
The Annotation dialog box opens.

**Step 3**
Enter your text.

Text that exceeds 255 characters is truncated without warning. (If this happens, you can add another annotation.)

**Step 4**
Click **OK**.
The pane refreshes and the annotation is noted in the event rows with the clipboard annotation icon.
Sending E-Mail in Response to an Event—Using the Device Fault Summary Tab

When you click Notify in an events display, LMS opens a dialog box that you can complete to manually send an e-mail notification to multiple recipients. The e-mail notification adds the event details for the selected event. (If you want to send automatic e-mail notifications when events occur on certain devices, use Notification Services to set up an e-mail notification subscription.

Step 1 From Fault Monitor, select a device from the Devices pane.
    The Faults sub-pane refreshes.
Step 2 Select one or more events in the Events sub-pane by selecting check boxes for them.
Step 3 Click Notify.
    The Notify Events dialog box opens.
Step 4 Enter a fully qualified DNS name or IP address for an SMTP server.
Step 5 Enter your e-mail address in the From Address field.
Step 6 Enter a comma-separated list of e-mail addresses in the Recipient Address(es) field.
Step 7 Enter a subject heading in the Header field.
Step 8 (Optional) Enter your comments in the Comments field.
Step 9 Click OK.

Viewing Data Using Faults Tab

To view event data and take action on events using the Event Tab, use the following topics:

- Acknowledging an Event—Using the Fault Monitor Events Tab
- Clearing an Event—Using the Fault Monitor Events Tab
- Annotating an Event—Using the Fault Monitor Events Tab
- Sending E-Mail in Response to an Event—Using the Fault Monitor Events Tab

Acknowledging an Event—Using the Fault Monitor Events Tab

Acknowledging active events signals to other users that you are aware of the event. When you own an event, this status change is populated to all events displays.

Use this procedure to own one or more events from the Fault Monitor Events tab.

Step 1 Select one or more events from the Events tab by selecting check boxes for them.
Step 2 Click Acknowledge. A confirmation dialog box appears.
Step 3 Enter your user name.
Step 4 Select Annotate if you want to insert text and type the desired annotation.
Step 5 Click Yes. The events display refreshes and the Status column displays acknowledged for the selected devices.
Clearing an Event—Using the Fault Monitor Events Tab

Clearing an event moves the event to the Cleared state. Cleared events are displayed for 20 minutes in the events display.

The event is purged from database. As a result, when the next event is raised for the same device, a new event ID is generated.

When you clear an event, this status change is populated to all events displays. Once an event is cleared, the status cannot be changed back. To get the existing state of the events for that device, you must manually delete and re-add the device to LMS. If any new event on the device recurs, the status reverts to active.

**Note**

The cleared event is removed from the Events display after LMS performs its normal polling and determines that the alarm has been in the cleared state for 30 minutes or longer (from the time of polling). The maximum time that a cleared event can be seen in the Events display is 60 minutes.

Use this procedure to clear one or more events from the Fault Monitor Events tab.

**Step 1**
From the Fault Monitor Faults tab, select one or more events by selecting check boxes for them.

**Step 2**
Click **Clear**.

A confirmation dialog box appears.

**Step 3**
Enter your initials.

**Step 4**
Click **OK**.

LMS clears the selected events and refreshes the events display.

Annotating an Event—Using the Fault Monitor Events Tab

You can annotate an event by clicking the **Annotate** button. An editable Annotation dialog box opens; in the dialog box, you can enter up to 255 characters. Any number of annotations can be entered. An annotation is shown whenever other users view the event from Fault Monitor.

**Step 1**
From the Fault Monitor Events tab, make a selection on what event or events to annotate and click **Annotate**. The Annotation dialog box opens.

**Step 2**
Enter your text. Text that exceeds 255 characters is truncated without warning. (If this happens, you can add another annotation.)

**Step 3**
Click **OK**. The pane refreshes and the annotation is noted in the event rows with the clipboard annotation icon.

Sending E-Mail in Response to an Event—Using the Fault Monitor Events Tab

When you click **Notify** in an events display, LMS opens a dialog box that you can complete to manually send an e-mail notification to multiple recipients. The e-mail notification adds the event details for the selected event. (If you want to send automatic e-mail notifications when events occur on certain devices, use Notification Services to set up an e-mail notification subscription.)
To do so:

**Step 1** From the Fault Monitor Events tab, select an event and click **Notify**. The E-mail Notification Recipient(s) dialog box opens.

**Step 2** Enter a fully qualified DNS name or IP address for an SMTP server.

**Step 3** Enter your e-mail address in the Sender Address field.

**Step 4** Enter a comma-separated list of e-mail addresses in the Recipient Address(es) field.

**Step 5** Enter a subject heading in the Header field.

**Step 6** (Optional) Enter your comments in the Comments field.

**Step 7** Click **OK**.

### Filtering Data in Fault Monitor Tabs

You can filter the data in the Device Fault Summary View tab in Fault Monitor using the following filter criteria:

- Event Severity
- Device Name
- Device IP
- Last Updated

You can filter the data in the Fault View in Fault Monitor tab using the following filter criteria:

- Event Name
- Severity
- Status
- Last Updated — You can select either Date or Time Interval.

  If you select Date, enter a date in mm/dd/yyyy format or select a date using the Datepicker.

  If you select Time Interval, do either of the following:

  - Enter the number of days, hours, weeks, or months in the text box provided.
  
  Or

  - Select a valid period of date.

### Event Forensics

Event Forensics refer to additional information related to the specific events that are polled by LMS server. The polled data are stored on the server and you can use this for troubleshooting.

You must enable the Event Forensics collection feature on LMS server to start collecting the event forensics data. To do so, click **Admin > Collection Settings > Fault > Fault Event Forensics Configuration**.
Using Event Monitor

LMS polls for Event Forensics data for the following events only:

- Device unavailability or unresponsiveness
- Flapping
- Operationally Down

**Table 4  Event Forensics**

<table>
<thead>
<tr>
<th>Events</th>
<th>Data Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device unavailability or unresponsiveness</td>
<td>For interface or ports unresponsiveness</td>
</tr>
<tr>
<td></td>
<td>• Output of Device ping</td>
</tr>
<tr>
<td></td>
<td>• Output of Device Traceroute</td>
</tr>
<tr>
<td></td>
<td>• Latest available running configuration on the device</td>
</tr>
<tr>
<td></td>
<td>For SNMP unresponsiveness</td>
</tr>
<tr>
<td></td>
<td>• Shows option to do credential sets</td>
</tr>
<tr>
<td></td>
<td>• Shows option to do SNMP tests</td>
</tr>
<tr>
<td>Flapping</td>
<td>• Shows interface CLI</td>
</tr>
<tr>
<td></td>
<td>• Shows running config of the interface</td>
</tr>
<tr>
<td></td>
<td>• Errors and discards on the interface</td>
</tr>
<tr>
<td>Operationally Down</td>
<td>For events on Operationally Down modules:</td>
</tr>
<tr>
<td></td>
<td>• Module type</td>
</tr>
<tr>
<td></td>
<td>• Serial number of the module</td>
</tr>
<tr>
<td></td>
<td>• Vendor type of the module</td>
</tr>
<tr>
<td></td>
<td>• Information on the module inventory</td>
</tr>
<tr>
<td></td>
<td>For events on Operationally Down interfaces:</td>
</tr>
<tr>
<td></td>
<td>• Shows the interface details</td>
</tr>
<tr>
<td></td>
<td>• Running config of the interface</td>
</tr>
<tr>
<td></td>
<td>• CDP neighbor connected to the interface</td>
</tr>
</tbody>
</table>

You can see the event forensics results when you move your mouse over the Annotations in the Faults table of Fault Monitor Device Faults Summary view tab.

**Using Event Monitor**

Event Monitor is a centralized place where you can view the event details of all devices and device groups. Event Monitor can the fault history, syslog and system events that are generated in:

- Last one hour
- Last two hours
- Last four hours
- Last eight hours
These topics describe how to use Event Monitor:

- Starting Event Monitor
- Understanding Event Monitor

## Starting Event Monitor

You can launch Event Monitor from one of the following ways:

- From the menu, select **Monitor > Monitoring Tools > Event Monitor**
- From the Fault Monitor Device Fault Summary View tab, select the Event Monitor action button from the Devices or Faults table
- From the Fault Monitor Faults View tab, select the Event Monitor action button from the Faults table

When Event Monitor is launched for the first time, it displays the data based on all devices in LMS and their events. After you select a device, it displays the events specific to the selected groups.

## Understanding Event Monitor

Event Monitor consists of four main parts:

- Device selector which lists the devices from various system-defined and user-defined groups of LMS to provide easy access to devices.

  **Note** If device selector has more than 2000 nodes, it takes some time to expand the nodes. The loading image may not get displayed while expanding the nodes. You can ignore the stop script error thrown by the browser while loading the nodes and select the No option to continue loading.

- Fault History view which provides a list of history events of all devices selected from the device selector located at the right pane.
- Syslogs view which provides a list of syslog events of all devices selected from the device selector located at the right pane.
- Systems view which provides a list of system events generated from LMS servers.

This section contains the information about:

- Understanding the Layout of Event Monitor Displays
- Accessing Event Details Windows from within Event Monitor Tabs
Understanding the Layout of Event Monitor Displays

These topics provide details about the information in the Event Monitor.

- **Device Selector**
- **Fault History Tab**
- **Syslogs Tab**
- **System Tab**
- **Window Tools Area**
- **Action Button Area on the Event Monitor Tabs**

**Device Selector**

The device selector shows all devices belonging to system and user-defined groups of LMS server in a tree-based format.

The device selector pane is updated every two minutes or when user refreshed. It shows up to 500 nodes of display by default.

**Note**

If the device selector has more than 2000 nodes, it takes some time to expand the group nodes. While expanding the nodes, a stop script popup may appear. You can ignore the stop script error and view the data. To view the data, click No from the popup window if you are using IE. If you are using Firefox, click Continue. This stop script popup may occur for two or three times. Each time when the popup appears, you have to click No or Continue depending upon your browser.

You can also do a simple search or advanced search of devices in the device selector. See *Administration of Cisco Prime LAN Management Solution 4.1* for information how to perform a simple search or an advanced search of devices.

**Fault History Tab**

This is the default page that you can see as soon as Event Monitor is launched. This tab displays the latest 100 events from the Fault History database.

A refresh icon is provided to view the contents after refreshing the tab manually.

A settings icon is also provided which allows you to choose to display the columns you want and customize the view of the Fault History tab.

For a description of the contents of the Fault tables in the Fault History tab, see Table 9-5.

### Table 9-5 Fault History Tab Contents

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio button</td>
<td>Allows you to select a fault record and perform operations.</td>
</tr>
<tr>
<td>Status icon</td>
<td>Indicates whether the fault is owned or yet to be taken with an action.</td>
</tr>
<tr>
<td>Event Name</td>
<td>Identifies event name. Events are sorted based on the time of the most recent event status changes.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Displays Device name or IP address. Accessing the link provided for Device Name or IP address launches the Device Details window.</td>
</tr>
<tr>
<td>Component Name</td>
<td>Device component name.</td>
</tr>
<tr>
<td>Last Updated Time</td>
<td>Date and time when the event was last updated.</td>
</tr>
</tbody>
</table>
The contents of the Syslogs tab in the Event Monitor page is described in Table 9-6.

A settings icon is also provided which allows you to choose the columns you want to display and customize the view of the Syslogs tab.

### Table 9-5 Fault History Tab Contents (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owned By</td>
<td>User owning the faults</td>
</tr>
</tbody>
</table>

### Table 9-6 Syslogs Tab Contents

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device name</td>
<td>Name or IP Address of the device generating the Syslog message.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Time when the Syslog message was generated. The format used by timestamp is:</td>
</tr>
<tr>
<td></td>
<td><em>mmm dd yyyy hh:mm:ss</em></td>
</tr>
<tr>
<td></td>
<td>where: <em>mmm</em> represents month</td>
</tr>
<tr>
<td></td>
<td><em>dd</em> represents date</td>
</tr>
<tr>
<td></td>
<td><em>yyyy</em> represents year</td>
</tr>
<tr>
<td></td>
<td><em>hh</em> represents hour</td>
</tr>
<tr>
<td></td>
<td><em>mm</em> represents minute</td>
</tr>
<tr>
<td></td>
<td><em>ss</em> represents second</td>
</tr>
<tr>
<td>Example</td>
<td><em>Nov 18 2008 12:24:36</em></td>
</tr>
<tr>
<td>Facility</td>
<td>Displays the facility or sub-facility codes. A facility is a hardware device,</td>
</tr>
<tr>
<td></td>
<td>a protocol, or a module of the system software. See the section, System</td>
</tr>
<tr>
<td></td>
<td>Error Messages in the Cisco IOS Reference manual, for a predefined list of</td>
</tr>
<tr>
<td></td>
<td>system facility codes.</td>
</tr>
<tr>
<td></td>
<td>A sub-facility is the sub-facility in the device that generates the Syslog</td>
</tr>
<tr>
<td></td>
<td>message.</td>
</tr>
<tr>
<td>Severity</td>
<td>Displays the message severity levels. Representations for the severity codes are:</td>
</tr>
<tr>
<td></td>
<td>0—Emergencies</td>
</tr>
<tr>
<td></td>
<td>1—Alerts</td>
</tr>
<tr>
<td></td>
<td>2—Critical</td>
</tr>
<tr>
<td></td>
<td>3—Errors</td>
</tr>
<tr>
<td></td>
<td>4—Warnings</td>
</tr>
<tr>
<td></td>
<td>5—Notifications</td>
</tr>
<tr>
<td></td>
<td>6—Informational</td>
</tr>
</tbody>
</table>
Table 9-6  Syslogs Tab Contents (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mnemonic</td>
<td>Codes that uniquely identifies an error message.</td>
</tr>
<tr>
<td>Example:</td>
<td>TEST_RUNNING</td>
</tr>
<tr>
<td></td>
<td>TEST_OK</td>
</tr>
<tr>
<td>Description</td>
<td>Description of each Syslog message.</td>
</tr>
<tr>
<td>Details</td>
<td>Other details for each Syslog message.</td>
</tr>
</tbody>
</table>

**System Tab**
The contents of the System tab in the Event Monitor page is described in Table 9-7. A settings icon is also provided which allows you to choose the columns you want to display and customize the view of the System tab.

Table 9-7  System Tab Contents

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio button</td>
<td>Allows you to select a record.</td>
</tr>
<tr>
<td>Severity icon</td>
<td>Fault status icon. Indicates the highest severity event on this device.</td>
</tr>
<tr>
<td>Status icon</td>
<td>Indicates whether the event is owned or yet to be taken with an action.</td>
</tr>
<tr>
<td>Event Name</td>
<td>Identifies event name. Events are sorted based on the time of the most recent event status changes.</td>
</tr>
<tr>
<td>LMS Server Name</td>
<td>LMS Server name or IP address.</td>
</tr>
<tr>
<td>Creation Time</td>
<td>Date and time event appeared.</td>
</tr>
</tbody>
</table>

**Note**
If you have more than 50 devices on your server and later installed LMS 50 devices license, DEVICES_AUTO_STATE_CHANGE_TO_SUSPENDED system event is triggered. This signifies that additional managed devices will be automatically moved to the Suspended state. See the *Installing and Migrating to Cisco Prime LAN Management Solution 4.1* document for the procedure to manage and unmanage the devices.

Window Tools Area
The top-right corner of the Fault Monitor display contains available tools buttons. All buttons are described in *Getting Started with Cisco Prime LAN Management Solution 4.1*. 
Action Button Area on the Event Monitor Tabs

The action buttons on the Event Monitor tabs provides you ways to respond to events.

Table 9-8 Event Monitor Tabs—Command Buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault History Tab</td>
<td></td>
</tr>
<tr>
<td>Report</td>
<td>Launches the Fault History report. See Reports Management With Cisco Prime LAN Management Solution 4.1 for details on this report.</td>
</tr>
<tr>
<td>Filter</td>
<td>Sets the filters on the selected display. The filter criteria that could be used are:</td>
</tr>
<tr>
<td></td>
<td>• Event Name</td>
</tr>
<tr>
<td></td>
<td>• Status</td>
</tr>
<tr>
<td></td>
<td>• Last Updated— You can either select Today or Time Interval. If you select Time Interval, you can select the duration or a valid period of date.</td>
</tr>
<tr>
<td></td>
<td>• Owned By</td>
</tr>
<tr>
<td>Clear Filter</td>
<td>Clears the filters set to display the selected devices.</td>
</tr>
<tr>
<td>Syslog Tab</td>
<td></td>
</tr>
<tr>
<td>Report</td>
<td>Launches the Syslog report. See Reports Management With Cisco Prime LAN Management Solution 4.1 for details on this report.</td>
</tr>
</tbody>
</table>
### Table 9-8  
**Event Monitor Tabs—Command Buttons (continued)**

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Sets the filters on the selected display.</td>
</tr>
<tr>
<td></td>
<td>The filter criteria that could be used are:</td>
</tr>
<tr>
<td></td>
<td>• EventSeverity</td>
</tr>
<tr>
<td></td>
<td>• Facility[Sub-Facility]</td>
</tr>
<tr>
<td></td>
<td>• Mnemonic</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Timestamp — You can either select Today or Time Interval.</td>
</tr>
<tr>
<td></td>
<td>If you select Time Interval, you can select the duration or a valid</td>
</tr>
<tr>
<td></td>
<td>period of date.</td>
</tr>
<tr>
<td></td>
<td>The duration could be:</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Hour</td>
</tr>
<tr>
<td></td>
<td>• Last 2 Hours</td>
</tr>
<tr>
<td></td>
<td>• Last 4 Hours</td>
</tr>
<tr>
<td></td>
<td>• Last 8 Hours</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Day</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Month</td>
</tr>
<tr>
<td>Clear Filter</td>
<td>Clears the filters set to display the selected devices.</td>
</tr>
</tbody>
</table>

#### System Tab

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report</td>
<td>Launches the System Events report.</td>
</tr>
<tr>
<td></td>
<td>If there are more records, the report can display first 2000 records</td>
</tr>
<tr>
<td></td>
<td>only.</td>
</tr>
<tr>
<td></td>
<td>See <em>Reports Management With Cisco Prime LAN Management Solution 4.1</em></td>
</tr>
<tr>
<td></td>
<td>for details on this report.</td>
</tr>
<tr>
<td>Filter</td>
<td>Sets the filters on the selected display.</td>
</tr>
<tr>
<td></td>
<td>The filter criteria that could be used are:</td>
</tr>
<tr>
<td></td>
<td>• Event Name</td>
</tr>
<tr>
<td></td>
<td>• Severity</td>
</tr>
<tr>
<td></td>
<td>• Status</td>
</tr>
<tr>
<td></td>
<td>• Last Updated — You can either select Today or Time Interval.</td>
</tr>
<tr>
<td></td>
<td>If you select Time Interval, you can select the duration or a valid</td>
</tr>
<tr>
<td></td>
<td>period of date.</td>
</tr>
<tr>
<td></td>
<td>The duration could be:</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Day</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Hour</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Month</td>
</tr>
<tr>
<td></td>
<td>• Last 2 Hours</td>
</tr>
<tr>
<td></td>
<td>• Last 4 Hours</td>
</tr>
<tr>
<td></td>
<td>• Last 8 Hours</td>
</tr>
<tr>
<td>Clear Filter</td>
<td>Clears the filters set to display the selected devices.</td>
</tr>
</tbody>
</table>
Accessing Event Details Windows from within Event Monitor Tabs

You can see the event details by hovering the event names listed in Event Monitor Windows for several seconds.

The mouse hover popup window for Events displays the details such as Event Description, Device IP, Device Type, Fault Last Updated At, Component, Component Class, Component Event Code, Event Category, Event Source, and so on.
Using NetShow Commands

Network show (NetShow) commands represent a set of read-only commands. These are primarily, show commands that you can run on devices that are managed in LMS.

You can specify the commands that you want to group together and then run these commands on one or many devices. The output is displayed in a browser window.

NetShow has the following features:

- Network Administrators can assign Command Sets to other users.
- Network Administrators and Network Operators (if permitted) can execute the custom commands. This allows them to run a command against multiple devices.
- Support for standard and non-standard Cisco devices.
- Simplified new device support.
- No device limit.
- Integration with the Output Interpreter tool.

LMS ships with system-defined NetShow Command Sets. You cannot edit or delete any of these Command Sets. See System-Defined Command Sets for the list of system-defined Command Sets in LMS.

You can run NetShow commands either from the Graphical User Interface (GUI) or from the Command Line Interface (CLI). NetShow allows you to add system-defined as well as adhoc commands within Command Sets and run them.

You must have the required privileges to perform these functions. See Viewing the Permission Report for the tasks that a user in a particular role can perform.

The major features of NetShow are:

- **NetShow Job Browser**
  The NetShow job browser allows you to create, edit, copy, retry, stop, or delete NetShow jobs and view the details of the jobs. You can run a job immediately or schedule it to run at a specified time, once, or periodically.

- **Archiving NetShow Job Output**
  You can access the stored output that is created from a NetShow job through the Output Archive.
Working With NetShow Jobs

The NetShow Jobs feature allows the user with appropriate privileges to perform tasks such as viewing job details, creating jobs, editing jobs, copying jobs, retrying failed jobs, stopping jobs, and deleting jobs.

For a list of NetShow Job tasks and the required user roles, use the Permission Report function (Reports > System > Users > Permission). See Viewing the Permission Report for more details.

Viewing the Permission Report

The Permission Report displays information on roles and tasks associated with the roles. It specifies the tasks that a user in a particular role can perform.

To use Cisco Prime LMS, you must have a valid login, which is a combination of a username and a password.

When you are assigned a username and password, you are also assigned to one or more of these roles:

- Help Desk (default role for all users) — Can access network status information only. Can access persisted data on the system but cannot perform any action on a device or schedule a job which will reach the network.
- Approver — Can approve all tasks.
- Network Operator — Can perform all Help Desk tasks. Can perform tasks related to network data collection but not any task that requires write access on the network.
- Network Administrator — Can perform all Network Operator tasks. Can perform tasks that result in a network configuration change.
- System Administrator — Can perform all Cisco Prime LMS system administration tasks.
These roles determine which Cisco Prime LMS applications, tools, and product features you are allowed to access.

Roles are not set up hierarchically, with each role including all the privileges of the corresponding role. Instead, these roles provide access privileges based on user needs.

To view the roles and corresponding tasks that these roles can perform in NetShow:

**Step 1** Select **Reports > System > Users > Permission > Generate Report.**

The Permission Report appears.

**Step 2** Check the Permission Report to verify which of the NetShow tasks each user role can perform.

The following table lists the NetShow tasks that each user role can perform.

<table>
<thead>
<tr>
<th>Task Name</th>
<th>System Administrator</th>
<th>Network Administrator</th>
<th>Network Operator</th>
<th>Approver</th>
<th>Help Desk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign Command Sets to Users</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create, Edit, Cancel, Delete Jobs</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create, Edit, Delete Command Sets</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Job Browser</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View Command Sets</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

By default, System-defined Command Sets are assigned to Network Administrators and Network Operators.

Only Network Administrators can assign Command Sets to Network Operators. They can also view Command Sets created by all users.

Network Operators can create and view Command Sets for themselves. These Command Sets will be automatically assigned to them. However, they cannot view Command Sets created by other Network Operators.

**NetShow Job Browser**

The NetShow Job Browser enables you to view the details of all NetShow Jobs. The job details that you can view are:

- Job ID
- Job status
- Job description
- Job owner
- Time the job is scheduled to run at
- Time the job completes
- Schedule type
To use the NetShow Job Browser:

**Step 1** Select **Monitor > Troubleshooting Tools > NetShow > NetShow Jobs**.

The NetShow Job Browser appears.

You can filter the jobs by any specified criteria using the Filter by drop-down list.

**Step 2** Select your criteria and click **Filter**.

The fields in the NetShow Job Browser are:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique ID of the job. Click the hyperlink to view the Job details. For periodic jobs, the Job IDs are in the number.x format, which stands for the number of instances of that job. For example, 1003.3 indicates that the Job ID is 1003 and it is the third instance of that job.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the job—Scheduled, Successful, Failed, Cancelled, Running, Missed Start, Rejected, Approved, Waiting for Approval. The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, if the status displays Failed(5), then the count of devices that had failed amounts to 5. This count of failed devices is not displayed for jobs restored from LMS or lesser versions.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the job.</td>
</tr>
<tr>
<td>Owner</td>
<td>Username of the job creator.</td>
</tr>
<tr>
<td>Scheduled At</td>
<td>Date and time at which the job was scheduled.</td>
</tr>
<tr>
<td>Completed At</td>
<td>Date and time at which the job was completed.</td>
</tr>
<tr>
<td>Schedule Type</td>
<td>Type of job schedule—Immediate, Once, 6-Hourly, 12-Hourly, Daily, Weekly, Monthly, Last Day of the Month. For periodic jobs, the subsequent instances will run only after the earlier instance of the job has completed. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10:00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.</td>
</tr>
<tr>
<td>Refresh (Icon)</td>
<td>Click the icon to refresh the NetShow job browser.</td>
</tr>
</tbody>
</table>

The NetShow Job Browser allows you to perform the following tasks:

- Viewing Job Details
- Masking Credentials
- Creating Jobs
• Editing Jobs
• Copying Jobs
• Retrying Jobs
• Stopping Jobs
• Deleting Jobs

Viewing Job Details

From the NetShow Job Browser, you can select a job and view its details. To view the Job Details:

Step 1
Select Monitor > Troubleshooting Tools > NetShow > NetShow Jobs. The NetShow Job Browser appears.

Step 2
Click the Job ID hyperlink of the job whose details you want to see. The NetShow Job Details pop-up appears, displaying the day, date and time details in the header at the top of the page. The Job ID and the Status appear in the header of the Job Result.

By default, the NetShow Job Details page appears with the Job Details list tree in the left pane and the Work Order, in the right pane.

The Job Details list tree contains the following:
• Job Summary—Displays the summary of the job.
• Device Details—Displays the status of the devices.
• Work Order—Displays the work order of the job.

The following table describes the Job Details page.

<table>
<thead>
<tr>
<th>Page/Folder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Details</td>
<td>Click to display summary of completed job:</td>
</tr>
<tr>
<td>Job Summary</td>
<td>• Deploy Summary:</td>
</tr>
<tr>
<td></td>
<td>- Status</td>
</tr>
<tr>
<td></td>
<td>- Start Time</td>
</tr>
<tr>
<td></td>
<td>- End Time</td>
</tr>
<tr>
<td></td>
<td>• Job Messages</td>
</tr>
<tr>
<td></td>
<td>- Pre-job Execution</td>
</tr>
<tr>
<td></td>
<td>- Post-job Execution</td>
</tr>
<tr>
<td></td>
<td>• Device Update</td>
</tr>
<tr>
<td></td>
<td>- Successful</td>
</tr>
<tr>
<td></td>
<td>- Failed</td>
</tr>
<tr>
<td></td>
<td>- Not Attempted</td>
</tr>
<tr>
<td></td>
<td>- Pending</td>
</tr>
</tbody>
</table>
### NetShow Job Browser

<table>
<thead>
<tr>
<th>Page/Folder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Details</td>
<td>Contains detailed job results for each device in a table:</td>
</tr>
<tr>
<td></td>
<td>- Device—List of devices on which the job ran.</td>
</tr>
<tr>
<td></td>
<td>- Status—Status of the device deployment (success or failure.)</td>
</tr>
<tr>
<td></td>
<td>- Protocol Used—Protocol used for the device.</td>
</tr>
<tr>
<td></td>
<td>- Message</td>
</tr>
<tr>
<td></td>
<td>- If the job failed on the device, the reason for failure appears.</td>
</tr>
<tr>
<td></td>
<td>- If the job succeeded on that device, the message Deploy Successful appears.</td>
</tr>
<tr>
<td></td>
<td>You can filter the devices by selecting a status and clicking <strong>Filter</strong>.</td>
</tr>
<tr>
<td></td>
<td>This page displays the number of rows you have set for display in the Rows per page field. You can increase the rows up to 500 on each page. You can navigate between the pages of the report using the navigation icons at the right bottom of this table.</td>
</tr>
<tr>
<td></td>
<td>Click the device name link to view the details of command sets and commands on the device. Go to <strong>Step 3</strong> for details.</td>
</tr>
<tr>
<td></td>
<td>You can view the output of all the commands for all the devices by clicking the <strong>Print</strong> button on the top right hand corner of the NetShow Job Details Page.</td>
</tr>
<tr>
<td>Pending Devices</td>
<td>Displays the list of devices that are awaiting command deployment.</td>
</tr>
<tr>
<td>Not Attempted Devices</td>
<td>Displays the list of devices on which the job has not attempted to deploy commands.</td>
</tr>
<tr>
<td>Work Order</td>
<td>Displays the Job Work Order. It contains the same information as the work order that appeared when the job was created. For retried jobs, job definitions are not updated. For such jobs the original job definitions are retained. See <a href="#">A sample Job Work Order is:</a> for details.</td>
</tr>
</tbody>
</table>

You can click the page icon in the left pane to get the corresponding results in the right pane.

**Step 3**

Click the device name link in the Device Details table.

The NetShow Device Details pop-up page appears with the device name and commands in the left pane and the commands output in the right pane.

By default, the command output is a consolidated one for all the listed commands.

To convert the output into a printer-friendly format click the **Printer** button.

A printer-friendly format of the consolidated output for all commands appears.

**Step 4**

Select a command from the Device list tree in the left pane and click **Analyze Output** to analyze the output of the command.

You can mask the credentials shown in the output of `show` commands. See [Masking Credentials](#) for more details on masking credentials and [Viewing and Analyzing NetShow Output](#) for more details on viewing and analyzing NetShow Output.

The Cisco.com and Proxy Server Credential Profile dialog box appears.
Step 5 Enter your Cisco.com username and password in the Cisco.com and Proxy Server Credential Profile dialog box
   If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.
   You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server
   hostname/IP and port are configured in Admin > System > Cisco.com Settings > Proxy Server Setup

Step 6 Click OK after entering the credential information.
   The credentials that you enter here will be used for the entire session.
   The Show Commands Output Interpreter Viewer appears, displaying the Report Name, date and time
details in the header at the top of the report.
   To convert the output into a printer-friendly format click the Printer button.
   A printer-friendly format of the output of the selected command appears.

Masking Credentials

You can mask the credentials shown in the output of show commands. If you want to mask the credentials
of a particular command, you must specify the command in the
NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\config\netshow\NSCre
dCmds.properties file.
   In this file you can specify all the commands whose output should be processed to mask the credentials.
   We recommend that you enter the complete command in the file. For example, you must enter show
   running-config, not
   show run. This file contains some default commands like show running-config.

Creating Jobs

From the NetShow Job Browser, you can create new jobs to run command sets. You can create immediate
as well as scheduled jobs.
   To create a new job from the NetShow Job Browser:

Step 1 Select Monitor > Troubleshooting Tools > NetShow > NetShow Jobs.
   The NetShow Job Browser appears.
Step 2 Click Create in the NetShow Job Browser.
   The Select Devices and Command Sets window appears.
Step 3 Select the device or Device Categories from the Device Selector pane in the Select Devices and
   Command Sets window.
Step 4 Select the Command Set from the Command Set List pane in the Select Devices and Command Sets
   window.
Step 5  Enter the custom commands in the Custom Commands text box.  
You can enter multiple commands; separate these commands by commas.  
The Custom Commands text box will be enabled only if you have custom commands execution privilege.  
See Assigning Custom Command Execution Privilege for more details on assigning custom command execution privilege.

Step 6  Click Next.  
The Set Schedule Options dialog box appears.

Step 7  Enter the following information in the Set Schedule Options dialog box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Run Type   | The run type of the job. The Run Types could be any or all of these, depending on the type of the job:  
• Immediate—Runs the job immediately.  
• Once—Once at the specified date and time.  
• 6-hourly—Every 6 hours, starting from the specified time.  
• 12-hourly—Every 12 hours, starting from the specified time.  
• Daily—Daily at the specified time.  
• Weekly—Weekly on the day of the week and at the specified time.  
• Monthly—Monthly on the day of the month and at the specified time.  
• Last day of Month—On the last day of the month at the specified time.  
The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete.  
For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10:00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3. |
| Date       | Scheduled date and time of the job. |
| **Job Information** |              |
| Job Description | Enter a description for the job. This is mandatory. You can enter only alphanumeric characters. |
| E-mail      | Enter the e-mail addresses to which the job sends messages at the beginning and at the end of the job.  
You can enter multiple e-mail addresses; separate these addresses by commas.  
Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences).  
We recommend that you configure the LMS Server E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS Server E-mail ID as the sender's address. |
| Comments    | Enter your comments for the job. Comments appear in the Job Work Order. |
| **Job Options** |         |
Chapter 10  Using NetShow Commands

NetShow Job Browser

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable Job Password   | • If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) enter the device login user name and password and Device Enable password.  
  • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) either:  
    - Enter the device login user name and password and Device Enable password.  
      The credentials are for contacting the device and not the Device Credential Repository credentials.  
    Or  
    - Disable the Job Password option in the Set Schedule Options dialog box. |
| Execution             | Specify the order in which the job should run on the devices.  
  • Parallel—Allows the job to run on multiple (up to five) devices at the same time.  
  • Sequential—Allows the job to run on only one device at a time. |
| Maker Comments        | This field appears if you have enabled Job Approval Policies for NetShow. Enter the Maker Comments. See Setting Up Job Approval for more details on enabling Job Approval Policies. |
| Maker E-mail          | This field appears if you have enabled Job Approval Policies for NetShow. Enter the Maker E-mail address. This is mandatory. See Setting Up Job Approval for more details on enabling Job Approval Policies. |

**Step 8**  Click Next.

The View Job Work Order page appears with the Job Work Order.

The Job Work Order contains general information on the job and on the:

• Job policies.
• Job approval details (if you have enabled job approval).
• Device details.
• Command Sets and the commands to be executed.

**Step 9**  Click Finish after you review the details of your job in the Job Work Order.

A message appears, Job ID created successfully.

The newly created job appears in the NetShow Job Browser.

If your job failed and you want to run the same job, click Retry and perform steps 7 through 9 above.
A sample Job Work Order is:

Work Order
Name: NetShow Job Work Order
Summary: General Info

---------------------------------------------
Job Id: 1018
Owner: admin
Description: cli scheduled
Schedule Type: Run Once
Schedule Time: Sat Mar 19 00:00:00 IST 2005

---------------------------------------------
Job Policies

E-mail Notification: Disabled
Execution Policy: Parallel
Job Password: Disabled

---------------------------------------------
Job Approval Details

Job Approval: Disabled

---------------------------------------------
Device Details

Device: 10.76.38.14
Applicable Commands:
Command Set Name: Show System Info
show version
show flash
show logging

ADHOC Commands
sh ver

---------------------------------------------
Editing Jobs

You can select a job and edit the job properties from the NetShow Job Browser. You can edit only the scheduled jobs.

You can change device and command set selection as required and re-submit the job. In such cases the Job ID will remain the same.

To edit a job from the NetShow Job Browser:

Step 1 Select Monitor > Troubleshooting Tools > NetShow > NetShow Jobs.
The NetShow Job Browser appears with a list of all jobs.

Step 2 Select a scheduled job and click Edit in the NetShow Job Browser.
The Select Devices and Command Sets window appears with the current settings.

Step 3 Select the device or Device Categories from the Device Selector pane in the Select Devices and Command Sets window.

Step 4 Select the Command Set from the Command Set List pane in the Select Devices and Command Sets window.

Step 5 Enter the custom commands in the Custom Commands text box.
You can enter multiple commands. Separate these commands by commas.
The Custom Commands text box will be enabled only if you have custom commands execution privilege.
See Assigning Custom Command Execution Privilege for more details on assigning custom command execution privilege.

Step 6 Click Next.
The Set Schedule Options dialog box appears.

Step 7 Enter the following information in the Set Schedule Options dialog box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>The run type of the job. The Run Types could be any or all of these, depending on the type of the job:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs the job immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Once at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>• 6-hourly—Every 6 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>• 12-hourly—Every 12 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Daily—Daily at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly—Weekly on the day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Monthly—Monthly on the day of the month and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Last day of Month—On the last day of the month at the specified time.</td>
</tr>
</tbody>
</table>

The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete.

For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10:00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
NetShow Job Browser

Chapter 10 Using NetShow Commands

Step 8 Click Next.

The View Job Work Order page appears with the Job Work Order.

The Job Work Order contains general information on the job and on the:

- Job policies.
- Job approval details (if you have enabled job approval).
- Device details.
- Command Sets and the commands to be executed.
Step 9  Click **Finish** after you review the details of your job in the Job Work Order.
A message appears, **Job ID edited successfully.**
The edited job appears in the NetShow Job Browser. This job retains the original Job ID.
See **A sample Job Work Order is:** for details.

---

**Copying Jobs**

From the Netshow Job Browser, you can select a job and create a copy of that job. You can either edit the job details or submit the same job. If you copy a job, it creates a new job with the current administrative settings.

To copy a job from the NetShow Job Browser:

**Step 1**  Select **Monitor > Troubleshooting Tools > NetShow > NetShow Jobs.**
The NetShow Job Browser appears with a list of all jobs.

**Step 2**  Select the job you want to create a copy and click **Copy.**
The Select Devices and Command Sets window appears with all your selections for the job that you are copying.

**Step 3**  Click **Next.**
The Set Schedule Options dialog box appears.

**Step 4**  Click **Next.**
The View Job Work Order dialog box appears with the Job Work Order.

**Step 5**  Click **Finish.**
A message appears, **Job ID created successfully.**
The newly created job with the copied job details appears in the NetShow Job Browser.

---

**Stopping Jobs**

This topic captures procedures for stopping and retrying jobs. From the NetShow Job Browser:

- You can select jobs that are not yet executed or jobs that are currently running, and stop them. You can select only one job at a time and stop it.
- You can select failed jobs and retry them (see **Retrying Jobs**).

When you use this feature to stop a job, the job status changes to the Cancelled state.

To stop a job from the NetShow Job Browser:

**Step 1**  Select **Monitor > Troubleshooting Tools > NetShow > NetShow Jobs.**
The NetShow Job Browser appears with a detailed list of all jobs.
Step 2 Select the job you want to stop and click Stop.
A message appears, The selected job will be stopped.

Step 3 Either:
- Click OK to confirm.
Or
- Click Cancel to prevent the job from stopping.
If you have selected a periodic job, a message appears, Do you want to stop all the instances?

Step 4 Either:
- Click OK to stop all instances of the job.
Or
- Click Cancel to stop only one instance of the job.
If you confirm stopping the job, a message appears, Job ID is being stopped. It may take a few seconds.

Step 5 Click OK.
The status of the job appears as Cancelled in the NetShow Job Browser.

Retrying Jobs

From the Netshow Job Browser, you can select a failed job and retry that job. You can only retry non-periodic jobs.

To retry a failed job from the NetShow Job Browser:

Step 1 Select Monitor > Troubleshooting Tools > NetShow > NetShow Jobs.
The NetShow Job Browser appears with a list of all jobs.

Step 2 Select the job you want to retry and click Retry.
The Set Schedule Options dialog box appears.
You can either retain or change the Schedule Options.

Step 3 Click Next.
The View Job Work Order dialog box appears with the Job Work Order.

Step 4 Click Finish.
A message appears, Job ID submitted for retry successfully.
The job appears in the NetShow Job Browser with the same ID.
Deleting Jobs

You can delete all jobs from the Job Browser except jobs that are already running. To delete a running job, you must first stop the job.

You can also delete individual instances of periodic jobs. However, if you try to delete the scheduled instance of the periodic job, you are prompted to confirm whether you want to delete all the instances of the job. You can delete multiple jobs at the same time.

Even if you delete a job that has completed, you can view the command output in the output archive unless you remove this archive.

To delete a job from the NetShow Job Browser:

Step 1  Select Monitor > Troubleshooting Tools > NetShow > NetShow Jobs.
        The NetShow Job Browser appears with a detailed list of all jobs.

Step 2  Select a job or a number of jobs that you want to delete and click Delete in the NetShow Job Browser.
        A message appears, Selected job(s) will be deleted.

Step 3  Either:
          • Click OK to confirm.
          Or
          • Click Cancel to prevent the jobs from deleting.

If you have selected periodic jobs, a message appears, If you delete periodic jobs or instances of a periodic job that are yet to be run, the jobs will no longer run, nor will they be scheduled to be run again. You must then recreate the deleted jobs. Do you want to continue?

Step 4  Either:
          • Click OK to delete all instances of the jobs.
          Or
          • Click Cancel to cancel deleting the jobs.

If you confirm deleting the job, a message appears, Job(s) deleted successfully.

Archiving NetShow Job Output

The Output Archive feature in NetShow helps you archive and access the stored output that is created from a NetShow job. The show command output is archived only if the jobs are executed completely.

The Output Archive Analyzer feature reads show command outputs, interprets the data and generates a report. The Output Interpreter tool in Cisco.com performs the show command analysis.

NetShow sends selected output to Cisco.com, gets the analyzed details and displays these details in a separate window. The final output is a complete analysis of the command output. The errors and potential problems are highlighted in the report.

You can analyze the complete output of a particular command on a device. The command output displays the analyzed output generated only for a selected command. You can generate a printer-friendly format of the command output.
This section explains:

- Viewing and Analyzing NetShow Output
- Deleting Output Archive

**Viewing and Analyzing NetShow Output**

You can view and analyze a NetShow Job Output.

To view and analyze the NetShow Output:

**Step 1** Select **Monitor > Troubleshooting Tools > NetShow > Output Archive**.

The Output Archive page appears.

You can use the Filter option to filter the archives based on All or Job ID or Description as the criteria. You can provide a search string in the text area and click **Filter** to filter the archives based on the search criteria.

**Step 2** Select an Archive ID and click **View**.

The NetShow Archive Details pop-up appears, displaying the day, date, and time details in the header at the top of the page. The Archive ID appears in the header of the Archive Result.

The Archive Details pop-up has two panes. The Archive Details appear in a tree format with Device Details and Deployed Devices in the left pane. The list of devices appears in a table in the right pane.

The following table describes the Archive Details page.

<table>
<thead>
<tr>
<th>Folder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive Details</td>
<td>Expand the list tree to view the Device Details and Deployed Devices.</td>
</tr>
<tr>
<td>Device Details</td>
<td>Expand the list tree to view the Deployed Devices.</td>
</tr>
<tr>
<td>Deployed Devices</td>
<td>Contains detailed job results for each device in a table:</td>
</tr>
<tr>
<td></td>
<td>- Device—List of devices on which the job ran.</td>
</tr>
<tr>
<td></td>
<td>- Status—Status of the device deployment (success or failure.)</td>
</tr>
<tr>
<td></td>
<td>- Protocol Used—Protocol used for the device.</td>
</tr>
<tr>
<td></td>
<td>- Message</td>
</tr>
<tr>
<td></td>
<td>- If the job failed on the device, the reason for failure appears.</td>
</tr>
<tr>
<td></td>
<td>- If the job succeeded on that device, the message <strong>Deploy Successful</strong> appears.</td>
</tr>
</tbody>
</table>

This page displays the number of rows you have set for display in the Rows per page field. You can increase the rows up to 500 for each page. You can navigate among the pages of the report using the navigation icons at the bottom right of this table.

Click the device name link to view the details of command sets and commands on the device. Go to **Step 3** for details.

**Step 3** Click the Status link in the Archive Details table. Alternatively, you can click on the device link and it takes you to the Device Center Home page providing more details about that device.

The NetShow Device Details pop-up appears with the device name, Command Sets and commands in the left pane and the command output in the right pane.
By default, the command output is a consolidated output for all the commands.

To get specific outputs for each command:

- Select a command from the Device list tree in the left pane.
- Click **Analyze Output** to view and analyze the output of the command.

If the selected command’s output appears as **No Output** in the right pane, the Analyze Output button is disabled.

You can mask the credentials shown in the output of `show` commands. See **Masking Credentials** for more details.

The Cisco.com Profile pop-up dialog box appears.

**Step 4**
Enter your Cisco.com Username and Password in the dialog box.

The credentials that you enter here will be used for the entire session.

The Show Commands Output Interpreter Viewer appears. It displays the report name, date, and time details in the header at the top of the report.

To convert the output in to a printer-friendly format click the Printer button.

---

### Deleting Output Archive

You can use this feature to delete the output of a NetShow Job archive. However, this action will not delete the corresponding job details.

To delete the Output Archive:

**Step 1**
Select **Monitor > Troubleshooting Tools > NetShow > Output Archive**.

The Output Archive page appears.

You can use the Filter option to filter the archives based on All or Job ID or Description as the criteria. You can provide a search string in the text area and click **Filter** to filter the archives based on the search criteria.

**Step 2**
Select the archives that you want to delete and click **Delete**.

A message appears, **Selected archives will be deleted**.

**Step 3**
Either:

- Click **OK** to delete the selected archives.
- Or
  - Click **Cancel** to cancel deleting the selected archives.
Command Sets

The Command Set represents a logical grouping of commands. Each command set is associated with a unique name.

NetShow provides a few pre-defined command sets that can be run against selected devices. See System-Defined Command Sets for more details on these command sets.

The command set can contain multiple commands in the following types of devices:

- Universal Gateways and Access Servers
- Content Networking
- DSL and Long Reach Ethernet (LRE)
- Optical Networking
- Routers
- Switches and Hubs
- Security and VPN
- Broadband Cable
- Storage Networking
- Voice and Telephony
- Network Management
- Wireless
- Cisco Interfaces and Modules

Since the command set itself contains `show` commands for different device types, you use them to run on multiple devices of various device types. You must identify the required command sets to solve a particular problem.

When you run command set on different types of devices, it sends only the `show` commands applicable for that device type. These command sets help you getting lab wide network status.

The Network Administrator and Network Operator can create command sets. The Network Administrator can assign command sets to other users.

When you migrate from LMS 2.x to LMS 3.x, Command Sets in LMS 2.x that have special characters will not appear in the LMS 3.x NetShow GUI. The valid characters for Command Set names are: A to Z, a to z, 0 to 9, -, _, ., ), (, /, and blank space.

Characters other than these are considered as special characters, and will not appear in the NetShow GUI.

This section contains System-Defined Command Sets.
# System-Defined Command Sets

The following table describes the System-defined command sets in NetShow:

<table>
<thead>
<tr>
<th>Command Set</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show ASP info</td>
<td>Shows information about the ASP macros</td>
</tr>
<tr>
<td>Show Cable Hop Information</td>
<td>Displays cable hop statistics</td>
</tr>
<tr>
<td>Show Cable Modem Info</td>
<td>Displays information for the registered and unregistered CMs</td>
</tr>
<tr>
<td>Show Cable Modulation-Profile</td>
<td>Displays modulation profile group information</td>
</tr>
<tr>
<td>Show Cable QoS Profile Info</td>
<td>Displays quality-of-service (QoS) profiles</td>
</tr>
<tr>
<td>Show Cable Spectrum Info</td>
<td>Displays information about spectrum groups</td>
</tr>
<tr>
<td>Show Cable Tech Info</td>
<td>Displays Cable Tech (system and configuration) information</td>
</tr>
<tr>
<td>Show Call Home Info</td>
<td>Displays information about Call Home such as:</td>
</tr>
<tr>
<td></td>
<td>• Show Call Home Detail</td>
</tr>
<tr>
<td></td>
<td>• Show Call Home Statistics</td>
</tr>
<tr>
<td>Show Configured GOLD Tests Info</td>
<td>Displays all the GOLD tests configured</td>
</tr>
<tr>
<td>Show Embedded Event Manager Info</td>
<td>Displays Embedded Event Manager information such as:</td>
</tr>
<tr>
<td></td>
<td>• Event Manager Policies Registered</td>
</tr>
<tr>
<td></td>
<td>• Event Manager Policies Available</td>
</tr>
<tr>
<td></td>
<td>• Event Manager Environmental Variables</td>
</tr>
<tr>
<td>Show GOLD Test Results</td>
<td>Displays results of the GOLD tests that are run</td>
</tr>
<tr>
<td>Show HCCP details Info</td>
<td>Displays information on groups associated with cable interfaces</td>
</tr>
<tr>
<td>Show IGMP Info</td>
<td>Displays information about multicast channels and interface</td>
</tr>
<tr>
<td>Show InlinePower Info</td>
<td>Displays status of inline power</td>
</tr>
<tr>
<td>Show Interface Info</td>
<td>Displays the current configuration and status</td>
</tr>
<tr>
<td>Show Interfaces Rate-Limit Info</td>
<td>Displays information about committed access rate</td>
</tr>
<tr>
<td>Show IP Routing Info</td>
<td>Displays the current state of the routing table</td>
</tr>
<tr>
<td>Show Protocol Info</td>
<td>Displays protocols configured for the entire system</td>
</tr>
<tr>
<td>Show SmartPort Macro Info</td>
<td>Displays information about SmartPort macros</td>
</tr>
<tr>
<td>Show SNMP Users and Groups Info</td>
<td>Displays SNMP information for a specific user and group</td>
</tr>
<tr>
<td>Show Switch VLAN Info</td>
<td>Displays information about VLAN and interface</td>
</tr>
<tr>
<td>Show System Info</td>
<td>Displays version, flash, logging, hardware, route</td>
</tr>
<tr>
<td>Show System Performance</td>
<td>Displays system interfaces, buffers, processes, memory</td>
</tr>
<tr>
<td>Show Tech Info</td>
<td>Displays system and configuration information</td>
</tr>
</tbody>
</table>
Managing Command Sets

The Command Set Administration task enables the administrator to view the details of an existing Command Set, create a new Command Set, edit an existing Command Set, and delete an existing Command Set.

Note
You must have Administrator privileges to perform any of these tasks.

This section contains:
- Viewing Command Set Details
- Creating a New Command Set
- Editing Command Sets
- Deleting Command Sets
- Adding and Deleting Adhoc Commands
- System-Defined Command Sets

Viewing Command Set Details

You can view the details of an existing Command Set using this feature.

To view the Command Set details:

**Step 1** Select Monitor > Troubleshooting Tools > NetShow > Command Sets. The Command Sets window appears.

**Step 2** Click the name of a Command Set in the List of Command Sets. The Command Set Details pop-up window appears.

**Step 3** Expand each of the list tree to view details of the Command Set assigned to each of the device category in the list.

**Step 4** Click Close to close the Command Set Details window.

Creating a New Command Set

You can create a new Command Set using this feature.

To create a new Command Set:

**Step 1** Select Monitor > Troubleshooting Tools > NetShow > Command Sets. The Command Sets window appears.

**Step 2** Click Create in the Command Sets window. The Select Device Category window appears.
Step 3  Enter the name of the Command Set in the Name field and a description for the Command Set in the Description field.

Step 4  Select the type of device from the Device Type Selector.

Step 5  Click Next to continue.

The Select Commands window appears.

Step 6  Select the command or commands you want to assign to the selected device or group of devices from the Available Commands pane in the Select Commands window.

- Select All Commands from the Commands Selection drop-down list to list all the commands available for the device or group of devices.
- Select Common Commands from the Commands Selection drop-down list to list only the common commands.

If you have a device category with no commands, it will not be considered for populating the Common Commands list.

Step 7  Click Add to add the selected commands.

The commands move to the Selected Commands pane in the Select Commands dialog box.

Step 8  Select commands from the Selected Commands pane and click Remove to delete the commands from the Selected Commands pane.

If you want to enter adhoc commands:

a. Enter them in the Adhoc Commands text box and click Add Adhoc.

The adhoc commands are added in the Available Commands pane.

b. Select the commands that you want to assign from the Available Commands and click Add.

See Adding and Deleting Adhoc Commands for more details on Adhoc Commands.

Step 9  Click Finish to create the new Command Set.

A message appears: Command Set Command Set name created successfully.

Step 10  Click OK.

The new Command Set appears in the List of Command Sets in the Command Sets Page.

---

Editing Command Sets

You can edit Command Sets using this feature. You can edit only user-defined Command Sets.

To edit a Command Set:

Step 1  Select Monitor > Troubleshooting Tools > NetShow > Command Sets.

The Command Sets window appears with the List of Command Sets.

Step 2  Select the name of the Command set in the List of Command Sets and click Edit.

The Select Device Category window appears with the device types that you have already selected and the Command Set name.

If you want to edit the Command Set for the particular device type, select the device type and click Next.

The Select Commands window appears.
Managing Command Sets

Step 3
Select the command or commands you want to assign to the selected device or group of devices from the Available Commands pane in the Select Commands window.

- Select All Commands from the Commands Selection drop-down list to list all the commands available for the device or group of devices.
- Select Common Commands from the Commands Selection drop-down list to list only the common commands.

If you have a device category with no commands, it will not be considered for populating the Common Commands list.

Step 4
Click:

- Add to add the selected commands.
  The commands move to the Selected Commands pane in the Select Commands dialog box.
- Remove to delete the commands from the Selected Commands pane.
- Enter the commands in the Adhoc Commands text box and click Add Adhoc.
- Select the adhoc commands from the Selected Commands pane and click Delete Adhoc to remove the adhoc commands.

See Adding and Deleting Adhoc Commands for more details on Adhoc Commands.

Step 5
Click Finish to edit the Command Set.
A message appears: Command Set Command Set name edited successfully.

Step 6
Click OK.

Deleting Command Sets

You can delete a Command Set or a list of Command Sets using this option. You can delete only user-defined Command Sets.

To delete Command Sets:

Step 1
Select Monitor > Troubleshooting Tools > NetShow > Command Sets.

The Command Sets window appears.

Step 2
Select the Command Sets you want to delete in the List of Command Sets and click Delete.

A message appears: Selected Command Sets will be deleted.

Step 3
Either:

- Click OK to confirm the deletion of the Command Sets.
  Or
- Click Cancel to cancel the deletion of the Command Sets.
Adding and Deleting Adhoc Commands

You can enter the following adhoc commands while creating a command set:
- show, version, where, ping, traceroute, and ?
You can use the short forms of these commands. For example you can use sh for show.

To add and delete Adhoc Commands:

**Step 1** Select Monitor > Troubleshooting Tools > NetShow > Command Sets.
The Command Sets window appears.

**Step 2** Click Create in the Command Sets window.
The Select Device Category window appears.

**Step 3** Enter the name of the Command Set in the Name field and a description for the Command Set in the Description field.

**Step 4** Select the type of device from the Device Type Selector.

**Step 5** Click Next to continue.
The Select Commands window appears.

**Step 6** Enter the adhoc commands in the Adhoc Commands text box and click Add Adhoc.
You can enter multiple commands; separate them by commas.
The adhoc commands are added to the Available Commands list.
- Select the adhoc commands from the Available Commands list and click Add.
  The adhoc commands are added to the Selected Commands list.
- Select the adhoc commands from the Selected Commands list and click Remove to remove them from the Command Set.

You can delete the adhoc commands permanently only if they are not assigned to any Command Set.

**Step 7** Click Finish to create the new command set.
A message appears: Command Set Command Set name created successfully.

**Step 8** Click OK.
The new Command Set appears in the List of Command Sets in the Command Sets Page.

Assigning Command Sets

Network Administrators can assign command sets to Network Operators to authorize them with executable Command Sets.

By default, all system-defined command sets are assigned to Network Administrators.
The Assigning Command Sets feature in NetShow allows you to specify which user or set of users can run NetShow commands.
Assigning Command Sets

Your login determines whether you can use this option. You can use the Assigning Command Sets feature in Netshow for:

- Showing Assigned Command Sets
- Assigning Command Sets to Users
- Assigning Custom Command Execution Privilege

Showing Assigned Command Sets

You can view the list of user-defined Command Sets assigned to a particular user using this feature.

To show the assigned Command Sets:

2. Enter the username in the Username field and click `Show Assigned`. The username must be that of a valid Cisco Prime LMS user. The Command Sets assigned to this user appears in the Selected User-Defined Command Sets pane in the Assign Command Sets window.

Assigning Command Sets to Users

To assign Command Sets to users:

2. Enter the username in the Username field.
3. Select the Command Sets that you want to allocate to the user from the Available User-Defined Command Sets list and click `Add`. The selected Command Sets appear in the Selected User-Defined Command Sets list.
4. Add all the required Command Sets to the Selected User-Defined Command Sets list box.
5. Click `Assign` to assign the Command Sets access privileges to the specified user. For a specified user to see the assigned Command Sets, enter the username in the Username field and click `Show Assigned`. The Command Sets assigned to the user appear in the Selected User-Defined Command Sets list.
Assigning Custom Command Execution Privilege

You can assign custom command execution privilege to selected users, using the Assigning Command Set feature. You can assign this privilege to one or more users. These users can enter custom commands while creating NetShow jobs only if this privilege is enabled.

To assign Custom Command Execution privilege:

---

**Step 1** Select *Monitor > Troubleshooting Tools > NetShow > Assigning Command Sets.*

The Assign Command Sets dialog box appears.

**Step 2** Enter the username in the Username field.

**Step 3** Check the Custom Command Execution check box to assign custom command execution privilege to this user.

Launching *show* Commands From Device Center

You can run *show* commands from Device Center.

To run *show* commands from Device Center:

---

**Step 1** Select *Device Troubleshooting > Device Center.*

The Device Center window appears with the device selector on the right and Device Center overview information on the left section of the screen.

**Step 2** Either:

- Enter the device name of the device you want to select and click *Go* in the Device Selector field.
- Or

  - Select a device from the list-tree.

The Device Summary and Functions Available panes appear in the right section of the screen.

**Step 3** Select *Run Show Command* from the Management Tasks tab under the Functions Available pane.

The Select Command Set window appears.

**Step 4** Select the Command Set from the Command Set List pane in the Show Commands Execution window.

**Step 5** Enter the custom commands in the Custom Commands text box.

**Step 6** Click *Next.*

The Set Schedule Options page appears with the Job Schedule and Options dialog box.
### Chapter 10      Using NetShow Commands

#### Launching show Commands From Device Center

**Step 7** Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>The Run Type of the job. The Run Types could be any or all of these, depending on the type of the job:</td>
</tr>
<tr>
<td></td>
<td>- Immediate—Runs the job immediately.</td>
</tr>
<tr>
<td></td>
<td>- Once—Runs the job once at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>- 6-hourly—Runs the job every 6 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>- 12-hourly—Runs the job every 12 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>- Daily—Runs daily at the specified time.</td>
</tr>
<tr>
<td></td>
<td>- Weekly—Runs weekly on the day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>- Monthly—Runs monthly on the day of the month and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>- Last day of Month—Runs on the last day of the month at the specified time.</td>
</tr>
<tr>
<td></td>
<td>The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete.</td>
</tr>
<tr>
<td></td>
<td>For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed.</td>
</tr>
<tr>
<td></td>
<td>If the 10:00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.</td>
</tr>
<tr>
<td></td>
<td>To change, select the required run type from the drop-down list.</td>
</tr>
<tr>
<td>Date</td>
<td>Scheduled date and time of the job.</td>
</tr>
<tr>
<td><strong>Job Information</strong></td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job.</td>
</tr>
<tr>
<td></td>
<td>You can enter multiple e-mail addresses; separate these addresses by commas.</td>
</tr>
<tr>
<td></td>
<td>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences).</td>
</tr>
<tr>
<td></td>
<td>We recommend that you configure the LMS Server E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent with the LMS Server E-mail ID as the sender's address.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter your comments for the job. Comments appear in the Job Work Order.</td>
</tr>
<tr>
<td><strong>Job Options</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Job Password</td>
<td>- If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin &gt; Network &gt; Configuration Job Settings &gt; Config Job Policies) enter the device login user name and password and Device Enable password.</td>
</tr>
<tr>
<td></td>
<td>- If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin &gt; Network &gt; Configuration Job Settings &gt; Config Job Policies) either:</td>
</tr>
<tr>
<td></td>
<td>- Enter the device login user name and password and Device Enable password.</td>
</tr>
<tr>
<td></td>
<td>- Or</td>
</tr>
<tr>
<td></td>
<td>- Disable the Job Password option in the Job Schedule and Options dialog box.</td>
</tr>
</tbody>
</table>
Using cwcli netshow Command

You can invoke Netshow features from Command Line Interface (CLI).

The cwcli netshow command let you use NetShow features from the command line. You can use the cwcli netshow commands to view, browse, create, delete, and cancel NetShow jobs and Command Sets.

This command is described in the cwcli framework chapter. For details, see the Configuration Online help.

---

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Execution</strong></td>
<td>Specify the order in which the job should run on the devices.</td>
</tr>
<tr>
<td></td>
<td>• Parallel—Allows the job to run on multiple devices at the same time.</td>
</tr>
<tr>
<td></td>
<td>By default, the job runs on five devices at a time.</td>
</tr>
<tr>
<td></td>
<td>• Sequential—Allows the job to run on only one device at a time.</td>
</tr>
<tr>
<td><strong>Maker Comments</strong></td>
<td>This field appears only if you have enabled Job Approval Policies for NetShow. Enter the Maker Comments. See Setting Up Job Approval for more details on enabling Job Approval Policies.</td>
</tr>
<tr>
<td><strong>Maker E-mail</strong></td>
<td>This field appears only if you have enabled Job Approval Policies for NetShow. Enter the Maker E-mail address. This is mandatory. See Setting Up Job Approval for more details on enabling Job Approval Policies.</td>
</tr>
</tbody>
</table>

**Step 8**

Click **Next**.

The View Job Work Order page appears with the Job Work Order.

The Job Work Order contains general information on the job and on the:

• Job policies.
• Job approval details (if you have enabled job approval).
• Device details.
• Command Sets and the commands to be run.

**Step 9**

Click **Finish** after you review the details of your job in the Job Work Order dialog box.

A message appears, **Job ID created successfully**.

The newly created job appears in the NetShow Job Browser.
About Troubleshooting Tools

This chapter provide information on:

- Troubleshooting Network Devices and Endhosts
- Troubleshooting VRF

Troubleshooting Network Devices and Endhosts

Troubleshooting workflow in LMS collects information from the network and helps you to overcome network management challenges.

Using this workflow, you can view the details of devices, endhosts, and links to troubleshoot the network connectivity problems or device diagnostics.

You can select either:

- Device Center — You can view the details of a device in the Device Troubleshooting page.
- End Host Center — You can view the details of an endhost in the Endhost Troubleshooting page.

See the following topics for more information:

- Troubleshooting Steps
- Troubleshooting Details
- Device Troubleshooting
- Link Troubleshooting
- Endhost Troubleshooting
Troubleshooting Steps

To troubleshoot the problems in your network:

**Step 1** Select one of the following paths from the menu and launch the workflow:

- **Monitor > Troubleshooting Tools > Troubleshooting Workflows**
- Or
- **Inventory > Tools > Device Center**

The troubleshooting workflow appears.

You can mouse hover on device IP Address or Hostname in the Global Search Results page for device and launch the troubleshooting workflows.

**Step 2** Select either Device Center or End Host Center.

**Step 3** Follow the steps mentioned in:

- **Using Endhost Center** to proceed with diagnosing endhosts.
- **Using Device Center** to proceed with diagnosing devices.

---

**Using Endhost Center**

If you have selected Endhost Center, enter the endhost details to get the details of the last connected switch. To do so:

**Step 1** Select a search parameter from the Attribute drop-down list.

The attributes are:

- IP Address
- MAC Address
  
The supported MAC Address formats are:
  - `xxxx:xxxx:xxxx`
  - `xxxxxxxxxxxx`
  - `xxxx:xxxx:xxxx`
  - `xx.xx.xx.xx.xx.xx`
  - `xxxx.xxxx.xxxx`
- Username
- Hostname
- IP Phone Number

On selecting an attribute, the corresponding field is displayed on the screen.

For example, if you select MAC Address, a field with label name as MAC Address appears.

**Step 2** Enter a value in the field that is located next to the Attribute drop-down list.
For example, if you select MAC Address, enter the MAC Address of the switch in the value field.

**Step 3**  
Click **Find Last Connected Switch**.  
The details of the last connected switch appears.

**Step 4**  
Click **View**.

**Step 5**  
Do the following to troubleshoot another device: 
   a. Click the switch icon and select the required switch.  
   b. Select the required port of the switch.  
   c. Click **View**.

The details of the selected device appear in the End Host tab on the right pane. See *Endhost Troubleshooting* for more information.

---

**Using Device Center**

Device Center allows you to select a device and view the details of a device in the Device Troubleshooting page. You can see reports for the selected device, invoke various tools on the selected device, and run the tasks that can be performed on the selected device.

If you have selected Device Center, enter the details of the device. To do so:

**Step 1**  
Click the device selector icon and select the required switch.

**Note**  
If device selector has more than 2000 nodes, it takes time to expand the nodes. The loading image may not get displayed immediately while expanding the nodes and a stop script error may be thrown by the browser. You can ignore the stop script error while loading the nodes and select the No option to continue loading.

**Step 2**  
Click **View**.

The details of the selected device appear in a tab on the right pane. See *Device Troubleshooting* for more information.
Troubleshooting Details

The troubleshooting information for a device, link, or an endhost appears in a new tab in the form of portlets under the respective panes.

Expand or collapse option is provided for each pane on a mouseclick. Each pane has several portlets, which displays the information on devices, endhosts, or links.

A refresh icon is provided for most of the portlets. You can refresh the portlets using this icon and get the latest details of portlet contents.

See the following topics for more details:
- Device Troubleshooting
- Link Troubleshooting
- Endhost Troubleshooting

You can view the topology of the network using the View Topology button. See Viewing Topology of Network for more information.

Viewing Topology of Network

Device Troubleshooting and Endhost Troubleshooting pages provide the View Topology button. You can view the network topology of the device using this option.

The default hop count used for launching the topology view is 1.

You can change the hop count and click the Refresh icon to launch the topology view with the specified number of hops. The maximum number of hops that you can enter is 3.

You can click the following network elements from the topology to view the details and troubleshoot your network problems:
- Devices — See Device Troubleshooting for more information.
- Links — See Link Troubleshooting for more information.
- Endhosts — See Endhost Troubleshooting for more information.

On clicking the network elements, the details appear in a mouse-hover popup window.
Device Troubleshooting

Device troubleshooting displays the following panes:

- Device Status — See Device Status Details for more information.
- Configuration Status — See Configuration Status Details for more information.
- Reachability Status — See Reachability Details for more information.
- Events and Faults — See Events and Faults Details for more information.
- Port Status — See Port Status Details for more information.
- Performance Details — See Performance Details for more information.

Device Status Details

The Device Status pane contains the following portlets:

- Device Information
- Reachability Status
- Latest Configuration Change
- Collector Status
- Technology Details

The Device Status pane provides option to see reports for the selected device, invoke various tools on the selected device, and run the tasks that can be performed on the selected device.

See Quick Links to Tools, Tasks, and Reports in Device Status Pane for more information.

Device Information

This portlet contains the device information as available in Device and Credential Repository (DCR).

Table 11-1 describes the fields in the Device Information portlet.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Display name of the device as entered in Device Credential repository.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the device.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device Type Information. For example, Cisco 2511 Access Server, etc.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname of the device as entered in Device Credential repository</td>
</tr>
<tr>
<td>Software Version</td>
<td>IOS version installed on the device</td>
</tr>
<tr>
<td>Image</td>
<td>Details of the software image</td>
</tr>
<tr>
<td>Location</td>
<td>Area, floor or the building where the device reside</td>
</tr>
<tr>
<td>Contact</td>
<td>E-mail address of the device administrator</td>
</tr>
<tr>
<td>EOL</td>
<td>End of Life information of the device hardware</td>
</tr>
<tr>
<td>EOS</td>
<td>End of Sale information of the device hardware</td>
</tr>
</tbody>
</table>
Troubleshooting Network Devices and Endhosts

Chapter 11  About Troubleshooting Tools

Troubleshooting Network Devices and Endhosts

Reachability Status

This portlet displays the device connectivity information on clicking the Test Now button.

Table 11-2 describes the fields in the Reachability Check portlet. The fields display the value as Success or Failed depending upon the connection status.

### Table 11-2  Reachability Check Portlet Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping</td>
<td>Ping status of the selected device. Checks whether the device is reachable. A ping tests an ICMP echo message and its reply.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Ping status of the selected device. Sends an HTTP request to the HTTP port 80 of the destination device.</td>
</tr>
<tr>
<td>SNMPv1 Read</td>
<td>Status of SNMPv1 Read Community string (service test, port 161) of the selected device. Sends an snmp get request to the destination device for an SNMP read test (SNMPR).</td>
</tr>
<tr>
<td>SNMPv1 Write</td>
<td>Status of SNMPv1 Write Community string (service test, port 161) of the selected device. Sends an snmp set request to the device to test SNMP write (SNMPW).</td>
</tr>
<tr>
<td>SNMPv2c Read</td>
<td>Status of SNMPv2c Read Community string (service test, port 161) of the selected device. Sends an snmp get request to the destination device for an SNMP read test (SNMPR).</td>
</tr>
<tr>
<td>SNMPv2c Write</td>
<td>Status of SNMPv2c Write Community string (service test, port 161) of the selected device. Sends an snmp set request to the device to test SNMP write (SNMPW).</td>
</tr>
</tbody>
</table>
Table 11-2 Reachability Check Portlet Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSHv1</td>
<td>SSHv1 credentials status (service test, port 22) of the selected device. Checks whether SSH is enabled on the device. If the destination device responds to SSH requests, this also tests whether LMS server can make SSH requests to that device. It does not verify the password in the database.</td>
</tr>
<tr>
<td>SSHv2</td>
<td>SSHv2 credentials status (service test, port 22) of the selected device. Checks whether SSH is enabled on the device. If the destination device responds to SSH requests, this also tests whether LMS server can make SSH requests to that device. It does not verify the password in the database.</td>
</tr>
<tr>
<td>Telnet</td>
<td>Telnet status (service test, port 23) of the selected device. Checks whether Telnet is enabled on the device and if the destination device responds to a Telnet request. It does not verify that the Telnet password in the database works.</td>
</tr>
</tbody>
</table>

Latest Configuration Change

You can view the following in this portlet:

- The time when the running configuration was archived in the Configuration Archive.
- The differences between the two archived running configurations in the Configuration Archive.

Collector Status

This portlet summarizes the status of the collection tasks occurred on the device.

Table 11-3 describes the fields in the Collector status portlet.

Table 11-3 Collector Status Portlet Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Collector Name | Name of the collection tasks. Possible values are:
| Status | Displays the status as Success or Failed. |
| Collection Time | Time when the collection was completed. |
Technology Details

This portlet summarizes the details of technologies enabled on the device. Table 11-4 describes the fields in the Technology Details portlet.

Table 11-4 Technology Details Portlet Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Name</td>
<td>Name of the Work Center technologies enabled on the device. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• EnergyWise</td>
</tr>
<tr>
<td></td>
<td>• Identity</td>
</tr>
<tr>
<td></td>
<td>• Smart Install</td>
</tr>
<tr>
<td></td>
<td>• Auto Smart Ports</td>
</tr>
<tr>
<td></td>
<td>• IPSLA</td>
</tr>
<tr>
<td></td>
<td>• Responder</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the technologies. The status could be Enabled, Disabled, or Software Incapable.</td>
</tr>
</tbody>
</table>

Quick Links to Tools, Tasks, and Reports in Device Status Pane

The Device Status pane provides the links to various diagnostic and connectivity tools, reports, and tasks.

All these links are categorized under the menus: Tools, Tasks, and Reports. Move the cursor on the menus or click the menus to view the entire list of quick links.

The Quick Links under the Tools, Tasks and Reports menus are listed in Table 11-5.
### Table 11-5 Links under the Tools, Tasks, and Reports menus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Quick Link</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tools</td>
<td>Chassis View</td>
<td>Allows you to launch the chassis view of the selected device. See <em>Inventory Management with Cisco Prime LAN Management Solution 4.1</em> for more information.</td>
</tr>
<tr>
<td>Cluster Management Suite</td>
<td></td>
<td>Launches the Cluster Management Suite for the selected device. This link works only when you select a device of type cluster switch.</td>
</tr>
<tr>
<td>Edit Device Credentials</td>
<td></td>
<td>Allows you to edit the credentials of a selected device such as primary credentials, secondary credentials, Auto Update Server managed credentials, and RxBoot mode credentials. See <em>Inventory Management with Cisco Prime LAN Management Solution 4.1</em> for more information.</td>
</tr>
<tr>
<td>Edit Device Identity</td>
<td></td>
<td>Allows you to edit the identity information of a selected device such as Device Name, Display Name, Cluster information, and so on. See <em>Inventory Management with Cisco Prime LAN Management Solution 4.1</em> for more information.</td>
</tr>
<tr>
<td>Management Station to Device</td>
<td></td>
<td>Allows you to check the device connectivity by a protocol to troubleshoot problems with un-managed or non-responding devices. The Management Station to Device tool helps you to diagnose Layer 4 (application) connectivity problems. See <em>Troubleshooting Network Devices and Endhosts</em> for more information.</td>
</tr>
<tr>
<td>Mini-RMON</td>
<td></td>
<td>Allows you to launch the CiscoView Mini-RMON manager. See <em>Inventory Management with Cisco Prime LAN Management Solution 4.1</em> for more information.</td>
</tr>
<tr>
<td>Packet Capture</td>
<td></td>
<td>Allows you to capture live data from LMS machine to aid in troubleshooting.</td>
</tr>
<tr>
<td>Proxy Ping</td>
<td></td>
<td>Proxy Ping allows you to ping another device or server from the selected device and displays the ping output. See <em>Proxy Ping</em> for more information.</td>
</tr>
<tr>
<td>Proxy Traceroute</td>
<td></td>
<td>Proxy Traceroute displays the output of traceroute of the device or server from the selected device. See <em>Proxy Traceroute</em> for more information.</td>
</tr>
<tr>
<td>SNMP Set</td>
<td></td>
<td>Allows you to use this option to set an SNMP object or multiple objects on a device for controlling the device.</td>
</tr>
<tr>
<td>SNMP Walk</td>
<td></td>
<td>Allows you to trace the MIB tree of a device starting from a given OID for troubleshooting, or gathering information about certain device.</td>
</tr>
<tr>
<td>Telnet/SSH</td>
<td></td>
<td>Allows you to connect to a specified device using Telnet or SSH.</td>
</tr>
</tbody>
</table>
### Troubleshooting Network Devices and Endhosts

**Table 11-5**  
**Links under the Tools, Tasks, and Reports menus**

<table>
<thead>
<tr>
<th><strong>Menu</strong></th>
<th><strong>Quick Link</strong></th>
<th><strong>Function</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tasks</strong></td>
<td>Add Images to Software Repository</td>
<td>Allows you to add the software images from the devices to software repository. See <em>Configuration Management with Cisco Prime LAN Management Solution 4.1</em> for more information.</td>
</tr>
<tr>
<td></td>
<td>Analyze using cisco.com Image</td>
<td>Allows you to enter the Cisco.com credentials and the proxy server credentials. These credentials that you enter are used throughout the session. See <em>Configuration Management with Cisco Prime LAN Management Solution 4.1</em> for more information.</td>
</tr>
<tr>
<td></td>
<td>Analyze using Repository Image</td>
<td>See <em>Configuration Management with Cisco Prime LAN Management Solution 4.1</em> for more information.</td>
</tr>
</tbody>
</table>
| | Check Device Credential | Allows you to check one or more of the following Device Credential options:  
- SNMP Read Community String  
- SNMP Write Community String  
- SNMPv3  
- Telnet  
- Telnet Enable Mode User Name and Password  
- SSH  
- SSH Enable Mode User Name and Password |
| | Configure IPSLA Collector | Allows you to configure IPSLA Collectors in the Collector Management screen. |
| | Create Poller | Allows you to create pollers in the Poller Management screen. |
| | Distribute images | Allows you to distribute images in your network and also you can analyze and determine the impact and prerequisites for new software images before distribution. See *Configuration Management with Cisco Prime LAN Management Solution 4.1* for more information. |
| | Edit Config | Allows you to edit the device configuration using Config Editor. |
| | Open TAC Case | Allows you to create new service requests to TAC, and query the list of Service requests. |
| | Run Show Command | Allows you to run the show commands on the selected device. |
| | Search Communities | Allows you to access the Cisco Search Communities page that lists the links of the cisco forums and posts related to the key words of the device type. |
| | Sync Archive | Allows you to use this feature to synchronize the device manually with the running configuration. |
| | Trigger User Tracking | Starts User Tracking acquisition. |
| | Update Inventory | Allows you to update the device inventory and create an immediate job to collect the Inventory for the selected device. |
| | View Config | Allows you to view the device configuration using the Config Viewer window. |
| | View Pending Jobs | Allows you to view the list of pending jobs in Configuration Browser. |
### Table 11-5: Links under the Tools, Tasks, and Reports menus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Quick Link</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports</td>
<td>24 Hours Change Audit Report</td>
<td>Allows you to generate 24 Hours Change Audit report for the device. This report displays the changes made in the past 24 hours from the data stored in the Change Audit log.</td>
</tr>
<tr>
<td></td>
<td>Call Home History</td>
<td>Allows you to launch the Smart Call Home report.</td>
</tr>
<tr>
<td></td>
<td>Credential Verification Report</td>
<td>Allows you to launch the Device Credential Verification Report for the selected device.</td>
</tr>
<tr>
<td></td>
<td>Detailed Device Report</td>
<td>Launches the Detailed Device report for the device selected. See <em>Reports Management with Cisco Prime LAN Management Solution 4.1</em> for more information.</td>
</tr>
<tr>
<td></td>
<td>Device Attribute Report</td>
<td>Allows you to generate the Device Attributes report.</td>
</tr>
<tr>
<td></td>
<td>Device Dashboard</td>
<td>Launches the Device Dashboard details for the device selected. See <em>Reports Management with Cisco Prime LAN Management Solution 4.1</em> for more information.</td>
</tr>
<tr>
<td></td>
<td>Fault History Report</td>
<td>Allows you to launch the Device Fault History report to gather historical information on alarms and events in the last 31 days.</td>
</tr>
<tr>
<td></td>
<td>Interface Errors Report</td>
<td>Allows you to view the Interface Error report that displays the error rate information of a device interface during the last 24 hours.</td>
</tr>
<tr>
<td>MAC Reports</td>
<td>Dormant MAC Report</td>
<td>Allows you to generate the Dormant MAC report that contains the details of MAC Addresses that are inactive for the specified number of days.</td>
</tr>
<tr>
<td></td>
<td>New MAC Report</td>
<td>Allows you to generate the New MAC report that contains the details of MAC Addresses that are newly added to the network.</td>
</tr>
<tr>
<td></td>
<td>Rogue MAC Report</td>
<td>Allows you to generate the Rogue MAC report that contains the details of MAC Addresses that are not authorized to exist in the network.</td>
</tr>
<tr>
<td></td>
<td>Port Attributes Report</td>
<td>Allows you to generate the Port Attributes report.</td>
</tr>
</tbody>
</table>
### Troubleshooting Network Devices and Endhosts

#### Table 11-5: Links under the Tools, Tasks, and Reports menus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Quick Link</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports (contd...)</td>
<td>Switch Port Reports</td>
<td>Allows you to generate the Recently Down Port Report from the report generator.</td>
</tr>
<tr>
<td></td>
<td>Recently Down Report</td>
<td>Recently Down Port report displays:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* Link ports that were connected to a device in the previous Data Collection, but found unconnected in the current Data Collection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* Access ports that were connected to an endhost in the last UT Major Acquisition cycle, but found unconnected in the current Data Collection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the ports are still in an Unconnected state when the next UT Major Acquisition cycle runs, they are classified as Unused Up or Unused Down ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>These ports are further moved to the Reclaim Unused Up Ports report or Reclaim Unused Down Ports report.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Link and access ports can be queried to generate the Unused Down report. It uses ports:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* That are administratively down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* That were previously connected to an endhost or a device but are unconnected at least for a period of one day.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can generate reports on ports that have been in Unused Down state for a specified interval of time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Link and access ports can be queried to generate the Unused Up report. It uses ports:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* That are administratively up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* That were previously connected to an endhost or a device but are unconnected at least for a period of one day.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can generate reports on ports that have been in Unused Up state for a specified interval of time.</td>
</tr>
</tbody>
</table>
Table 11-5  Links under the Tools, Tasks, and Reports menus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Quick Link</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports (contd..)</td>
<td>Switch Port Reports (contd..)</td>
<td>Allows you to generate the Switch Port Capacity Report from the report generator. The Switch Port Capacity report lists switches that have crossed utilization threshold limits, along with the value of percentage port utilization. This report enables you to do capacity planning for network growth.</td>
</tr>
<tr>
<td>Switch Port Capacity Report</td>
<td>Switch Port Summary Report</td>
<td>Allows you to generate the Switch Port Summary Report from the report generator. Switch Port Summary report gives the number of Connected, Free, and Free Down ports in each switch. Ports that are administratively up but are not connected to a device or endhost are Free Ports. Ports that are administratively down and are not connected to a device or endhost are Free Down ports. This report also displays the sum of Connected, Free, and Free Down ports in each switch. This report lists all the Down ports in a switch, regardless of whether they were previously connected to an endhost or not. The number for Connected, Free and Free Down ports are given as links. Clicking on them launches a detailed report giving the Port, Port name, Administrative and Operational status of the ports for the selected device.</td>
</tr>
<tr>
<td>Syslog Messages Report</td>
<td></td>
<td>Allows you to generate the Syslog Messages report. This report displays the number of Syslog messages based on the severity that are logged in the past 24 hours.</td>
</tr>
<tr>
<td>UT End Host Report</td>
<td></td>
<td>Allows you to generate User Tracking End Host report.</td>
</tr>
<tr>
<td>VLAN Report</td>
<td></td>
<td>Allows you to generate VLAN reports for devices, switch clouds, or VTP domains.</td>
</tr>
</tbody>
</table>

Configuration Status Details

The following portlets are displayed under Configuration Status pane:

- Configuration Details
- Inventory Collection

Configuration Details

This portlet summarizes the configuration details on the device.

Table 11-6 describes the fields in the Configuration Details portlet.

Table 11-6  Configuration Details Portlet Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSLA</td>
<td>Displays true when the device is IPSLA enabled.</td>
</tr>
<tr>
<td>Responder Enabled</td>
<td>Displays true when responder is enabled on the device.</td>
</tr>
<tr>
<td>Maximum Number of Collectors</td>
<td>Displays the maximum number of collectors available.</td>
</tr>
</tbody>
</table>
### Inventory Collection

You can view the following details in this portlet:

- RAM size (in MB)
- Chassis Serial Number
- Partitions
- Number of modules

### Reachability Details

The following portlets are displayed under Reachability Details pane:

- **Device Availability**
- **Ping device from LMS Server**
- **Traceroute device from LMS Server**

---

**Table 11-6 Configuration Details Portlet Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured Collectors</td>
<td>Displays the number of collectors configured already.</td>
</tr>
<tr>
<td>Configurable Collectors</td>
<td>Displays the number of collectors that can be configured.</td>
</tr>
<tr>
<td>PSIRTs</td>
<td>Display the number of PSIRT announcements applicable for the device. The hyperlink provided on the value leads to PSIRT reports.</td>
</tr>
<tr>
<td>Endhosts</td>
<td>Displays the number of endhosts connected to the device.</td>
</tr>
<tr>
<td>IP Phones</td>
<td>Displays the number of IP Phones connected to the device.</td>
</tr>
<tr>
<td>VTP Domain</td>
<td>VTP domain name of the device where the endhost is connected.</td>
</tr>
<tr>
<td>VTP Mode</td>
<td>VTP mode of the device where the endhost is connected.</td>
</tr>
<tr>
<td>VTP Version</td>
<td>Displays the VTP version.</td>
</tr>
<tr>
<td>Number of VLANs</td>
<td>Displays the number of VLANs associated with the device. The hyperlink provided on the value leads to the VLAN reports.</td>
</tr>
</tbody>
</table>
Device Availability

The Device Availability portlet enables you to view the availability status of the selected device managed in the network in the last one day or one hour.

The following information about the last polled devices is displayed in the portlet in a graphical format:

- Last Polled Status — Displays the percentage of devices available in the network in the last polling cycle.
- Minimum (%) — Displays the minimum percentage of devices available in the network in the last polled cycles.
- Maximum (%) — Displays the maximum percentage of devices available in the network in the last polled cycles.
- Average (%) — Displays the average percentage of devices available in the network in the last polled cycles.
- Histograph — Displays an icon, which when clicked displays the Histograph chart.
- Livegraph — Displays an icon, which when clicked displays the Livegraph chart.

Table 11-7 displays the color and the percentage of the availability status of the device.

<table>
<thead>
<tr>
<th>Color</th>
<th>Availability Status of the Devices in Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Availability status of the device from 90 to 100%</td>
</tr>
<tr>
<td>Yellow</td>
<td>Availability status of the device from 50 to 90%</td>
</tr>
<tr>
<td>Orange</td>
<td>Availability status of the device from 10 to 50%</td>
</tr>
<tr>
<td>Red</td>
<td>Availability status of the device from 0 to 10%</td>
</tr>
</tbody>
</table>

Ping device from LMS Server

This portlet displays the output or result of pinging the device from the LMS Server, and the ping statistics, on clicking the Test Now button.

The ping statistics include packets transmitted, packets received, and the percentage of packet loss.

Traceroute device from LMS Server

This portlet displays the output of traceroute of the device from a LMS Server, and the traceroute statistics, on clicking the Test Now button.

Events and Faults Details

The following portlets are displayed under Events and Faults pane:

- Faults
- Syslogs
- Change Audit
Faults

This portlet summarizes the Fault details of the device managed in the network in the last one hour or one day.

Table 11-8 describes the fields in the Fault Details portlet.

Table 11-8  Fault Details Portlet Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Fault Severity. This can be Critical, Informational, or Warning.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Identifier of the fault</td>
</tr>
<tr>
<td>Description</td>
<td>Description about the fault</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the fault; whether they are owned or cleared by the user</td>
</tr>
<tr>
<td>Category</td>
<td>Fault category. Possible values for this field could be:</td>
</tr>
<tr>
<td></td>
<td>• Application</td>
</tr>
<tr>
<td></td>
<td>• Connectivity</td>
</tr>
<tr>
<td></td>
<td>• Environment</td>
</tr>
<tr>
<td></td>
<td>• Interface</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td></td>
<td>• Reachability</td>
</tr>
<tr>
<td></td>
<td>• System Hardware</td>
</tr>
<tr>
<td></td>
<td>• Utilization</td>
</tr>
<tr>
<td>Duration</td>
<td>Time span between creation of faults and the current server time for the active or owned faults.</td>
</tr>
<tr>
<td></td>
<td>Time span between creation of faults and the time of clearing faults.</td>
</tr>
<tr>
<td>Last Occurrence</td>
<td>Date and time when the fault has occurred.</td>
</tr>
</tbody>
</table>

Syslogs

This portlet summarizes the Syslog details of the device managed in the network in the last one day or one hour.

Table 11-9 describes the fields in the Syslogs portlet.

Table 11-9  Syslog Details Portlet Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Name of the device generating the Syslog message.</td>
</tr>
<tr>
<td>Severity</td>
<td>Message severity level. LMS captures the following severity levels: Emergencies(0), Alerts (1), Critical (2), Errors (3).</td>
</tr>
<tr>
<td>Mnemonic</td>
<td>Code that uniquely identifies the error message. Note that older Catalyst messages do not display a mnemonic. An example of a mnemonic for an IOS message is CONFIG I.</td>
</tr>
<tr>
<td>Description</td>
<td>Syslog Message description.</td>
</tr>
</tbody>
</table>
Change Audit

This portlet summarizes the Change Audit details of the device managed in the network in the last one hour or one day.

Table 11-10 describes the fields in the Change Audit portlet.

**Table 11-10  Change Audit Details Portlet Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Username on which the automated action has to be triggered</td>
</tr>
<tr>
<td>Connection Mode</td>
<td>Name of the user who performed the change. This is the name entered when the user logged in</td>
</tr>
<tr>
<td>Message</td>
<td>Brief summary of the network change.</td>
</tr>
<tr>
<td>Application Name</td>
<td>Name of the application on which the automated action has to be triggered.</td>
</tr>
<tr>
<td>Creation Time</td>
<td>Time at which the automated action is created.</td>
</tr>
</tbody>
</table>
Port Status Details

The following portlets are displayed under Port Status pane:

- **Link Ports**
- **Access Ports**
- **Trunk Ports**

These portlets can contain 100 records by default.

**Link Ports**

This portlet summarizes the status of link ports of the device. You can use the refresh icon to see the latest content of the portlet.

*Table 11-11* describes the fields in the Link Ports portlet.

*Table 11-11  Link Ports Portlet Fields*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Name of the link port</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Displays whether port has been brought down intentionally</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Displays whether port is active or inactive</td>
</tr>
<tr>
<td>Port Description</td>
<td>Description of the port that you have entered</td>
</tr>
<tr>
<td>Type</td>
<td>Media type, such as Ethernet</td>
</tr>
<tr>
<td>Speed</td>
<td>Link port speed</td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Displays the duplex mode; whether half-duplex or full-duplex.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Name of the VLAN.</td>
</tr>
<tr>
<td>L2L3</td>
<td>Shows whether the port is in Layer 2 or Layer 3, switched or routed.</td>
</tr>
</tbody>
</table>

**Access Ports**

This portlet summarizes the status of access ports of the device. You can use the refresh icon to see the latest content of the portlet.

*Table 11-12* describes the fields in the Access Ports portlet.

*Table 11-12  Access Ports Portlet Fields*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Name of the access port</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Displays whether port has been brought down intentionally</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Displays whether port is active or inactive</td>
</tr>
<tr>
<td>Port Description</td>
<td>Description of the port that you have entered</td>
</tr>
<tr>
<td>Type</td>
<td>Media type, such as Ethernet</td>
</tr>
<tr>
<td>Speed</td>
<td>Access port speed</td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Displays the duplex mode; whether half-duplex or full-duplex.</td>
</tr>
</tbody>
</table>
Chapter 11 About Troubleshooting Tools

### Trunk Ports

This portlet summarizes the status of trunk ports of the device. You can use the refresh icon to see the latest content of the portlet.

Table 11-13 describes the fields in the Trunk Ports portlet.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Name of the trunk port</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Displays whether port has been brought down intentionally</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Displays whether port is active or inactive</td>
</tr>
<tr>
<td>Port Description</td>
<td>Description of the port that you have entered</td>
</tr>
<tr>
<td>Type</td>
<td>Media type, such as Ethernet</td>
</tr>
<tr>
<td>Speed</td>
<td>Trunk port speed</td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Displays the duplex mode; whether half-duplex or full-duplex</td>
</tr>
<tr>
<td>VLAN</td>
<td>Name of the VLAN</td>
</tr>
<tr>
<td>L2L3</td>
<td>Shows whether the port is in Layer 2 or Layer 3, switched or routed</td>
</tr>
<tr>
<td>Trunk Encapsulation</td>
<td>Shows whether ISL or IEEE 802.1Q encapsulation is enabled on the switch port</td>
</tr>
<tr>
<td>Trunk Mode</td>
<td>Trunk mode of the port. The trunk modes are desirable, on, off, auto, or no negotiate</td>
</tr>
</tbody>
</table>

### Performance Details

The following portlets are displayed under Performance Details pane:

- CPU Utilization
- Memory Utilization
- Environmental Temperature
- PathEcho Information
- IPSLA Statistics

### CPU Utilization

The CPU Utilization portlet displays information about CPU utilization percentage of the device managed in network for last one day or one hour.

Table 11-14 displays the color and the percentage of the CPU Utilization of the device.
Table 11-14  
**Color and Percentage of CPU Utilization of the Device**

<table>
<thead>
<tr>
<th>Color</th>
<th>CPU Utilization of the Device in Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>CPU Utilization of the device from 0 to 10%</td>
</tr>
<tr>
<td>Yellow</td>
<td>CPU Utilization of the device from 10 to 30%</td>
</tr>
<tr>
<td>Orange</td>
<td>CPU Utilization of the device from 30 to 80%</td>
</tr>
<tr>
<td>Red</td>
<td>CPU Utilization of the device from 80 to 100%</td>
</tr>
</tbody>
</table>

Table 11-15 lists the CPU Utilization portlet details.

Table 11-15  
**CPU Utilization Portlet Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Name</td>
<td>Instance which occupies the CPU at the particular period of time</td>
</tr>
<tr>
<td>Current Value (%)</td>
<td>Current value of CPU utilization percentage value in a device</td>
</tr>
<tr>
<td>Minimum (%)</td>
<td>Minimum CPU utilization percentage value in a device</td>
</tr>
<tr>
<td>Maximum (%)</td>
<td>Maximum CPU utilization percentage value in a device</td>
</tr>
<tr>
<td>Average (%)</td>
<td>Average CPU utilization percentage value in a device</td>
</tr>
<tr>
<td>HistoGraph</td>
<td>Displays an icon which when clicked displays the Histograph chart</td>
</tr>
<tr>
<td>LiveGraph</td>
<td>Displays an icon which when clicked displays the Livegraph chart</td>
</tr>
</tbody>
</table>

**Memory Utilization**

The Memory Utilization portlet displays information about Memory utilization percentage of the device managed in network for last one day or one hour.

Table 11-16 displays the color and the percentage of the Memory Utilization of the device.

Table 11-16  
**Color and Percentage of Memory Utilization of the Device**

<table>
<thead>
<tr>
<th>Color</th>
<th>Memory Utilization of the Device in Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Memory Utilization of the device from 0 to 50%</td>
</tr>
<tr>
<td>Yellow</td>
<td>Memory Utilization of the device from 50 to 70%</td>
</tr>
<tr>
<td>Orange</td>
<td>Memory Utilization of the device from 70 to 90%</td>
</tr>
<tr>
<td>Red</td>
<td>Memory Utilization of the device from 90 to 100%</td>
</tr>
</tbody>
</table>

Table 11-17 lists the Memory Utilization portlet details.

Table 11-17  
**Memory Utilization Portlet Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Name</td>
<td>Instance which occupies the Memory at the particular period of time</td>
</tr>
<tr>
<td>Current Value (%)</td>
<td>Current value of Memory utilization percentage value in a device</td>
</tr>
<tr>
<td>Minimum (%)</td>
<td>Minimum Memory utilization percentage value in a device</td>
</tr>
<tr>
<td>Maximum (%)</td>
<td>Maximum Memory utilization percentage value in a device</td>
</tr>
</tbody>
</table>
### Environmental Temperature

The Environmental Temperature portlet displays the temperature of the device managed in network for last one day or one hour.

Table 11-18 lists the Environmental Temperature portlet details.

#### Table 11-18  Environmental Temperature Portlet Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Name</td>
<td>Name of the instance for which the Environment Temperature to be monitored</td>
</tr>
<tr>
<td>Current Value</td>
<td>Current temperature value in the device</td>
</tr>
<tr>
<td>Minimum (°C)</td>
<td>Minimum temperature value in the device</td>
</tr>
<tr>
<td>Maximum (°C)</td>
<td>Maximum temperature value in the device</td>
</tr>
<tr>
<td>Average (°C)</td>
<td>Average temperature value in the device</td>
</tr>
<tr>
<td>HistoGraph</td>
<td>Displays an icon which when clicked displays the Histograph chart</td>
</tr>
<tr>
<td>LiveGraph</td>
<td>Displays an icon which when clicked displays the Livegraph chart</td>
</tr>
</tbody>
</table>

### PathEcho Information

PathEcho measures hop by hop latency in an IP network.

Select a target device from the Target drop-down list box in the PathEcho information portlet to display the PathEcho information. The PathEcho information portlet displays the hop by hop latency from the source device to the target device.

### IPSLA Statistics

Select a target device from the Target drop-down list box in the IPSLA Statistics portlet to display the IPSLA Statistics information.

The IPSLA Statistics portlet displays the information in Table 11-19.

#### Table 11-19  IPSLA Statistics Portlet Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector Name</td>
<td>Name of the collector for which the IPSLA Statistics is collected</td>
</tr>
<tr>
<td>Service Name</td>
<td>Name of the service for which the IPSLA Statistics is collected</td>
</tr>
<tr>
<td>Last Polled Time</td>
<td>Displays the time when the IPSLA Statistics was last collected</td>
</tr>
<tr>
<td>Latency (ms)</td>
<td>Displays the latency value in milliseconds</td>
</tr>
</tbody>
</table>
Troubleshooting Network Devices and Endhosts

Chapter 11      About Troubleshooting Tools

Troubleshooting Network Devices and Endhosts

Link Troubleshooting

The Link troubleshooting tab displays the details of a selected link from the topology map.

Link troubleshooting displays the following panes:

- Port Status — See Port Status for more information.
- Event and Faults — See Events and Faults for more information.
- Utilization and Errors — See Utilization and Errors for more information.

Port Status

The following portlets are displayed under Port Status pane:

- Port Details
- Configlet

Port Details

This pane summarizes the status of link ports of the device.

Table 11-20 describes the fields in the Port Status pane.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>IP addresses of the devices forming the link</td>
</tr>
<tr>
<td>Port</td>
<td>Port numbers of the devices forming the link</td>
</tr>
<tr>
<td>Port Description</td>
<td>Description of the port that you have entered</td>
</tr>
<tr>
<td>Type</td>
<td>Media type, such as Ethernet</td>
</tr>
</tbody>
</table>
Table 11-20  Port Status pane

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Port</td>
<td>Click this link to shutdown the port and then enable it. You can monitor</td>
</tr>
<tr>
<td></td>
<td>the changes in the Change Audit report (Reports &gt; Change Audit), if syslogs</td>
</tr>
<tr>
<td></td>
<td>are enabled in the device. When you click the Reset Port link, Inventory</td>
</tr>
<tr>
<td></td>
<td>is triggered for the device, and the status is updated from MIB. Click the</td>
</tr>
<tr>
<td></td>
<td>refresh icon in the portlet to get the data from database after a successful</td>
</tr>
<tr>
<td></td>
<td>inventory collection.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Administrative status of the port. This displays whether port has been</td>
</tr>
<tr>
<td></td>
<td>brought down intentionally.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Displays whether port is active or inactive.</td>
</tr>
<tr>
<td>Speed</td>
<td>Displays the link port speed.</td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Displays the duplex mode; whether half-duplex or full-duplex.</td>
</tr>
<tr>
<td>Protocol Enabled</td>
<td>Protocol enabled on the device. Example: IP, IPX</td>
</tr>
<tr>
<td>Protocol Seen</td>
<td>Protocol seen on the device. Example: IP, IPX</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN to which the port is a part.</td>
</tr>
<tr>
<td>L2L3</td>
<td>Shows whether the port is routed or switched.</td>
</tr>
<tr>
<td>isChannel</td>
<td>Shows whether the port is connected to another device, which is managed in</td>
</tr>
<tr>
<td></td>
<td>LMS.</td>
</tr>
<tr>
<td>Discrepancies Found</td>
<td>Displays the number of discrepancies found associated with the port. If</td>
</tr>
<tr>
<td></td>
<td>you click on the number, the Discrepancies report is launched.</td>
</tr>
<tr>
<td>Best Practice Deviations Found</td>
<td>Displays the number of best practice deviations found associated with the port. If you click on the value it launches, the Best Practice Deviations report is launched.</td>
</tr>
</tbody>
</table>

**Configlet**

LMS provides configlets to view the configurations on link ports. Each port has a separate configlet, which shows the CLI commands for particular services and features.

**Events and Faults**

The Events and Faults pane displays the following portlets:

- **Faults**
- **Syslogs**
Faults

This portlet summarizes the Fault details in the network link in the last one hour or one day. Table 11-21 describes the fields in the Fault Details portlet.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Fault Severity. This can be Critical, Informational, or Warning.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Identifier of the fault</td>
</tr>
<tr>
<td>Description</td>
<td>Description about the fault</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the fault; whether they are owned or cleared by the user</td>
</tr>
</tbody>
</table>

Few possible values for this field could be:
- Connectivity
- Environment
- Other
- Reachability
- Utilization

Duration         Time span between creation of faults and the current server time for the active or owned faults.

Time span between creation of faults and the time of clearing faults.

Last Occurrence  Date and time when the fault has occurred.

Syslogs

This portlet summarizes the Syslog details of the device managed in the network in the last one day or one hour. It displays the details for the selected interface. Table 11-22 describes the fields in the Syslogs portlet.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Number</td>
<td>Name or IP Address of the interface in that device generating the Syslog message.</td>
</tr>
<tr>
<td>Source</td>
<td>Name of the device generating the Syslog message.</td>
</tr>
<tr>
<td>Severity</td>
<td>Message severity level. LMS captures the following severity levels: Emergencies(0), Alerts (1), Critical (2), Errors (3).</td>
</tr>
<tr>
<td>Mnemonic</td>
<td>Code that uniquely identifies the error message. Note that older Catalyst messages do not display a mnemonic. An example of a mnemonic for an IOS message is CONFIG I.</td>
</tr>
<tr>
<td>Description</td>
<td>Syslog Message description.</td>
</tr>
</tbody>
</table>
**Table 11-22**  Syslog Details Portlet Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>Date and time the message was logged. This is the timestamp provided by the device. Syslog daemon provides a timestamp if the device does not send one.</td>
</tr>
<tr>
<td>Details</td>
<td>Name of the Syslog message. Displays a new window containing the Syslog message description. When you click on the User_URL icon, you are linked to a customized web page, if you have defined one; otherwise, it defaults to a sample Perl script for creating a user URL. When you click the '*' symbol, the description of the Syslog message is displayed.</td>
</tr>
</tbody>
</table>

**Utilization and Errors**

The Utilization and Errors pane displays the following portlets:

- Utilization
- Errors

**Utilization**

This portlet summarizes the Utilization details of the selected device interface managed in the network in the last one day or one hour.

*Table 11-23* describes the fields in the Utilization portlet.

**Table 11-23**  Utilization Portlet Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilization Parameter</td>
<td>Name of the utilization parameter of the selected interface monitored in the last one day or one hour</td>
</tr>
<tr>
<td>Minimum (%)</td>
<td>Minimum utilization percentage value in a device interface</td>
</tr>
<tr>
<td>Maximum (%)</td>
<td>Maximum utilization percentage value in a device interface</td>
</tr>
<tr>
<td>Average (%)</td>
<td>Average utilization percentage value in a device interface</td>
</tr>
<tr>
<td>HistoGraph</td>
<td>Displays an icon which when clicked displays the Histogram chart</td>
</tr>
<tr>
<td>LiveGraph</td>
<td>Displays an icon which when clicked displays the Livegraph chart</td>
</tr>
</tbody>
</table>

**Errors**

This portlet summarizes the Utilization error details of the selected device interface managed in the network in the last one day or one hour.
Table 11-24 describes the fields in the Utilization Errors portlet.

### Table 11-24  Utilization Errors Portlet Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilization Parameters</td>
<td>Name of the utilization parameter of the selected interface monitored in the last one day or one hour</td>
</tr>
<tr>
<td>Minimum (Pkts/s)</td>
<td>Minimum utilization error value in a device</td>
</tr>
<tr>
<td>Maximum (Pkts/s)</td>
<td>Maximum utilization percentage value in a device</td>
</tr>
<tr>
<td>Average (Pkts/s)</td>
<td>Average utilization percentage value in a device</td>
</tr>
<tr>
<td>HistoGraph</td>
<td>Displays an icon which when clicked displays the Histograph chart</td>
</tr>
<tr>
<td>LiveGraph</td>
<td>Displays an icon which when clicked displays the Livegraph chart</td>
</tr>
</tbody>
</table>

### Endhost Troubleshooting

The Endhost troubleshooting tab displays the details of a selected endhost.

Endhost troubleshooting displays the following panes:
- **End Host Status**— See **End Host Status** for more information.
- **Identity Status Details**— See **Identity Status Details** for more information.
- **EnergyWise Details**— See **EnergyWise Details** for more information.

### End Host Status

The End Host Status pane displays the following portlets:
- **User Tracking Report**
- **Ping the endhost from LMS Server**
- **Traceroute the endhost from LMS Server**

### User Tracking Report

This portlet summarizes the User Tracking details of the endhost collected from the network.

Table 11-25 describes the fields in the User Tracking portlet.

### Table 11-25  User Tracking Report Portlet Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>MAC Address of the endhost</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the endhost</td>
</tr>
<tr>
<td>Username</td>
<td>Username of the endhost</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname of the endhost</td>
</tr>
<tr>
<td>Switch</td>
<td>Name of the switch to which the endhost is connected</td>
</tr>
<tr>
<td>Switch IP Address</td>
<td>IP Address of the switch to which the endhost is connected</td>
</tr>
<tr>
<td>Port Name</td>
<td>Name of the switch port that is connected to the endhost</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the switch port that is connected to the endhost</td>
</tr>
</tbody>
</table>
Troubleshooting Network Devices and Endhosts

Table 11-25  User Tracking Report Portlet Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Speed</td>
<td>Switch port speed</td>
</tr>
<tr>
<td>VTP Domain</td>
<td>VTP domain name of the device where the endhost is connected</td>
</tr>
<tr>
<td>VLAN Details</td>
<td>Name of the VLAN</td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Displays the duplex mode; whether half-duplex or full-duplex</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of Medianet endpoint.</td>
</tr>
<tr>
<td>Location</td>
<td>Displays all the location attributes configured on the Medianet endpoints.</td>
</tr>
<tr>
<td></td>
<td>For more details, see Default Layout of Location Attributes.</td>
</tr>
</tbody>
</table>

You can customize the display of the location attributes using the medianet.properties file located at:

- For Windows — NMSROOT\lib\classpath
- For Solaris or Soft Appliance — /opt/CSCOpx/lib/classpath

LMS also has the medianet.properties.orig file with the default layout of the location attributes. You can use this file if the medianet.properties file gets corrupted. The location attributes that appear in the Endhost details popup vary according to the type of Medianet endpoint. For more details see, Customizing the Display of Location Attributes.

Note: This field appears only if the end host is a Medianet endpoint.

Customizing the Display of Location Attributes

When you move the mouse over the MAC address columns of the Medianet portlets, you can view the location attributes in the Endhost details popup. You can customize the display of the location attributes in this popup using the medianet.properties file located at:

- For Windows — NMSROOT\lib\classpath
- For Solaris or Soft Appliance — /opt/CSCOpx/lib/classpath

LMS also has the medianet.properties.orig file with the default layout of the location attributes. You can use this file if the medianet.properties file gets corrupted. If the medianet.properties file gets corrupted, you should take a copy of the medianet.properties.orig file and replace the corrupted medianet.properties file.

The location attributes that appear in the Endhost details popup vary according to the type of Medianet endpoint. See Sample Default medianet.properties File.

You can add any location attribute to any address line. By default, the address of the Medianet endpoint is five lines. If the you want to add or remove a line, you should change the value of the property MOUSEOVER.DMP.LOCATION.NUMBER_OF_LINES.

For example, to add the sixth line to the DMP endpoint address in the Endhost details popup, you should:

- Add MOUSEOVER.DMP.LINE6={1}, {2}.
- Modify the MOUSEOVER.DMP.LOCATION.NUMBER_OF_LINES to 6.

The numbers within the braces refer to the location attribute listed in the properties file. In this example, it is State and County, respectively. See Sample Default medianet.properties File.
If you choose to add a line in between, you need to modify the subsequent lines.
You can also move the mouse over the end host records in the search results and view the location attributes only for Medianet endpoints.

### Sample Default medianet.properties File

#### Location attributes order

```properties
# Location Attributes format for DMP Mouse Hover
MOUSEHOVER.DMP.LOCATION.NUMBER_OF_LINES=5
MOUSEHOVER.DMP.LINE1={14},
MOUSEHOVER.DMP.LINE2={17}, {18}, {19},
MOUSEHOVER.DMP.LINE3={25}, {9},
```

<table>
<thead>
<tr>
<th>SNo</th>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>State</td>
<td>National subdivision (state)</td>
</tr>
<tr>
<td>2</td>
<td>County</td>
<td>Land area of local government</td>
</tr>
<tr>
<td>3</td>
<td>City</td>
<td>City</td>
</tr>
<tr>
<td>4</td>
<td>City Division</td>
<td>City division</td>
</tr>
<tr>
<td>5</td>
<td>Neighborhood</td>
<td>Neighborhood</td>
</tr>
<tr>
<td>6</td>
<td>Street Group</td>
<td>Group of streets</td>
</tr>
<tr>
<td>7</td>
<td>Leading Street Direction</td>
<td>Leading street direction</td>
</tr>
<tr>
<td>8</td>
<td>Trailing Street Direction</td>
<td>Trailing street direction</td>
</tr>
<tr>
<td>9</td>
<td>Street Suffix</td>
<td>Street suffix</td>
</tr>
<tr>
<td>10</td>
<td>House</td>
<td>House number</td>
</tr>
<tr>
<td>11</td>
<td>Street Number</td>
<td>Street number suffix</td>
</tr>
<tr>
<td>12</td>
<td>Landmark</td>
<td>Landmark</td>
</tr>
<tr>
<td>13</td>
<td>Additional Location</td>
<td>Additional location information</td>
</tr>
<tr>
<td>14</td>
<td>Name</td>
<td>Name of the resident</td>
</tr>
<tr>
<td>15</td>
<td>Zipcode</td>
<td>Postal/Zip Code</td>
</tr>
<tr>
<td>16</td>
<td>Building</td>
<td>Building name</td>
</tr>
<tr>
<td>17</td>
<td>Unit</td>
<td>Unit</td>
</tr>
<tr>
<td>18</td>
<td>Floor</td>
<td>Floor number</td>
</tr>
<tr>
<td>19</td>
<td>Room</td>
<td>Room number</td>
</tr>
<tr>
<td>20</td>
<td>Place</td>
<td>Place type</td>
</tr>
<tr>
<td>21</td>
<td>PostalCommunity Name</td>
<td>Postal community name</td>
</tr>
<tr>
<td>22</td>
<td>PostOffice Box</td>
<td>PO Box</td>
</tr>
<tr>
<td>23</td>
<td>Additional Code</td>
<td>Additional code information</td>
</tr>
<tr>
<td>24</td>
<td>Seat</td>
<td>Seat number</td>
</tr>
<tr>
<td>25</td>
<td>Primary Road</td>
<td>Primary road or street name</td>
</tr>
<tr>
<td>26</td>
<td>Road Section</td>
<td>Road section name</td>
</tr>
<tr>
<td>27</td>
<td>Road Branch</td>
<td>Road branch name</td>
</tr>
<tr>
<td>28</td>
<td>Road SubBranch</td>
<td>Road sub-branch name</td>
</tr>
<tr>
<td>29</td>
<td>StreetName PreMod</td>
<td>Street pre modifier name</td>
</tr>
<tr>
<td>30</td>
<td>StreetName PostMod</td>
<td>Street post modifier name</td>
</tr>
<tr>
<td>31</td>
<td>Country Code</td>
<td>Country</td>
</tr>
</tbody>
</table>

---

If you choose to add a line in between, you need to modify the subsequent lines.
You can also move the mouse over the end host records in the search results and view the location attributes only for Medianet endpoints.

### Sample Default medianet.properties File

#### Location attributes order

```properties
# Location Attributes format for DMP Mouse Hover
MOUSEHOVER.DMP.LOCATION.NUMBER_OF_LINES=5
MOUSEHOVER.DMP.LINE1={14},
MOUSEHOVER.DMP.LINE2={17}, {18}, {19},
MOUSEHOVER.DMP.LINE3={25}, {9},
```

<table>
<thead>
<tr>
<th>SNo</th>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>State</td>
<td>National subdivision (state)</td>
</tr>
<tr>
<td>2</td>
<td>County</td>
<td>Land area of local government</td>
</tr>
<tr>
<td>3</td>
<td>City</td>
<td>City</td>
</tr>
<tr>
<td>4</td>
<td>City Division</td>
<td>City division</td>
</tr>
<tr>
<td>5</td>
<td>Neighborhood</td>
<td>Neighborhood</td>
</tr>
<tr>
<td>6</td>
<td>Street Group</td>
<td>Group of streets</td>
</tr>
<tr>
<td>7</td>
<td>Leading Street Direction</td>
<td>Leading street direction</td>
</tr>
<tr>
<td>8</td>
<td>Trailing Street Direction</td>
<td>Trailing street direction</td>
</tr>
<tr>
<td>9</td>
<td>Street Suffix</td>
<td>Street suffix</td>
</tr>
<tr>
<td>10</td>
<td>House</td>
<td>House number</td>
</tr>
<tr>
<td>11</td>
<td>Street Number</td>
<td>Street number suffix</td>
</tr>
<tr>
<td>12</td>
<td>Landmark</td>
<td>Landmark</td>
</tr>
<tr>
<td>13</td>
<td>Additional Location</td>
<td>Additional location information</td>
</tr>
<tr>
<td>14</td>
<td>Name</td>
<td>Name of the resident</td>
</tr>
<tr>
<td>15</td>
<td>Zipcode</td>
<td>Postal/Zip Code</td>
</tr>
<tr>
<td>16</td>
<td>Building</td>
<td>Building name</td>
</tr>
<tr>
<td>17</td>
<td>Unit</td>
<td>Unit</td>
</tr>
<tr>
<td>18</td>
<td>Floor</td>
<td>Floor number</td>
</tr>
<tr>
<td>19</td>
<td>Room</td>
<td>Room number</td>
</tr>
<tr>
<td>20</td>
<td>Place</td>
<td>Place type</td>
</tr>
<tr>
<td>21</td>
<td>PostalCommunity Name</td>
<td>Postal community name</td>
</tr>
<tr>
<td>22</td>
<td>PostOffice Box</td>
<td>PO Box</td>
</tr>
<tr>
<td>23</td>
<td>Additional Code</td>
<td>Additional code information</td>
</tr>
<tr>
<td>24</td>
<td>Seat</td>
<td>Seat number</td>
</tr>
<tr>
<td>25</td>
<td>Primary Road</td>
<td>Primary road or street name</td>
</tr>
<tr>
<td>26</td>
<td>Road Section</td>
<td>Road section name</td>
</tr>
<tr>
<td>27</td>
<td>Road Branch</td>
<td>Road branch name</td>
</tr>
<tr>
<td>28</td>
<td>Road SubBranch</td>
<td>Road sub-branch name</td>
</tr>
<tr>
<td>29</td>
<td>StreetName PreMod</td>
<td>Street pre modifier name</td>
</tr>
<tr>
<td>30</td>
<td>StreetName PostMod</td>
<td>Street post modifier name</td>
</tr>
<tr>
<td>31</td>
<td>Country Code</td>
<td>Country</td>
</tr>
</tbody>
</table>

---

If you choose to add a line in between, you need to modify the subsequent lines.
You can also move the mouse over the end host records in the search results and view the location attributes only for Medianet endpoints.
Ping the endhost from LMS Server

This portlet displays the output or result of pinging the endhost from the LMS Server and the ping statistics.

You can use the Test Now button to get the statistics and see the latest content of the portlet.

Traceroute the endhost from LMS Server

This portlet displays the output or result of tracerouting the device from the LMS Server and the ping statistics.

You can use the Test Now button to get the statistics and see the latest content of the portlet.
Identity Status Details

The Identity Status Details pane displays the following portlets:

- Identity Information from MAC History
- Identity Information from User History
- Identity Information for Switch Port

Identity Information from MAC History

This portlet summarizes the identity information from the MAC History reports.

Table 11-26 describes the fields in the Identity Information from MAC History portlet.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch IP Address</td>
<td>IP Address of the switch to which the endhost is connected to</td>
</tr>
<tr>
<td>Port Name</td>
<td>Port name in device to which a host is connected</td>
</tr>
<tr>
<td>Status</td>
<td>Authentication status success or failure</td>
</tr>
<tr>
<td>Type</td>
<td>Authentication type such as MAB, dot1x or webauth</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN name to which the device belongs to</td>
</tr>
<tr>
<td>DACL</td>
<td>Access Control Lists that you can download from the RADIUS server</td>
</tr>
<tr>
<td>Authentication time</td>
<td>Time of authenticating</td>
</tr>
</tbody>
</table>

Identity Information from User History

This portlet summarizes the identity information from the User History reports.

Table 11-27 describes the fields in the Identity Information from User History portlet.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch IP Address</td>
<td>IP Address of the switch to which the endhost is connected to</td>
</tr>
<tr>
<td>Port Name</td>
<td>Port name in device to which a host is connected</td>
</tr>
<tr>
<td>Status</td>
<td>Authentication status success or failure</td>
</tr>
<tr>
<td>Type</td>
<td>Authentication type such as MAB, dot1x or webauth</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN name to which the device belongs to</td>
</tr>
<tr>
<td>DACL</td>
<td>Access Control Lists that you can download from the RADIUS server</td>
</tr>
<tr>
<td>Authentication time</td>
<td>Time of authenticating</td>
</tr>
</tbody>
</table>
Identity Information for Switch Port

This portlet summarizes the identity information for Switch Port reports.

Table 11-28 describes the fields in the Identity Information for Switch Port portlet.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch IP Address</td>
<td>IP Address of the switch to which the endhost is connected to</td>
</tr>
<tr>
<td>Port Name</td>
<td>Port name in device to which a host is connected</td>
</tr>
<tr>
<td>Status</td>
<td>Authentication status success or failure</td>
</tr>
<tr>
<td>Type</td>
<td>Authentication type such as MAB, dot1x or webauth</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN name to which the device belongs to</td>
</tr>
<tr>
<td>DACL</td>
<td>Access Control Lists that you can download from the RADIUS server</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Time of authenticating</td>
</tr>
</tbody>
</table>

EnergyWise Details

The EnergyWise Details pane displays the Endhost EnergyWise Details portlet.

Endhost EnergyWise Details

This portlet summarizes the information of EnergyWise Details for the selected endhost.

Table 11-29 describes the fields in the Identity Information for Switch Port portlet.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Level</td>
<td>Displays the EnergyWise power level ranging from 0 to 10. The EnergyWise power level manages power usage consistently corresponding to the power status of the endhost.</td>
</tr>
<tr>
<td>Current Value (W)</td>
<td>Displays the current value of power in the endhost in units of Watts.</td>
</tr>
</tbody>
</table>

Using Troubleshooting Tools

This section contains:

- Using Management Station to Device Tool
- Using Ping
- Using Traceroute
- Proxy Ping
- Proxy Traceroute
- Using SNMP Walk
- Using SNMP Set
- Using Packet Capture
Using Management Station to Device Tool

To troubleshoot problems with un-managed or non-responding devices, you can check the device connectivity by protocol. The Management Station to Device tool helps you diagnose Layer 4 (application) connectivity problems.

Layer 4 tests include the key services Essentials needs to manage network devices: debugging and measurement tools (UDP and TCP), the web server (HTTP), file transfer (TFTP), the terminal (Telnet), and read-write access (SNMP).

Note

The Management Station to Device check will be done only for protocol connectivity. The credentials for the corresponding protocols will not be tested or verified.

If you enter a hostname instead of an IP address, the program performs Name Lookup to find out the address. This task will fail if it cannot find an address.

You can test:

- **UDP (echo test, port 7)**
  Sends an echo request to UDP port 7.

- **TCP (echo test, port 7)**
  Sends an echo request to TCP port 7.

- **HTTP (availability test, port 80)**
  Sends an HTTP request to the HTTP port 80 of the destination device.

- **TFTP (availability test, port 69; device must be configured as a TFTP server)**
  Sends a TFTP request to the TFTP port (69) of the destination device.

- **Telnet (service test, port 23)**
  Checks whether Telnet is enabled on the device and if the destination device responds to a Telnet request. It does not verify whether the Telnet password in the database works.
  Since Telnet runs on top of TCP, when Telnet succeeds, it means TCP is enabled on the device. If Telnet fails, there is no way to automatically determine if TCP is enabled or not. Perform a TCP test to check whether TCP is up or not.

- **SNMP (service test, port 161)**
  Sends an `snmp get` request to the destination device for an SNMP read test (SNMPR). It also sends an `snmp set` request to the device to test SNMP write (SNMPW). This protocol is supported for the versions of v1, v2c, and v3.

- **SSH (service test, port 22)**
  Checks whether SSH is enabled on the device. If the destination device responds to SSH requests, this also tests whether LMS Server can make SSH requests to that device. It does not verify the password in the database.

If you launch Management Station To Device with Network Operator/Help Desk privilege, device credential fetching fails and the fields of read/write community strings of SNMP v1/v2c, read/write SNMPv3 credentials are set to default values. You have to manually enter SNMP v1/v2c/v3 credentials.
To invoke Management Station to Device tool:

**Step 1** Select **Inventory > Tools > Device Center**.

**Step 2** Select a type of problem from the Problem Type drop-down list.

**Step 3** Follow the steps mentioned in **Using Device Center** to proceed with diagnosing devices.

The troubleshooting information for a device appears in a new tab in the form of portlets under the respective panes.

**Step 4** Click the Device Status pane.

**Step 5** Click **Management Station to Device** from the list of Quick Links.

The Management Station to Device dialog box appears.
Step 6  Select the connectivity applications you want to select.
All information you enter in the fields are case sensitive.
If you select SNMP v1/v2c, you should:
• Select either SNMP v1 or v2c. The default is SNMP v2c.
• Enter the Read Community String.
• Enter the Write Community String.
• Enter the Time out in seconds. The default is 2 seconds.
If you select SNMP v3 (NoAuthNoPriv security levels), enter the:
• Read Username.
• Write Username.
• Timeout (in seconds). The default value is 2 seconds.
If you select SNMP v3 (AuthNoPriv security levels), enter the:
• Read Username.
• Read Auth Password.
• Read Auth Protocol. Select MD5 or SHA from the drop-down list.
• Write Username.
• Write Auth Password.
• Write Auth Protocol. Select MD5 or SHA from the drop-down list.
• Timeout (in seconds). The default value is 2 seconds.
If you select SNMP v3 (AuthPriv security level), enter the:
• Read Username.
• Read Auth Password.
• Read Auth Protocol. Select MD5 or SHA from the drop-down list.
• Read Privacy Password.
• Read Privacy Protocol. Select a privacy protocol from the drop-down list. The list items are:
  – DES
  – 3DES
  – AES128
  – AES192
  – AES256
• Write Username.
• Write Auth Password.
• Write Auth Protocol. Select MD5 or SHA from the drop-down list.
• Write Privacy Password.
• Write Privacy Protocol. Select a privacy protocol from the drop-down list. The list items are:
  - DES
  - 3DES
  - AES128
  - AES192
  - AES256
• Timeout (in seconds). Default value is 2 seconds.
If you select SSH as the connectivity application, you should:
  • Select either SSH ver1 or SSH ver2.

**Step 7**
Enter the Timeout in seconds and click **OK**.
The default is 2 seconds.
The Interface Test Results popup displays the results. The Interface Details results screen shows the interfaces tested and the test results for each option.

---

**Note**
The read/write username and password for SNMPv3 and the read/write community string for SNMP v1/v2c are case sensitive.

---

**Using Ping**

Use the Ping tool to test whether the device is reachable. A **ping** tests an ICMP echo message and its reply. Since **ping** is the simplest test for a device, use it first.

You can view the packets transmitted, and received, percentage of packet loss, and round-trip time in milliseconds. If **ping** fails, try using **traceroute**.

See **Ping device from LMS Server** and **Proxy Ping** for more details.

---

**Using Traceroute**

Use the Traceroute tool to detect routing errors between the network management station and the target device.

Traceroute helps you understand why **ping** fails or why applications time out. It does this by diagnosing TCP/IP Layer 3 (transport) problems. You can view each hop (or gateway) on the route to your device and how long each hop took.

See **Traceroute device from LMS Server** and **Proxy Traceroute** for more details.
Proxy Ping

Proxy Ping allows you to ping another device or server from the selected device and displays the ping output.

To do a proxy ping:

**Step 1** Select **Inventory > Tools > Device Center**.
**Step 2** Select Device Center.
**Step 3** Follow the steps mentioned in **Using Device Center** to proceed with diagnosing devices.
   The troubleshooting information for a device appears in a new tab in the form of portlets under the respective panes.
**Step 4** Click the Tools Menu from the Device Status pane.
**Step 5** Click **Proxy Ping**.
**Step 6** Enter the IP Address of the device or server to be pinged in the Proxy Ping dialog box.
**Step 7** Click the Proxy Ping button.
   The ping statistics are displayed on the text area in the Proxy Ping dialog box.

Proxy Traceroute

Proxy Traceroute displays the output of traceroute of the device or server from the selected device.

To do a proxy traceroute:

**Step 1** Select **Inventory > Tools > Device Center**.
**Step 2** Select Device Center.
**Step 3** Follow the steps mentioned in **Using Device Center** to proceed with diagnosing devices.
   The troubleshooting information for a device appears in a new tab in the form of portlets under the respective panes.
**Step 4** Click the Tools Menu from the Device Status pane.
**Step 5** Click **Proxy Traceroute**.
**Step 6** Enter the IP Address of the device or server to be pinged in the Proxy Traceroute dialog box.
**Step 7** Click the Proxy Traceroute button.
   The Traceroute statistics are displayed on the text area in the Proxy Traceroute dialog box.
Using SNMP Walk

SNMP Walk allows you to trace the MIB tree of a device starting from a given OID for troubleshooting, or gathering information about a certain device.

You should have System Administrator privileges to use this feature.

To use SNMP Walk:

**Step 1** Select **Inventory > Tools > Device Center**.

**Step 2** Select Device Center.

**Step 3** Follow the steps mentioned in Using **Device Center** to proceed with diagnosing devices.

The troubleshooting information for a device appears in a new tab in the form of portlets under the respective panes.

**Step 4** Click the Tools Menu from the Device Status pane.

**Step 5** Click **SNMP Walk**.

The SNMP Walk dialog box appears.

**Step 6** Enter the IP address or DNS name.

**Step 7** Select the SNMP Version to be used.

For SNMP Version 1 and 2c (if it is a 64-bit counter, use SNMP v2):

a. Enter the Read community string.

For SNMP Version 3 (NoAuthNoPriv and AuthNoPriv security levels):

a. Enter the SNMPv3 Username.

b. Enter the SNMPv3 Auth Password.

c. Specify the SNMP v3 Auth Protocol. Select either the MD5 radio button or the SHA radio button.

d. Enter the SNMP Context Name. This is optional.

For SNMP Version 3 (AuthPriv Security level):

a. Enter the SNMPv3 Username.

b. Enter the SNMPv3 Auth Password.

c. Specify the SNMP v3 Auth Protocol. Select either the MD5 radio button or the SHA radio button.

d. Enter the Privacy Password.

e. Select a Privacy Protocol from the drop-down list. The available items are:

   - DES
   - 3DES
   - AES128
   - AES192
   - AES256

f. Enter the SNMP Context Name. This is optional.

**Step 8** Enter the starting OID (optional). If you leave this field blank, the tool will start from 1.

**Step 9** Enter the SNMP Timeout. The default value is 10 seconds.
Step 10 Select the Output OIDs Numerically check box to print the output OIDs numerically. This is optional. By default, the corresponding name of the OID is printed in the output window.

Step 11 Select the Output Indexes Numerically check box to show the output index numerically. This is optional.

Step 12 Select the Debug check box to enable the debugging option. This is optional.

Note All the fields are case-sensitive.

Step 13 Click OK to get the results.

The results will be based on the parameters you entered. When the walk is complete, you can save it as text. A full walk may take a long time.

The read/write username and password for SNMPv3 and the read/write community string for SNMP v1/v2c are case sensitive. The SNMP walk dialog box displays the credentials (SNMP v1/v2c/v3) for the device from Device Credential Repository, if these are available. Otherwise, the default values for the respective SNMP versions are displayed.

If you launch SNMP Walk feature with Network Operator/Help Desk privilege, device credential fetching fails and the fields of read/write community strings of SNMP v1/v2c, read/write SNMPv3 credentials are set to default values.

You have to manually enter SNMP v1/v2c/v3 credentials.

Using SNMP Set

You can use this option to set an SNMP object or multiple objects on a device for controlling the device. You should have System Administrator privileges to use this feature.

To use SNMP set:

Step 1 Select Inventory > Tools > Device Center.

Step 2 Select Device Center.

Step 3 Follow the steps mentioned in Using Device Center to proceed with diagnosing devices.

The troubleshooting information for a device appears in a new tab in the form of portlets under the respective panes.

Step 4 Click the Tools Menu from the Device Status pane.

The SNMP set dialog box appears.

Step 5 Enter the IP address or the DNS name.
**Step 6**  Select the SNMP Version.

For SNMP Version 1 and 2c (if it is a 64-bit counter, use SNMP v2):

a. Enter the Read/Write community string.

b. Enter the object ID that you want to set along with the instance ID or number.

c. Select the Object Type from the drop-down list. The available values are:
   - Integer
   - Unsigned Integer
   - TimeTicks
   - IP Address
   - Object ID
   - String
   - Hex String
   - Decimal String

d. Enter a new value. This depends on the Object Type you specify.

For SNMP Version 3 (NoAuthNoPriv and AuthNoPriv security levels):

a. Enter the SNMPv3 Username.

b. Enter the SNMPv3 Auth Password.

c. Specify the SNMPv3 Auth Protocol. Select either the MD5 radio button or the SHA radio button.

d. Enter the object ID that you are trying to set along with the instance ID or number.

e. Select the Object Type from the drop-down list. The available items are:
   - Integer
   - Unsigned Integer
   - TimeTicks
   - IP Address
   - Object ID
   - String
   - Hex String
   - Decimal String
   - Bits
   - Unsigned 64-bit Integer
   - Signed 64-bit Integer

f. Enter a new value. This depends on the Object Type you specify.

g. Enter the SNMPv3 Context Name. This is optional.

For SNMP Version 3 (AuthPriv Security level):

a. Enter the SNMPv3 Username.

b. Enter the SNMPv3 Auth Password.

c. Specify the SNMP v3 Auth Protocol. Select either the MD5 radio button or the SHA radio button.

d. Enter the Privacy Password.
e. Select a Privacy Protocol from the drop-down list. The available items are:
   - DES
   - 3DES
   - AES128
   - AES192
   - AES256

f. Enter the object ID that you are trying to set along with the instance ID or number.

g. Select the Object Type from the drop-down list. The available items are:
   - Integer
   - Unsigned Integer
   - TimeTicks
   - IP Address
   - Object ID
   - String
   - Hex String
   - Decimal String
   - Bits
   - Unsigned 64-bit Integer
   - Signed 64-bit Integer

h. Enter a new value. This depends on the Object Type you specify.

i. Enter the SNMPv3 Context Name. This is optional.

Step 7 Enter the SNMP Timeout. The default is 10 seconds.

Step 8 Select the debug check box to enable the debugging option.

Step 9 Click Next if you wish to add more SNMP objects on the device.

The SNMP Set dialog box appears.

Step 10 Fill in all required fields and click Next. Repeat this until you have added as many objects as you want.

Step 11 Click OK to get the results.

The results will be based on the parameters you entered. After you have completed setting the SNMP objects, you can save it as text and mail the output.

The read/write username and password for SNMPv3 and the read/write community string for SNMP v1/v2c are case sensitive. The SNMP Set dialog box displays the credentials (SNMP v1/v2c/v3) for the device from Device and Credential Repository, if these are available. Otherwise, the default values for the respective SNMP versions will be displayed.

If you launch SNMP Set feature with Network Operator/Help Desk privilege, device credential fetching fails and the fields of read/write community strings of SNMP v1/v2c, read/write SNMPv3 credentials are set to default values.

You have to manually enter SNMP v1/v2c/v3 credentials.
Using Packet Capture

The Packet Capture tool can be used to capture live data from the LMS machine to aid in troubleshooting. You should have System Administrator privileges to use this feature.

**Note**

WinPcap must be installed to use this feature on Windows machines. The executable is available at: \NMSROOT\objects\jet\bin\winpcap.exe, where \NMSROOT\ is the LMS Installation Directory.

To capture the data from a machine:

**Step 1**
Select **Inventory > Tools > Device Center**.

**Step 2**
Select Device Center.

**Step 3**
Follow the steps mentioned in **Using Device Center** to proceed with diagnosing devices.

The troubleshooting information for a device appears in a new tab in the form of portlets under the respective panes.

**Step 4**
Click the Tools Menu from the Device Status pane.

**Step 5**
Click **Packet Capture**.

The Packet Capture dialog box appears.

A list of archived capture files is displayed. If no capture files are archived, then this dialog box displays that there are no records.

**Step 6**
Click **Create** in the Packet Capture dialog box.

The Packet Capture Inputs dialog box appears with the default values.

**Step 7**
Enter the following information:

- **Interface**
  If you have multiple interfaces on the machine, you must first select the interface that you want to use for the capture.

- **Address**
  This field accepts one or more addresses (separated by a single space). This value is used to locate the LMS machine in the network while capturing the packet.

- **Protocols and Ports or Applications (for data capture)**
  You can capture the data using either:

  - **Protocols and Ports**
    By default, the packets are captured from the specified machine using the Protocol/Port Selection.

    You may select this option if you know the number of the port.

    Select the protocols, **TCP**, **UDP**, or **ICMP**, you want to include in the capture.

    Select **Any** to include all three protocols (TCP, UDP, ICMP). By default, the TCP Protocol is selected.

    You can enter the list of ports to capture data for TCP and UDP. The Port(s) field accepts one or more TCP or UDP ports separated by a single space. If you specify port without specifying the addresses in the Address field, the data is captured for that port for all the active devices.
Or
- Applications
  Click the Applications radio button and select from a preconfigured list of common LMS applications and standard applications, if you want to capture data using applications.

- Cycle
  You must specify when to stop the packet capture. You can terminate the capture after:
  - A certain period time.
  - The filter has captured a certain amount of data.
  - A certain number of packets have been captured.
  By default, capture cycles stop after 60 seconds.

Step 8 Click OK.

The Packet Capture status popup appears with the current status of the capture. If you click OK with the default values (without setting any of the parameters) the screen will try to capture for the next 60 seconds.

After the capture is performed, the Packet Capture dialog box displays the new packet capture file along with the list of the archived capture files.

If you click Stop Capture in the popup, the capture stops. The packet capture information till then is added in the Packet Capture dialog box, among the archive files.

Step 9 Click on the new packet capture file link to get a sniffer output of packets received by the LMS Server.

The result can be opened in any sniffer application, such as Ethereal. These files are in binary libpcap format with a .jet extension. You can download these files directly through your web browser and e-mail them to the Cisco TAC for further analysis.

To delete an existing packet capture file:

Step 1 Select Inventory > Tools > Device Center.
Step 2 Select Device Center.
Step 3 Follow the steps mentioned in Using Device Center to proceed with diagnosing devices.

The troubleshooting information for a device appears in a new tab in the form of portlets under the respective panes.

Step 4 Click the Tools Menu from the Device Status pane.
Step 5 Click Packet Capture.

The Packet Capture dialog box appears.

Step 6 Select the Packet Capture file you want to delete.
Step 7 Click Delete in the Packet Capture dialog box.

The file is removed from the list of archived capture files.
Troubleshooting VRF

Network administrators can verify the end-to-end connectivity of the VRF configured devices using the Troubleshooting feature. You can check the device reachability of VRF configured devices participating in a VRF.

This section contains:

- Ping or Traceroute
- Show Results

Ping or Traceroute

The following section explains the usage of Ping or Traceroute command in VRF.

- Ping
  
The ping command allows you to check the VRF connectivity between the source device and the destination device that are a part of the selected VRF, at various locations on the network. OR Ping is used to check the accessibility of devices in a VRF configured network.
  
The ping command sends an echo request out to a remote device (part of the selected VRF) at an IP address that you specify. If the destination interfaces is not reachable, the packets are lost and displays if the packets have succeeded or failed.
  
  Ping is used to check the accessibility of devices in a VRF configured network. You can test the device reachability from the Source to the Destination device.

- Traceroute
  
  Displays a list of the routes traversed by the data packet to reach the Destination device in a particular VRF.

Only the following users can troubleshoot VRFs:

- Network Operator
- Network Administrator
- System Administrator

To use Ping or Traceroute:

Step 1

Click the Troubleshooting Tab in the VRF home page.

The Ping or Traceroute page appears with Ping or Traceroute option selected by default.
Step 2  Enter the required information as given in Table 11-30.

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Represents the process used to troubleshoot VRF Operation are:</td>
<td>Click the process you want to run for troubleshooting the devices</td>
</tr>
<tr>
<td></td>
<td>Ping</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Traceroute</td>
<td></td>
</tr>
<tr>
<td>Enable Bi-directional</td>
<td>Enables Bi-directional troubleshooting for Traceroute only. This option does not support Ping command.</td>
<td>Check the Enable Bi-directional Ping check box to enable bi-directional Traceroute</td>
</tr>
</tbody>
</table>

**Source Device**

<table>
<thead>
<tr>
<th>Source Device</th>
<th>Source Device details.</th>
<th>Select a device using Select. A Device Selector appears on the screen.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Click Select to select the VRF configured device you want to troubleshoot.</td>
<td>• Click the radio button to select the devices listed in the device selector.</td>
</tr>
<tr>
<td></td>
<td>The Device Selector dialog box appears in the Device selector window.</td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>Or</td>
<td>• Enter the Source device name.</td>
</tr>
<tr>
<td></td>
<td>• Enter the Source Device details.</td>
<td>If you enter first four characters, it populates ten device names.</td>
</tr>
</tbody>
</table>

**VRF Details**

<table>
<thead>
<tr>
<th>VRF</th>
<th>Displays the VRFs configured in all devices on the network. The details provided are from the global table.</th>
<th>From the VRF drop-down list, choose the VRF you want to troubleshoot.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you select Global Table, the global table is used for troubleshooting with all the interfaces, that are not assigned to any VRF, will be populated in the Source and Destination Interface fields.</td>
<td></td>
</tr>
</tbody>
</table>

**Destination Device**

<table>
<thead>
<tr>
<th>Destination Device</th>
<th>Comprises the combination of:</th>
<th>Select the devices using the Device Selector.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• VRF configured devices, specific to the VRF selected in the VRF drop-down list and</td>
<td>• Click the radio button to select the device in the groups listed and click Select.</td>
</tr>
<tr>
<td></td>
<td>• Excludes the Source Devices</td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
<td>• Enter the Destination device name.</td>
</tr>
<tr>
<td></td>
<td>Consider device A and B as VRF configured devices where device B is configured with VRF Name as Red.</td>
<td>If you enter the first four characters, it suggests the device names.</td>
</tr>
<tr>
<td></td>
<td>If you select Device A from the source and VRF Red from the VRF drop-down list, the Device Selector of the Destination Device, displays only Device B.</td>
<td></td>
</tr>
</tbody>
</table>
Step 3  Click **Ping or Traceroute** to run the Troubleshooting process.

---

**Sample Ping**

cmx-uranus#ping vrf GreenVRF 10.77.22.2 source 10.77.22.3  
Primary Login Succeeded / Primary Enable Succeeded

Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.77.22.2, timeout is 2 seconds:  
Packet sent with a source address of 10.77.22.3.!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms PE3745-L3-2#  
****************************************************************************************

**Understanding Ping Commands**
The following VRF configuration details are pushed in the selected devices. The description of the VRF configuration details is given in Table 11-31.

---

### Table 11-30 Ping or Traceroute Settings (continued)

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Details</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Source Interface | Displays all the interfaces in the Source device.  
If you select a source interface, data packets will be routed through the selected source interface to execute Ping command. | From the Source Interface drop-down list, choose the Source interface |
| Destination Interface | Displays all interfaces connected to the Destination device | From the Destination Interface drop-down list, choose the Destination interface |
| View Command | Displays the command used to: Ping or Traceroute | Click **View Command** to view the commands used to Ping or Traceroute |
| Monitor Real Time | Enables you to view the real-time status of the interfaces of the VRF-configured devices.  
The details about the real-time status is retrieved using IPSLA and the status is displayed in a graphical format. | Click **Monitor Real Time** |
| Ping or Traceroute | Ping or Traceroute command is executed. | Click **Ping or Traceroute** |
| Result | Shows the result of VRF-Lite Troubleshooting processes- Ping or Traceroute. | Display only. |
| Reset | Resets the details provided to Ping or Traceroute. | Click **Reset** |
| Clear Result | Clears the result displayed in Result field of Ping or Traceroute page | Click **Clear Result** to clear the result |
Troubleshooting VRF

**Show Results**

Show Results page displays the result of the VRF-specific show commands. For example, you can get the output of

`show ip route vrf <selected vrf> <selected protocol>`

To use Show Results:

**Step 1**
Click the Troubleshooting Tab in the Virtual Network Manager home page. The Ping or Traceroute page appears.

**Step 2**
Select **Troubleshooting > Show Results**. The Show Results page appears.

**Step 3**
Enter the required information as given in **Table 11-32**.

---

### Table 11-31 Ping Command details

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ping vrf vrf-name ip-address</code></td>
<td>Pings an IP Address that has a specific VRF</td>
</tr>
<tr>
<td><code>ping destination interface source source interface</code></td>
<td>Allows you to enter the interface configuration mode and specify the Layer 3 interface to be associated with the VRF. The interface can be a routed port or SVI.</td>
</tr>
</tbody>
</table>
### Table 11-32 Settings in Show Results

<table>
<thead>
<tr>
<th>Window Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Device</td>
<td>Source Device details.</td>
<td>Select a device using <strong>Select</strong>. A Device Selector appears on the screen.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Select</strong> to select the VRF configured device you want to troubleshoot.</td>
<td>• Click the radio button to select the devices listed in the device selector.</td>
</tr>
<tr>
<td></td>
<td>The Device Selector window appears.</td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>• Enter the Source device name.</td>
<td>• Enter the Source device name.</td>
</tr>
<tr>
<td></td>
<td>Or</td>
<td>If you enter first four characters, it populates ten device names.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Select</strong> to select the VRF configured device you want to troubleshoot.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Device Selector window appears.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter the Source device name.</td>
<td></td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>Represents the Routing Protocols used to troubleshoot VNM. The Routing protocols used are:</td>
<td>Click the Routing Protocol you want to use to troubleshoot the devices.</td>
</tr>
<tr>
<td></td>
<td>• OSPF</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EIGRP</td>
<td></td>
</tr>
<tr>
<td>View Command</td>
<td>Displays the show command specific to a VRF.</td>
<td>Click <strong>View Command</strong> to view the show commands specific to a VRF</td>
</tr>
<tr>
<td></td>
<td>• For OSPF, the commands used are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>show ip protocol vrf vrf name</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>show ip OSPF</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For EIGRP, the commands used are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>show ip eigrp vrf vrf name neighbors</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Here, neighbor refers to the neighboring devices that participate in a VRF.</td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting VRF

Sample of Show Results

cmx-uranus# show ip eigrp vrf Green neighbors
Primary Login Succeeded
/ Primary Enable Succeeded

IP-EIGRP neighbors for process 65
PE3745-L3-2#
********************************************************************************

Understanding Commands in Show Results

The following VRF configuration details are fetched from selected devices. The description of the VRF show results details is given in Table 11-33.

Table 11-33  Show Results details

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip vrf vrf-name</td>
<td>Displays the set of VRFs and interfaces</td>
</tr>
<tr>
<td>show ip route vrf vrf-name</td>
<td>Displays the IP routing table for a VRF</td>
</tr>
<tr>
<td>show ip protocols vrf vrf-name</td>
<td>Displays the routing protocol information associated with the VRF</td>
</tr>
<tr>
<td>show ip OSPF</td>
<td>Verifies the configuration of the OSPF network</td>
</tr>
<tr>
<td>show ip eigrp vrf vrf-name neighbor</td>
<td>Displays the Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors that are on the interfaces and part of the specified VRF instance. It is also used to debug certain type of transport problems.</td>
</tr>
</tbody>
</table>
Embedded Event Manager (EEM)

This chapter consists of the following:

- What is EEM?
- Components of Cisco IOS EEM
- Types of Actions
- Support for EEM

What is EEM?

EEM (Embedded Event Manager) is an IOS technology that runs on the control plane of the Cisco Catalyst 6500 device. This EEM technology is integrated with Cisco IOS Software and because of this, the Cisco IOS Software, EEM is aware of the state of the network from the perspective of the device on which it is operating. The Cisco Catalyst 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches also support EEM.

This intelligence, combined with the programmability of EEM, provides a powerful facility that can be leveraged in many ways. It is a combination of processes designed to monitor key system parameters such as:

- CPU Utilization
- Interface Errors
- Counters
- SNMP Events
- Syslog Events
- Diagnostics Events

After monitoring the system parameters, EEM acts on specific events or thresholds or counters that are exceeded.

The Cisco IOS Software Infrastructure allows triggering pre-programmed local actions when specific events are detected. Cisco IOS Software Embedded Event Manager, harnesses network intelligence through event detectors and takes action according to pre-defined policies. This results in greater manageability, control, and resiliency.

The EEM is a framework to monitor and detect certain conditions that might impact network services. It includes methods to program corrective actions when incorrect events are detected.
Components of Cisco IOS EEM

The Cisco IOS EEM consists of two components:

- **Event Detectors**
  Cisco IOS Software EEM event detectors provide an interface between the monitored agent and the action policies. Event detectors determine that a particular event has occurred and notify the event manager.

- **Policy Engines**
  Policy engines are the methods of programming in EEM. There are two policy engines:
  - Cisco IOS Software CLI Applet interface
  - TCL subsystem and interpreter.

A policy consists of an event trigger coupled with some defined action. A policy must be registered with one of these two policy engine facilities.

After a policy is registered, the event manager invokes the policy after the corresponding event detector detects the trigger event. Policies reference environment variables to determine the specifics of particular events.

Types of Actions

There are two types of events and actions that you can configure on the Cisco IOS Catalyst 6500, 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches:

- **Applets**
  An applet is a simple policy that is defined within the CLI configuration. It is a combination of events and actions. You can use it to define simple policies that are triggered by specific events.

- **TCL Scripts**
  You can create extensive policies using the script policy engine. You can develop TCL-based policies that interact with Cisco IOS Software using CLI commands and a set of environment variables.

  A TCL policy when registered, becomes an event subscriber. After a registered event is detected, the EEM server will trigger all corresponding event subscribers interested in this particular event.
You cannot deploy TCL scripts using TFTP, RCP and SCP protocols using Embedded Event Manager task.

**Support for EEM**

You can use LMS EEM functionality to configure the following on Cisco Catalyst 6500, 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches:

- Environmental Variables
- Applets
- TCL Scripts

You can use LMS NetConfig EEM-specific tasks to configure the EEM-specific scripts, applets and variables on the devices managed by LMS.

This section consists of:

- LMS NetConfig Tasks for EEM
- Configuring EEM Using LMS
- EEM and LMS Reports
- EEM and LMS NetShow
- EEM Show Commands
- EEM Syslogs

**LMS NetConfig Tasks for EEM**

You can configure EEM scripts, applets, or variables using NetConfig tasks available for this purpose. The EEM-specific NetConfig tasks are:

- EEM Environmental Variables Task
- Embedded Event Manager Task

**EEM Environmental Variables Task**

You can use this task to configure EEM Environmental Variables (that are used by the TCL script) on Cisco Catalyst 6500, 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches.

For more details, see the Configuration Online help.

You can enter the details for this task in the Environmental Variables Configuration dialog box. To invoke this dialog box, see the Configuration Online help.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see the Configuration Online help.
The fields in the EEM Environmental Variables Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IOS Parameters</strong></td>
<td></td>
</tr>
<tr>
<td><strong>EEM Environmental Variables</strong></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Select either:</td>
</tr>
<tr>
<td></td>
<td>• Add - to add one or more variables.</td>
</tr>
<tr>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>• Remove - to remove one or more variables.</td>
</tr>
<tr>
<td>Variable Name</td>
<td>Enter the name for the variable.</td>
</tr>
<tr>
<td></td>
<td>Example: my_counter</td>
</tr>
<tr>
<td></td>
<td>You can create a maximum of five variables at a time. If you want to create more variables, create another instance by clicking Add Instance Button.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter the value for the variable.</td>
</tr>
<tr>
<td></td>
<td>Example: 15</td>
</tr>
<tr>
<td></td>
<td>Now the variable my_counter will have the value 15.</td>
</tr>
<tr>
<td>Applicable Devices</td>
<td>Allows you to view the IOS devices in your selection, to which these variables would be applied.</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the information you have specified.</td>
</tr>
<tr>
<td>Reset</td>
<td>Clears all fields and reverts to the default setting.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Ignores your changes.</td>
</tr>
</tbody>
</table>

**Embedded Event Manager Task**

You can use this task to configure EEM Scripts or Applets on Cisco Catalyst 6500, 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches.

For more details, see the Configuration Online help.

You can enter the details for this task in the Embedded Event Manager Configuration dialog box. (To invoke this dialog box, see the Starting a New NetConfig Job topic in Configuration Online help.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see the Understanding the System-defined Task User Interface (Dialog Box) topic in Configuration Online help.

The fields in the Embedded Event Manager Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IOS Parameters</strong></td>
<td></td>
</tr>
<tr>
<td><strong>EEM Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Policy Type</td>
<td>Select either Script or Applet as the policy.</td>
</tr>
<tr>
<td>Action</td>
<td>Select Register or Unregister to register or unregister a script or applet.</td>
</tr>
</tbody>
</table>
### Device Directory Options

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New Directory</td>
<td>Check this option if you want to create a new directory on the device to copy the applet or script. If you select this check box, the input given in the Directory Name textbox is used to create a new directory. This option is activated only when the Script Policy and Register Action options are selected.</td>
</tr>
<tr>
<td>Directory Name</td>
<td>Enter the absolute path of the directory where the file needs to be placed on the device. <strong>Example:</strong> <code>disk0:/Testing</code> Here a new directory Testing is created in the device under disk0 Partition. Ensure that the selected directory has enough space before the script files are copied. This option is activated only when the Script Policy and Register Action options are selected.</td>
</tr>
</tbody>
</table>

### Upload Script/Applet files from Server

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| Files                 | Use this option to either:  
  • Enter the file location to upload the scripts to deploy on the device. Ensure that you enter the absolute path along with the filename. You can specify multiple filenames separated by commas.  
  Or  
  • Browse to the directory and select one or more scripts to deploy on the device.  
    - Use CTRL to select more than one file.  
    - Use **Browse** to browse to the directory. You cannot combine tcl files and applet files in a single NetConfig task. |
| Applicable Devices    | Allows you to view the IOS devices in your selection, to which the scripts or applets apply. |
| Save                  | Saves the information you have specified. |
| Reset                 | Clears all fields and reverts to the default setting. |
| Cancel                | Ignores your changes. |

### Configuring EEM Using LMS

You can configure the following using LMS NetConfig Tasks:

- Environmental Variables, see Configuring Environmental Variables
- Embedded Event Manager, see Configuring Embedded Event Manager
Configuring Environmental Variables

To configure Environmental Variables using LMS:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <strong>Configuration &gt; NetConfig &gt; NetConfig Jobs</strong>. The NetConfig Job Browser appears.</td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Create</strong>. The Devices and Tasks dialog box appears.</td>
</tr>
<tr>
<td>3</td>
<td>Click <strong>Create</strong>. Select the devices from the Device Selector pane. For more information on Device Selector, see the Admin Online help.</td>
</tr>
<tr>
<td>4</td>
<td>Select the Environmental Variables task, using the Task Selector.</td>
</tr>
<tr>
<td>5</td>
<td>Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>6</td>
<td>Select <strong>Environmental Variables</strong> from the Applicable Tasks pane and click <strong>Add Instances</strong>. The Environmental Variables Configuration dialog box appears. For more information on the fields in the Environmental Variables Configuration dialog box, see <a href="#">Embedded Event Manager Task</a>.</td>
</tr>
<tr>
<td>7</td>
<td>Set the parameters in the task dialog box and click <strong>Save</strong>. To reset the values that you have selected click <strong>Reset</strong>. Click <strong>Cancel</strong> to return to the previous dialog box, without saving your changes. You will see the instance of the task in the Added Tasks pane of the Add Tasks dialog box. The instance appears in this format: <code>Taskname_n</code>, where <code>Taskname</code> is the name of the task you have added, and <code>n</code> is the number of the instance. For example, the first instance of a Environmental Variables task is <code>Environmental Variables_1</code>. You can add as many instances as required, for a task.</td>
</tr>
<tr>
<td>8</td>
<td>Click <strong>Next</strong>. The Job Schedule and Options dialog box appears with these panes:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td>Allows you to schedule the job.</td>
</tr>
<tr>
<td>Job Options</td>
<td>Allows you to set the job options.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td>Select the run type or frequency for the job—Immediate, Once, Daily, Weekly, Monthly, or Last Day of Month. If Job Approval is enabled, the Immediate option is not available.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the start date for the job.</td>
</tr>
</tbody>
</table>
### Step 10
Set the job options, in the Job Options pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>at</td>
<td>Select the start time for the job from the hour and minute drop-down lists.</td>
</tr>
</tbody>
</table>

**Job Info**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Description</td>
<td>Enter the Job Description. Enter unique descriptions to help you to identify jobs easily. This is mandatory.</td>
</tr>
</tbody>
</table>
| E-mail        | Enter e-mail addresses to which the job will send status notices. Separate multiple addresses with commas or semicolons. You must configure the SMTP server to send e-mails (Admin > System > System Preferences).
If the user who has created the job has a valid e-mail address, an e-mail notification is sent with the user address in the sender address field, when job is started and completed.
If the user who has created the job does not have a valid e-mail address, then the notification e-mails will be sent with the sender address field blank.
Notification e-mails include a URL that displays the job details (see Viewing Job Details for more information about what details are displayed). If you are not logged in, you must log in using the provided login panel to view the job details. |
| Comments      | Enter your comments for the job. Comments appear in the work order of the job and are stored in the configuration archive. |
| Approver Comments | Enter comments for the Job Approver. This field is displayed only if you have enabled Job Approval for NetConfig. |
| Maker E-mail  | Enter the e-mail-ID of the job creator. This field is displayed only if you have enabled Job Approval for NetConfig. This is a mandatory field. |

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail on Mismatch of Config Versions</td>
<td>Causes the job to be considered as failed when the most recent configuration version in the configuration archive is not identical to the most recent configuration version that was in the configuration archive when you created the job.</td>
</tr>
<tr>
<td>Sync Archive before Job Execution</td>
<td>Causes the job to archive the running configuration before making configuration changes.</td>
</tr>
<tr>
<td>Copy Running Config to Startup</td>
<td>Causes the job to write the running configuration to the startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.</td>
</tr>
</tbody>
</table>

**Enable Job Password**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Username</td>
<td>Enter the Login username. This option is available if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.</td>
</tr>
<tr>
<td>Login Password</td>
<td>Enter the Login password. This option is available if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.</td>
</tr>
</tbody>
</table>
### Enable Password
Enter the Enable password. This option is available if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.

### Failure Policy
Select one of these options to specify what the job should do if it does not run on a device.

- **Stop on failure:**
  If the job does not run on a device, the job is stopped. The database is updated only for the devices on which the job was run successfully.

- **Ignore failure and continue**
  If the job fails on a device, the job skips the device and continues running on the remaining devices. The database is updated only for the devices on which the job was run successfully.

- **Rollback device and stop**
  Rolls back the changes on the failed device and stops the job.

- **Rollback device and continue**
  Rolls back the changes on the failed device and continues the job.

- **Rollback job on failure**
  Rolls back the changes on all devices and stops the job. Roll back configuration changes to failed device or all devices configured by job.

### Execution
Specify the order in which the job should run on the devices.

- **Parallel**
  Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time.

- **Sequential**
  Allows the job to run on only one device at a time. If you select sequential execution, you can click **Set Device Order** to set the order of the devices. In the Device Ordering dialog box:
  
  a. Select a device name
  
  b. Click **Move Up** or **Move Down** to change its place in the order.
  
  c. Click **OK** to save the current order and close the dialog box
  
  or
  
  Click **Cancel** to close the dialog box without making any changes.

---

**Step 11**
Click **Device Order** to view the device order.

The Set Device Order pop-up appears. You can reset the order in which the job should be run on the devices using the Up and Down arrows.

**Step 12**
Click **Done** after re-ordering the devices.

The pop-up closes.
Step 13  Click Next.

The Job Work Order dialog box appears with information about the job, the job policies, the job approval
details (if you have enabled Job Approval), the device details, and the task. It also displays details of the
CLI commands that will be run on the selected devices as part of this job.

Step 14  Click Finish after you review the details of your job in the Job Work Order dialog box.

A notification message appears along with the Job ID. The newly created job appears in the NetConfig
Job Browser.

Configuring Embedded Event Manager

To configure Embedded Event Manager scripts or applets using LMS:

Step 1  Select Configuration > NetConfig > NetConfig Jobs.

The NetConfig Job Browser appears.

Step 2  Click Create.

The Devices and Tasks dialog box appears.

Step 3  Select the devices from the Device Selector pane.

See the Admin Online help for more details on Device Selector.

Step 4  Select the Embedded Event Manager Task, using the Task Selector.

Step 5  Click Next.

Step 6  Select Embedded Event Manager from the Applicable Tasks pane and click Add Instances.

The Embedded Event Manager Configuration dialog box appears.

For more information on the fields, see EEM Environmental Variables Task.

Step 7  Set the parameters in the Task dialog box and click Save.

To reset the values that you have selected click Reset. Click Cancel to return to the previous dialog box,
without saving your changes.

You will see the instance of the task in the Added Tasks pane of the Add Tasks dialog box. The instance
appears in this format:

Taskname_n, where Taskname is the name of the task you have added, and n is the number of the
instance. For example, the first instance of a Embedded Event Manager task is Embedded Event
Manager_1.

You can add as many instances as required, for a task.

Step 8  Click Next.

The Job Schedule and Options dialog box appears with these panes:

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td>Allows you to schedule the job.</td>
</tr>
<tr>
<td>Job Options</td>
<td>Allows you to set the job options.</td>
</tr>
</tbody>
</table>
Step 9  Set the schedule for the job, in the Scheduling pane:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>Select the run type or frequency for the job—Immediate, Once, Daily, Weekly, or Last Day of Month. If Job Approval is enabled, the Immediate option is not available.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the start date for the job.</td>
</tr>
<tr>
<td>at</td>
<td>Select the start time for the job from the hour and minute drop-down lists.</td>
</tr>
<tr>
<td>Job Info</td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter the Job Description. Enter unique descriptions to help you to identify jobs easily. This is mandatory.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job will send status notices. Separate multiple addresses with commas or semicolons. You must configure the SMTP server to send e-mails (Admin &gt; System &gt; System Preferences). If the user who has created the job has a valid e-mail address, an e-mail notification is sent with the user’s address in the sender address field, when job is started and completed. If the user who has created the job does not have a valid e-mail address, then the notification e-mails will be sent with the sender address field blank. Notification e-mails include a URL that displays the job details (see Viewing Job Details for the more information about what details are displayed). If you are not logged in, you must log in using the provided login panel to view the job details.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter your comments for the job. Comments appear in the work order of the job and are stored in the configuration archive.</td>
</tr>
<tr>
<td>Approver Comments</td>
<td>Enter comments for the Job Approver. This field is displayed only if you have enabled Job Approval for NetConfig.</td>
</tr>
<tr>
<td>Maker E-mail</td>
<td>Enter the e-mail-ID of the job creator. This field is displayed only if you have enabled Job Approval for NetConfig. This is a mandatory field.</td>
</tr>
</tbody>
</table>

Step 10  Set the job options, in the Job Options pane:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail on Mismatch of Config Versions</td>
<td>Causes the job to be considered as failed when the most recent configuration version in the configuration archive is not identical to the most recent configuration version that was in the configuration archive when you created the job.</td>
</tr>
<tr>
<td>Sync Archive before Job Execution</td>
<td>Causes the job to archive the running configuration before making configuration changes.</td>
</tr>
<tr>
<td>Copy Running Config to Startup</td>
<td>Causes the job to write the running configuration to the startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Job Password</td>
<td></td>
</tr>
<tr>
<td>Login Username</td>
<td>Enter the Login username. This option is available if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.</td>
</tr>
<tr>
<td>Login Password</td>
<td>Enter the Login password. This option is available if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the Enable password. This option is available if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.</td>
</tr>
<tr>
<td>Failure Policy</td>
<td>Select one of these options to specify what the job should do if it fails to run on a device.</td>
</tr>
<tr>
<td></td>
<td>• Stop on failure:</td>
</tr>
<tr>
<td></td>
<td>If the job does not run on a device, the job is stopped. The database is updated only for the devices on which the job was run successfully.</td>
</tr>
<tr>
<td></td>
<td>• Ignore failure and continue</td>
</tr>
<tr>
<td></td>
<td>If the job fails on a device, the job skips the device and continues running on the remaining devices. The database is updated only for the devices on which the job was run successfully.</td>
</tr>
<tr>
<td></td>
<td>• Rollback device and stop</td>
</tr>
<tr>
<td></td>
<td>Rolls back the changes on the failed device and stops the job.</td>
</tr>
<tr>
<td></td>
<td>• Rollback device and continue</td>
</tr>
<tr>
<td></td>
<td>Rolls back the changes on the failed device and continues the job.</td>
</tr>
<tr>
<td></td>
<td>• Rollback job on failure</td>
</tr>
</tbody>
</table>
|                       |   Rolls back the changes on all devices and stops the job. Roll back configuration changes to failed device or all devices configured by job.
Support for EEM

Chapter 12  Embedded Event Manager (EEM)

EEM and LMS Reports

You can use LMS Custom Reports along with Syslogs to generate Embedded Event Manager reports. Before you generate reports, you need to configure those devices on which EEM is configured, to send Syslog messages to the LMS server.

Each device sends out Syslog messages after running each EEM policy. You can identify the EEM Syslog messages, based on their facility names. The facility names for EEM Syslog messages will consist of HA_EM.

You can use the Syslog Embedded Event Manager Custom report to ascertain the results of the scripts run on each device.

Field | Description
--- | ---
Execution | Specify the order in which the job should run on the devices.

- **Parallel**
  Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time.

- **Sequential**
  Allows the job to run on only one device at a time. If you select sequential execution, you can click **Set Device Order** to set the order of the devices.

In the Device Ordering dialog box:

1. Select a device name
2. Click **Move Up** or **Move Down** to change its place in the order.
3. Click **OK** to save the current order and close the dialog box
   or
   Click **Cancel** to close the dialog box without making any changes.

Step 11  Click **Device Order** to view the device order.

The Set Device Order pop-up appears. You can reset the order in which the job should run on the devices using the Up and Down arrows.

Step 12  Click **Done** after re-ordering the devices.

The pop-up closes.

Step 13  Click **Next**.

The Job Work Order dialog box appears with the information about the job, the job policies, the Job Approval details (if you have enabled Job Approval), the device details, the task. It also displays details of the CLI commands that will be run on the selected devices as part of this job.

Step 14  Click **Finish** after you review the details of your job in the Job Work Order dialog box.

A notification message appears along with the Job ID. The newly created job appears in the NetConfig Job Browser.
To generate this custom report, see the Reports Online help. The fields in the generated Syslog EEM Custom Report are given below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device generating the Syslog message.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name or IP Address of the interface in that device generating the Syslog message.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Time when the Syslog message was generated.</td>
</tr>
<tr>
<td>Facility/Sub Facility</td>
<td>Displays the facility or sub-facility codes. A facility is a hardware device, a protocol, or a module of the system software. See System Error Messages in the Cisco IOS Reference manual, for a predefined list of system facility codes. A sub-facility is the sub-facility in the device that generates the Syslog message.</td>
</tr>
</tbody>
</table>
| Severity          | Displays the message severity levels. Representations for the severity codes are:  
|                   | 0—Emergencies  
|                   | 1—Alerts  
|                   | 2—Critical  
|                   | 3—Errors  
|                   | 4—Warnings  
|                   | 5—Notifications  
|                   | 6—Informational |
| Mnemonics         | Codes that uniquely identifies an error message. Example: LOG |
| Description       | Description of each Syslog message. |
| Details           | Other details for each Syslog message. |
EEM and LMS NetShow

LMS NetShow allows you to generate reports based on various commandsets. You can use LMS NetShow to generate a Report on the EEM Configurations on Each Device.

Report on the EEM Configurations on Each Device

Use LMS NetShow to view the EEM configurations on each device.

The commandset which is used for this purpose is Show Embedded Event Manager Info. This commandset consists of the following commands:

- `show event manager policy available`
- `show event manager policy registered`
- `show event manager environment all`
- `show event manager policy pending`
- `show event manager directory user policy`

To generate this report:

1. Select Configuration > NetConfig > NetConfig Jobs.
2. The NetShow Job Browser window appears.
3. Click Create.
   The Select Devices and Commandsets window appears.
4. Select the devices from the Device Type Selector.
5. Select Show Embedded Event Manager Info commandset from the Commandset List
   You can enter custom commands in the Custom Commands text area if required.
6. Click Next to continue.
   The Set Schedule Options dialog box appears.
**Step 6** Enter the following information in the Set Schedule Options dialog box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>The Run Type of the job. The Run Types could be any or all of these, depending on the type of the job:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs the job immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Once at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>• 6-hourly—Every 6 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>• 12-hourly—Every 12 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Daily—Daily at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly—Weekly on the day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Monthly—Monthly on the day of the month and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Last day of Month—On the last day of the month at the specified time.</td>
</tr>
<tr>
<td>Date</td>
<td>Scheduled date and time of the job.</td>
</tr>
<tr>
<td><strong>Job Information</strong></td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter the Job Description. This is mandatory. Enter unique descriptions to help you to identify jobs easily.</td>
</tr>
<tr>
<td></td>
<td>You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter the e-mail addresses to which the job sends messages at the beginning and at the end of the job.</td>
</tr>
<tr>
<td></td>
<td>You can enter multiple e-mail addresses; separate these addresses by commas.</td>
</tr>
<tr>
<td></td>
<td>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences).</td>
</tr>
<tr>
<td></td>
<td>We recommend that you configure the LMS Server E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences).</td>
</tr>
<tr>
<td></td>
<td>When the job starts or completes, an e-mail is sent with the LMS Server E-mail ID as the sender's address.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter your comments for the job. Comments appear in the work order of the job.</td>
</tr>
</tbody>
</table>
Support for EEM

Chapter 12  Embedded Event Manager (EEM)

Step 7  Click Next.

The View Job Work Order page appears with the Job Work Order.

The Job Work Order contains general information on the job and on:

• Job policies.
• Job Approval details (if you have enabled Job Approval).
• Device details.
• Command sets and the commands to be run.

Step 8  Click Finish after you review the details of your job in the Job Work Order.

A message appears, \textit{Job ID created successfully}.

The newly created job appears in the NetShow Job Browser.

If your job failed and you want to run the same job, click Retry and perform steps 7 through 9 above.

Step 9  Click on the Job ID to view the results of the NetShow job created.
**EEM Show Commands**

See the Configuration Online help for configuring the NetConfig Show Commands job for devices that supports EEM.

**EEM Syslogs**

See the Reports Online help for the steps to generate EEM Syslogs report.
Generic OnLine Diagnostics (GOLD)

This chapter consists of the following:

- **What is GOLD?**
- **Types of Diagnostics**
- **Support for GOLD Tests**

## What is GOLD?

GOLD (Generic OnLine Diagnostics) is a device-specific IOS feature with fault detection capabilities. It defines a common framework for diagnostic operations across Cisco platforms running Cisco IOS Software.

**Note**

Only Cisco Catalyst 6500 (IOS), 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches are supported.

It provides:

- Fault Detection framework
- Proactive Diagnostics to detect hardware and software failures

The GOLD framework specifies the platform-independent fault-detection architecture for centralized and distributed systems.

The platform-specific diagnostics provide hardware-specific fault-detection tests and take corrective action in response to diagnostics test results.

### Diagnostics Operations

GOLD implementation checks the health of hardware components and verifies proper operation of the system data and control planes. Some tests take effect when the system starts, whereas other tests take effect when the system is running.
Types of Diagnostics

The diagnostics performed by GOLD (Generic OnLine Diagnostics) are:

- Boot-Up Diagnostics
- Runtime Monitoring

Boot-Up Diagnostics

A booting module goes through a series of checks before coming online. This allows the system to detect faults in the hardware components at boot-up time and helps to ensure that a failing module is not introduced in a live network.

When boot-up diagnostics detect a diagnostics failure on a Cisco Catalyst 6500 Series, the failing modules are shut down.

As an administrator, you can enable or disable the boot-level diagnostics. If you enable the boot level diagnostics, you can set the diagnostics levels to either Complete or Minimal. See GOLD Boot Level Task for more information.

Runtime Monitoring

Defects are also diagnosed during system operation or runtime. A series of diagnostics checks can be enabled to determine the condition of an online system. You must take care to distinguish between disruptive and non-disruptive diagnostics tests.

Although non-disruptive tests occur in the background and do not affect the system data or control planes, disruptive tests do affect live packet flows and should be scheduled during special maintenance windows.

The Runtime monitoring tests consist of Health-monitoring Diagnostics Tests

Health-monitoring Diagnostics Tests

Health-monitoring diagnostics tests are non-disruptive, and they run in the background while the system is in operation. The role of online diagnostics health monitoring is to proactively detect hardware failures in the live network environment and inform appropriate entities of a failure.

Health-monitoring tests do not affect system performance. However, the software restricts the health-monitoring interval to a minimum threshold to prevent affecting the CPU performance.

When health monitoring tests detect several consecutive failures, they can reset a module. By default, health-monitoring tests include:

- Data verification
- Control Plane verification
- Verification of proper function of hardware registers
Support for GOLD Tests

You can use LMS to configure the following on Cisco Catalyst 6500, 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E Switches:

- Bootup Diagnostics
- Health Monitoring Diagnostics

You can use LMS NetConfig Gold-specific tasks to configure the diagnostic tests on the Cisco Catalyst 6500 IOS switches, Cisco Catalyst 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches managed by LMS.

This section consists of:

- LMS NetConfig Tasks for GOLD Tests
- Configuring GOLD Tests using LMS
- GOLD Tests and LMS Reports
- GOLD Tests and LMS NetShow

LMS NetConfig Tasks for GOLD Tests

You can configure GOLD tests using NetConfig tasks available for this purpose. The GOLD-specific NetConfig tasks are:

- GOLD Boot Level Task
- GOLD Monitoring Test Task
- GOLD Health Monitoring Test Task

GOLD Boot Level Task

You can use this task to configure Boot Level Diagnostic tests on the following device category:

- Cisco Catalyst 6500 devices

For more details, see the NetConfig System-Defined Tasks Supported by the Device Categories topic under the Configuration Online help.

You can enter the details for this task in the GOLD Boot Level Configuration dialog box. (To invoke this dialog box, see the Starting a New NetConfig Job topic under the Configuration Online help.

For the features of system-defined tasks and a description of a system-defined task dialog box, see the Understanding the System-defined Task User Interface (Dialog Box) under the Configuration Online help.

The fields in the GOLD Bootup Level Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Select either Enable to enable the actions or Disable to disable the actions</td>
</tr>
<tr>
<td>Level</td>
<td>Select either Complete to set the boot level to Complete or Minimal to set the boot level to Minimal This option is activated only if the Action option is enabled. This option is not activated, if you have selected Disable in the Action field.</td>
</tr>
</tbody>
</table>
Support for GOLD Tests

Chapter 13      Generic OnLine Diagnostics (GOLD)

Support for GOLD Tests

GOLD Monitoring Test Task

You can use this task to configure GOLD Monitoring tests on the following device categories:
- Cisco Catalyst 6500 IOS switches
- Cisco Catalyst 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E Switches

For more details, see the NetConfig System-Defined Tasks Supported by the Device Categories topic under the Configuration Online help.

You can enter the details for this task in the GOLD Boot Level Configuration dialog box. (To invoke this dialog box, see the Starting a New NetConfig Job topic under the Configuration Online help.

For the features of system-defined tasks and a description of a system-defined task dialog box, see the Understanding the System-defined Task User Interface (Dialog Box) under the Configuration Online help.

The fields in the GOLD Monitoring Test Configuration dialog box are:

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves the information you have specified.</td>
</tr>
<tr>
<td>Reset</td>
<td>Clears all fields and reverts to the default setting.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Ignores your changes.</td>
</tr>
</tbody>
</table>

### GOLD Monitoring Test Task

You can use this task to configure GOLD Monitoring tests on the following device categories:
- Cisco Catalyst 6500 IOS switches
- Cisco Catalyst 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E Switches

For more details, see the NetConfig System-Defined Tasks Supported by the Device Categories topic under the Configuration Online help.

You can enter the details for this task in the GOLD Boot Level Configuration dialog box. (To invoke this dialog box, see the Starting a New NetConfig Job topic under the Configuration Online help.

For the features of system-defined tasks and a description of a system-defined task dialog box, see the Understanding the System-defined Task User Interface (Dialog Box) under the Configuration Online help.

The fields in the GOLD Monitoring Test Configuration dialog box are:

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOLD Monitoring Test Config</td>
<td>Select any of the following:</td>
</tr>
<tr>
<td>Action</td>
<td>- Add Interval - To add an interval</td>
</tr>
<tr>
<td></td>
<td>- No Interval. - To not to add an interval</td>
</tr>
<tr>
<td></td>
<td>- No Change - No change to the Action</td>
</tr>
<tr>
<td>Enter Vendor Type or Name</td>
<td>Enter the Vendor type or Module Name. You can enter one or more comma separated module names. Example: cevCat6kVsS72010G This is a mandatory field and is available only if you select Cisco Catalyst 6500 devices.</td>
</tr>
<tr>
<td>Enter Switch ID</td>
<td>Enter the Switch ID. You can enter a single switch ID or a number of switch IDs separated by comma. Example 1: Enter 2 if you want to include switch with ID 2. Example 2: Enter 3, 6 if you want to include switches with IDs 3 and 6. This is a mandatory field and is available only if you select Cisco Catalyst 2900XL, 2970, 2960, 3550, 3560, 3750, or 3750E stack switches.</td>
</tr>
</tbody>
</table>
### Support for GOLD Tests

#### Enable/Disable Health Monitoring Diagnostics Test

**Action**
- **Enable** - To start the Health Monitoring tests
- **Disable** - To stop the running Health Monitoring tests.
  - The tests once stopped, will not start again until the Action is enabled.
- **No Change** - No change to Action

#### Test Details

- **All**
  - Allows you to configure all diagnostic tests.

- **Enter Testnames**
  - Allows you to manually enter the test names.
  - Enter one or more test names separated by comma.
  - This option is activated only if the Enable Action is selected.

- **Range**
  - Allows you to enter a range for tests to be run.
  - This option is activated only if the Enable Action is selected.
  - Example:
    - Enter 2-8 if you want to run tests with IDs from 2 to 8.

#### Configure Health Monitoring Interval

- **No. of Days**
  - Enter the number of days till which you require the tests to be run on the devices.
  - The number of days can be any value between 0 - 20.
  - The default value is 1 day.

- **Hours**
  - Select the hour frequency at which the tests should be run. You can enter any value between 00 and 23 for hour.
  - This is a mandatory field and is enabled only if you have selected Add Interval.

- **Minutes**
  - Select the minute frequency at which the tests should be run. You can enter any value between 00 and 59 for the minute.
  - This is a mandatory field and is enabled only if you have selected Add Interval.

- **Seconds**
  - Enter the seconds frequency at which the tests should be run. You can enter any value between 00 and 59 for the second.
  - This is a mandatory field and is enabled only if you have selected Add Interval.

- **Milliseconds**
  - Enter the millisecond frequency at which the tests should be run. You can enter any value between 0 and 999 for the second.
  - This is a mandatory field and is enabled only if you have selected Add Interval.

- **Applicable Devices**
  - Allows you to view the IOS devices in your selection that you want to monitor with GOLD Monitoring Tests.

- **Save**
  - Saves the information you have specified.

- **Reset**
  - Clears all fields and reverts to the default setting.

- **Cancel**
  - Ignores your changes.
**GOLD Health Monitoring Test Task**

You can use this task to configure GOLD Health Monitoring tests on Cisco Catalyst 6500 IOS switches device categories.

This task is available only for the Module-based netconfig job wizard.

You can enter the details for this task in the GOLD Boot Level Configuration dialog box. (To invoke this dialog box, see the *Starting a New NetConfig Job* topic under the Configuration Online help.

You can enter the details of this task in the Gold Health Monitoring Test Configuration dialog box. To invoke this dialog box, see *Create a NetConfig Job based on Module or Port*.

The fields in the GOLD Health Monitoring Test Configuration dialog box are:

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GOLD Health Monitoring Test Configuration</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Configuring Health-Monitoring Diagnostics for Cat6k Devices</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Select any of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Run Test</strong> - To run a test</td>
</tr>
<tr>
<td></td>
<td>- <strong>Add Test</strong> - To add a test</td>
</tr>
<tr>
<td></td>
<td>- <strong>Remove Test</strong> - To remove a test</td>
</tr>
<tr>
<td><strong>Test Details</strong></td>
<td></td>
</tr>
<tr>
<td><strong>All</strong></td>
<td>Allows you to configure all diagnostic tests.</td>
</tr>
<tr>
<td><strong>Pre-defined</strong></td>
<td>Allows you to select the following pre-defined tests:</td>
</tr>
<tr>
<td></td>
<td>- TestLoopback</td>
</tr>
<tr>
<td></td>
<td>- TestNetflowInlineRewrite</td>
</tr>
<tr>
<td></td>
<td>- TestEobcStressPing</td>
</tr>
<tr>
<td></td>
<td>- TestFirmwareDiagStatus</td>
</tr>
<tr>
<td></td>
<td>- TestAsicSync</td>
</tr>
<tr>
<td><strong>Enter Testnames</strong></td>
<td>Allows you to manually enter the test names. Enter one or more test names separated by comma.</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td>Allows you to enter a range for tests to be run.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Enter 2-8 if you want to run tests with IDs from 2 to 8.</td>
</tr>
<tr>
<td><strong>Configure Health Monitoring Interval</strong></td>
<td></td>
</tr>
<tr>
<td><strong>No. of Days</strong></td>
<td>Enter the number of days till which you require the tests to be run on the devices.</td>
</tr>
<tr>
<td></td>
<td>The number of days can be any value between 0 - 20.</td>
</tr>
<tr>
<td></td>
<td>The default value is one day.</td>
</tr>
<tr>
<td></td>
<td>This field is enabled only if you have selected <strong>Add Test</strong>.</td>
</tr>
<tr>
<td><strong>Hours</strong></td>
<td>Select the hour frequency at which the tests should be run. You can enter any value between 00 and 23 for the hour.</td>
</tr>
<tr>
<td></td>
<td>This field is enabled only if you have selected <strong>Add Test</strong>.</td>
</tr>
</tbody>
</table>
Chapter 13  Generic OnLine Diagnostics (GOLD)

Support for GOLD Tests

Configuring GOLD Tests using LMS

You can configure the following GOLD Tests using LMS NetConfig:

- GOLD Boot Level Tests, see Configuring GOLD Boot Level Tests
- GOLD Monitoring Tests, see Configuring GOLD Monitoring Tests
- GOLD Health Monitoring Tests, see Configuring GOLD Health Monitoring Tests

Configuring GOLD Boot Level Tests

To configure GOLD tests using LMS:

Step 1  Select Monitor > Diagnostic Tools > Generic Online Diagnostics > Configure.

The Devices and Tasks dialog box appears.

Step 2  Select the devices from the Device Selector pane.
Step 3  Select the GOLD Boot Level task, using the Task Selector.

Step 4  Click Next.

The Add Tasks dialog box appears.

Step 5  Select **GOLD Boot Level** from the Applicable Tasks pane and click **Add Instances**.

The GOLD Boot Level Configuration dialog box appears. For more information on the fields in the GOLD Boot Level Configuration dialog box, see **GOLD Boot Level Task**.

Step 6  Set the parameters in the task dialog box and click **Save**.

To reset the values that you have selected click **Reset**. Click **Cancel** to return to the previous dialog box, without saving your changes.

You will see the instance of the task in the Added Tasks pane of the Add Tasks dialog box. The instance appears in this format:

\[ \text{Taskname}_n, \text{where Taskname is the name of the task you have added, and } n \text{ is the number of the instance. For example, the first instance of a GOLD Boot Level task is } \text{Gold Boot Level}_1. \]

You can add as many instances as required, for a task.

Step 7  Click **Next**.

The Set Schedule Options dialog box appears with these panes:

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td>Allows you to schedule the job.</td>
</tr>
<tr>
<td>Job Options</td>
<td>Allows you to set the job options.</td>
</tr>
</tbody>
</table>
Step 8  Set the schedule for the job, in the Scheduling pane:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>Select the frequency at which the job should be run—Immediate, Once, Daily, Weekly, Monthly, or Last Day of Month. If Job Approval is enabled, the Immediate option is not available.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the start date for the job.</td>
</tr>
<tr>
<td>at</td>
<td>Select the start time for the job from the hour and minute drop-down lists.</td>
</tr>
<tr>
<td>Job Info</td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter the Job Description. Enter unique descriptions to help you to identify jobs easily. This is mandatory.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job will send status notices. Separate multiple addresses with commas or semicolons. You must configure the SMTP server to send e-mails (&lt;Admin &gt; System &gt; System Preferences). If the user who has created the job has a valid e-mail address, an e-mail notification is sent with the user’s address in the sender address field, when job is started and completed. If the user who has created the job does not have a valid e-mail address, then the notification e-mails will be sent with the sender address field blank. Notification e-mails include a URL that displays the job details. If you are not logged in, you must log in using the provided login panel to view the job details.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter your comments for the job. Comments appear in the work order of the job and are stored in the configuration archive.</td>
</tr>
<tr>
<td>Approver Comments</td>
<td>Enter comments for the Job Approver. This field is displayed only if you have enabled Job Approval for NetConfig.</td>
</tr>
<tr>
<td>Maker E-mail</td>
<td>Enter the e-mail-ID of the job creator. This field is displayed only if you have enabled Job Approval for NetConfig. This is a mandatory field.</td>
</tr>
</tbody>
</table>

Step 9  Set the job options, in the Job Options pane:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail on Mismatch of Config Versions</td>
<td>Causes the job to be considered as failed when the most recent configuration version in the configuration archive is not identical to the most recent configuration version that was in the configuration archive when you created the job.</td>
</tr>
<tr>
<td>Sync Archive before Job Execution</td>
<td>Causes the job to archive the running configuration before making configuration changes.</td>
</tr>
<tr>
<td>Copy Running Config to Startup</td>
<td>Causes the job to write the running configuration to the startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.</td>
</tr>
</tbody>
</table>
Support for GOLD Tests

Chapter 13  Generic OnLine Diagnostics (GOLD)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Job Password</strong></td>
<td></td>
</tr>
<tr>
<td>Login Username</td>
<td>Enter the Login username. This option is available if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.</td>
</tr>
<tr>
<td>Login Password</td>
<td>Enter the Login password. This option is available if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the Enable password. This option is available if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.</td>
</tr>
</tbody>
</table>
Support for GOLD Tests

Chapter 13  Generic OnLine Diagnostics (GOLD)

Step 10  Click Device Order to view the device order.

The Set Device Order pop-up appears. You can reset the order in which the job should be run on the devices using the Up and Down arrows.

Step 11  Click Done after re-ordering the devices.

The pop-up closes.

Step 12  Click Next.

The Job Work Order dialog box appears with information about the job policies, the job approval details (if you have enabled Job Approval), the device details, and the task. It also displays details of the CLI commands that will be run on the selected devices as part of this job.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Policy</td>
<td>Select one of these options to specify what the job should do if it does not run on a device.</td>
</tr>
<tr>
<td></td>
<td>• Stop on failure:</td>
</tr>
<tr>
<td></td>
<td>If the job does not run on a device, the job is stopped. The database is updated only for the devices on which the job was run successfully.</td>
</tr>
<tr>
<td></td>
<td>• Ignore failure and continue</td>
</tr>
<tr>
<td></td>
<td>If the job fails on a device, the job skips the device and continues running on the remaining devices. The database is updated only for the devices on which the job was run successfully.</td>
</tr>
<tr>
<td></td>
<td>• Rollback device and stop</td>
</tr>
<tr>
<td></td>
<td>Rolls back the changes on the failed device and stops the job.</td>
</tr>
<tr>
<td></td>
<td>• Rollback device and continue</td>
</tr>
<tr>
<td></td>
<td>Rolls back the changes on the failed device and continues the job.</td>
</tr>
<tr>
<td></td>
<td>• Rollback job on failure</td>
</tr>
<tr>
<td></td>
<td>Rolls back the changes on all devices and stops the job. Roll back configuration changes to failed device or all devices configured by job.</td>
</tr>
<tr>
<td>Execution</td>
<td>Specify the order in which the job should run on the devices.</td>
</tr>
<tr>
<td></td>
<td>• Parallel</td>
</tr>
<tr>
<td></td>
<td>Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time.</td>
</tr>
<tr>
<td></td>
<td>• Sequential</td>
</tr>
<tr>
<td></td>
<td>Allows the job to run on only one device at a time. If you select sequential execution, you can click Set Device Order to set the order of the devices. In the Device Ordering dialog box:</td>
</tr>
<tr>
<td></td>
<td>a. Select a device name</td>
</tr>
<tr>
<td></td>
<td>b. Click Move Up or Move Down to change its place in the order.</td>
</tr>
<tr>
<td></td>
<td>c. Click OK to save the current order and close the dialog box or</td>
</tr>
<tr>
<td></td>
<td>Click Cancel to close the dialog box without making any changes.</td>
</tr>
</tbody>
</table>
Step 13  Click **Finish** after you review the details of your job in the Job Work Order dialog box. A notification message appears along with the Job ID. The newly created job appears in the NetConfig Job Browser.

---

**Configuring GOLD Monitoring Tests**

To configure GOLD Monitoring tests using LMS:

**Step 1** Select **Configuration > Tools > NetConfig > NetConfig Jobs**. The NetConfig Job Browser appears.

**Step 2** Click **Create**. The Job Flow Type page appears, displaying the following Job Flows:
- Device Based
- Module Based
- Port Based

**Step 3** Select **Device Based** and click **Go**. The Devices and Tasks dialog box appears.

**Step 4** Select the devices from the Device Selector pane. For more information on Device Selector, see the Admin Online help.

**Step 5** Select the GOLD Monitoring Tests task, using the Task Selector.

**Step 6** Click **Next**. The Add Tasks dialog box appears.

**Step 7** Click **Add Instances**. The GOLD Boot Level Configuration dialog box appears. For more information on the fields, see **GOLD Monitoring Test Task**.
Step 8  Set the parameters in the task dialog box and click **Save**.

To reset the values that you have selected click **Reset**. Click **Cancel** to return to the previous dialog box, without saving your changes.

You will see the instance of the task in the Added Tasks pane of the Add Tasks dialog box. The instance appears in this format:

`Taskname_n`, where `Taskname` is the name of the task you have added, and `n` is the number of the instance. For example, the first instance of a GOLD Monitoring task is `Gold Monitoring Tests_1`.

You can add as many instances as required, for a task.

Step 9  Click **Next**.

The Job Schedule and Options dialog box appears with these panes:

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td>Allows you to schedule the job.</td>
</tr>
<tr>
<td>Job Options</td>
<td>Allows you to set the job options.</td>
</tr>
</tbody>
</table>

Step 10  Set the schedule for the job, in the Scheduling pane:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>Select the frequency at which the job should be run—Immediate, Once, Daily, Weekly, Monthly, or Last Day of Month.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the start date for the job.</td>
</tr>
<tr>
<td>at</td>
<td>Select the start time for the job from the hour and minute drop-down lists.</td>
</tr>
<tr>
<td>Job Info</td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter the Job Description. Enter unique descriptions to help you to identify jobs easily. This is mandatory.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job will send status notices. Separate multiple addresses with commas or semicolons.</td>
</tr>
<tr>
<td></td>
<td>You must configure the SMTP server to send e-mails (<a href="#">Admin &gt; System &gt; System Preferences</a>).</td>
</tr>
<tr>
<td></td>
<td>If the user who has created the job has a valid e-mail address, an e-mail notification is sent with the user’s address in the sender address field, when job is started and completed.</td>
</tr>
<tr>
<td></td>
<td>If the user who has created the job does not have a valid e-mail address, then the notification e-mails will be sent with the sender address field blank.</td>
</tr>
<tr>
<td></td>
<td>Notification e-mails include a URL that displays the job details. If you are not logged in, you must log in using the provided login panel to view the job details.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter your comments for the job. Comments appear in the work order of the job and are stored in the configuration archive.</td>
</tr>
</tbody>
</table>
### Step 11
Set the job options, in the Job Options pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approver Comments</td>
<td>Enter comments for the Job Approver. This field is displayed only if you have enabled Job Approval for NetConfig.</td>
</tr>
<tr>
<td>Maker E-mail</td>
<td>Enter the e-mail-ID of the job creator. This field is displayed only if you have enabled Job Approval for NetConfig. This is a mandatory field.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail on Mismatch of Config Versions</td>
<td>Causes the job to be considered as failed when the most recent configuration version in the configuration archive is not identical to the most recent configuration version that was in the configuration archive when you created the job.</td>
</tr>
<tr>
<td>Sync Archive before Job Execution</td>
<td>Causes the job to archive the running configuration before making configuration changes.</td>
</tr>
<tr>
<td>Copy Running Config to Startup</td>
<td>Causes the job to write the running configuration to the startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.</td>
</tr>
</tbody>
</table>

**Enable Job Password**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Username</td>
<td>Enter the Login Username. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of LMS.</td>
</tr>
<tr>
<td>Login Password</td>
<td>Enter the job password. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Password</td>
<td>Enter the Enable password. This option is available if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.</td>
</tr>
<tr>
<td>Failure Policy</td>
<td>Select one of these options to specify what the job should do if it does not run on a device.</td>
</tr>
<tr>
<td></td>
<td>- Stop on failure:</td>
</tr>
<tr>
<td></td>
<td>If the job does not run on a device, the job is stopped. The database is updated only for the devices on which the job was run successfully.</td>
</tr>
<tr>
<td></td>
<td>- Ignore failure and continue</td>
</tr>
<tr>
<td></td>
<td>If the job fails on a device, the job skips the device and continues running on the remaining devices. The database is updated only for the devices on which the job was run successfully.</td>
</tr>
<tr>
<td></td>
<td>- Rollback device and stop</td>
</tr>
<tr>
<td></td>
<td>Rolls back the changes on the failed device and stops the job.</td>
</tr>
<tr>
<td></td>
<td>- Rollback device and continue</td>
</tr>
<tr>
<td></td>
<td>Rolls back the changes on the failed device and continues the job.</td>
</tr>
<tr>
<td></td>
<td>- Rollback job on failure</td>
</tr>
<tr>
<td></td>
<td>Rolls back the changes on all devices and stops the job. Roll back configuration changes to failed device or all devices configured by job.</td>
</tr>
<tr>
<td>Execution</td>
<td>Specify the order in which the job should run on the devices.</td>
</tr>
<tr>
<td></td>
<td>- Parallel</td>
</tr>
<tr>
<td></td>
<td>Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time.</td>
</tr>
<tr>
<td></td>
<td>- Sequential</td>
</tr>
<tr>
<td></td>
<td>Allows the job to run on only one device at a time. If you select sequential execution, you can click Set Device Order to set the order of the devices. In the Device Ordering dialog box:</td>
</tr>
<tr>
<td></td>
<td>a. Select a device name</td>
</tr>
<tr>
<td></td>
<td>b. Click Move Up or Move Down to change its place in the order.</td>
</tr>
<tr>
<td></td>
<td>c. Click OK to save the current order and close the dialog box or Click Cancel to close the dialog box without making any changes.</td>
</tr>
</tbody>
</table>

**Step 12** Click **Device Order** to view the device order.

The Set Device Order pop-up appears. You can reset the order in which the job should be run on the devices, using the Up and Down arrows.

**Step 13** Click **Done** after re-ordering the devices.

The pop-up closes.
**Step 14** Click **Next**

The Job Work Order dialog box appears with information about the job policies, the Job Approval details (if you have enabled Job Approval), the device details, and the task. It also displays details of the CLI commands that will be run on the selected devices as part of this job.

**Step 15** Click **Finish** after you review the details of your job in the Job Work Order dialog box.

A notification message appears along with the Job ID. The newly created job appears in the NetConfig Job Browser.

---

**Configuring GOLD Health Monitoring Tests**

To configure GOLD Health Monitoring tests using LMS:

**Step 1** Select **Configuration** > **NetConfig** > **NetConfig Jobs**.

The NetConfig Job Browser appears.

**Step 2** Click **Create**.

The Job Flow Type page appears, displaying the following Job Flows:

- Device Based
- Module Based
- Port Based

**Step 3** Select **Module Based** and click **Go**.

The Device and Group Selector dialog box appears.

**Step 4** Either:

- Select the devices using the Device Selector option.
- Or
  - Select the groups using the Group Selector option.

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

The Module Groups page appears.

**Step 6** Either:

- Select **Custom Group**—Allows you to select the module groups on which the NetConfig job has to run.
- Or
  - Select **Adhoc Rule**—Allows you to create Adhoc module groups by defining rules.

**Step 7** Click **Next**.

The Module Tasks page appears.

**Step 8** Select the GOLD Health Monitoring Tests task, using Task Selector.

**Step 9** Click **Next**.

The Add Tasks dialog box appears.
**Step 10**  Click **Add Instances**.

The GOLD Health Monitoring Test Configuration dialog box appears.

For more information on the fields, see **GOLD Health Monitoring Test Task**.

**Step 11**  Set the parameters in the Task dialog box and click **Save**.

- To reset the values that you have selected click **Reset**.
- To return to the previous dialog box without saving your changes, click **Cancel**.

You will see the instance of the task in the Added Tasks pane of the Add Tasks dialog box. The instance appears in this format:

Taskname_n, where Taskname is the name of the task you have added, and n is the number of the instance. For example, the first instance of a GOLD Monitoring task is **Gold Monitoring Tests_1**.

You can add as many instances as required, for a task.

**Step 12**  Click **Next**.

The Job Schedule and Options dialog box appears with these panes:

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td>Allows you to schedule the job.</td>
</tr>
<tr>
<td>Job Options</td>
<td>Allows you to set the job options.</td>
</tr>
</tbody>
</table>

**Step 13**  Set the schedule for the job, in the Scheduling pane:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>Select the frequency at which the job should be run—Immediate, Once, Daily, Weekly, Monthly, or Last Day of Month. If Job Approval is enabled, the Immediate option is not available.</td>
</tr>
<tr>
<td>Date</td>
<td>Select the start date for the job.</td>
</tr>
<tr>
<td>at</td>
<td>Select the start time for the job from the hour and minute drop-down lists.</td>
</tr>
<tr>
<td>Job Info</td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter the Job Description. Enter unique descriptions to help you to identify jobs easily. This is mandatory.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter e-mail addresses to which the job will send status notices. Separate multiple addresses with commas or semicolons. You must configure the SMTP server to send e-mails (<a href="#">Admin &gt; System &gt; System Preferences</a>). If the user who has created the job has a valid e-mail address, an e-mail notification is sent with the user’s address in the sender address field, when job is started and completed. If the user who has created the job does not have a valid e-mail address, then the notification e-mails will be sent with the sender address field blank. Notification e-mails include a URL that displays the job details. If you are not logged in, you must log in using the provided login panel to view the job details.</td>
</tr>
</tbody>
</table>
Step 14 Set the job options, in the Job Options pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td>Enter your comments for the job. Comments appear in the work order of the job and are stored in the configuration archive.</td>
</tr>
<tr>
<td>Approver Comments</td>
<td>Enter comments for the Job Approver. This field is displayed only if you have enabled Job Approval for NetConfig.</td>
</tr>
<tr>
<td>Maker E-mail</td>
<td>Enter the e-mail-ID of the job creator. This field is displayed only if you have enabled Job Approval for NetConfig. This is a mandatory field.</td>
</tr>
</tbody>
</table>

**Field Description**

- **Fail on Mismatch of Config Versions**: Causes the job to be considered as failed when the most recent configuration version in the configuration archive is not identical to the most recent configuration version that was in the configuration archive when you created the job.
- **Sync Archive before Job Execution**: Causes the job to archive the running configuration before making configuration changes.
- **Copy Running Config to Startup**: Causes the job to write the running configuration to the startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.
- **Enable Job Password**
  - **Login Username**: Enter the Login Username. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of LMS.
  - **Login Password**: Enter the job password. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Password</td>
<td>Enter the Enable password. This option is available if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you had entered when you added the device in the Device and Credentials Administration module of LMS.</td>
</tr>
<tr>
<td>Failure Policy</td>
<td>Select one of these options to specify what the job should do if it does not run on a device.</td>
</tr>
<tr>
<td></td>
<td>• Stop on failure:</td>
</tr>
<tr>
<td></td>
<td>If the job does not run on a device, the job is stopped. The database is updated only for the devices on which the job was run successfully.</td>
</tr>
<tr>
<td></td>
<td>• Ignore failure and continue</td>
</tr>
<tr>
<td></td>
<td>If the job fails on a device, the job skips the device and continues running on the remaining devices. The database is updated only for the devices on which the job was run successfully.</td>
</tr>
<tr>
<td></td>
<td>• Rollback device and stop</td>
</tr>
<tr>
<td></td>
<td>Rolls back the changes on the failed device and stops the job.</td>
</tr>
<tr>
<td></td>
<td>• Rollback device and continue</td>
</tr>
<tr>
<td></td>
<td>Rolls back the changes on the failed device and continues the job.</td>
</tr>
<tr>
<td></td>
<td>• Rollback job on failure</td>
</tr>
<tr>
<td></td>
<td>Rolls back the changes on all devices and stops the job. Roll back configuration changes to failed device or all devices configured by job.</td>
</tr>
<tr>
<td>Execution</td>
<td>Specify the order in which the job should run on the devices.</td>
</tr>
<tr>
<td></td>
<td>• Parallel</td>
</tr>
<tr>
<td></td>
<td>Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time.</td>
</tr>
<tr>
<td></td>
<td>• Sequential</td>
</tr>
<tr>
<td></td>
<td>Allows the job to run on only one device at a time. If you select sequential execution, you can click Set Device Order to set the order of the devices. In the Device Ordering dialog box:</td>
</tr>
<tr>
<td></td>
<td>In the Device Ordering dialog box:</td>
</tr>
<tr>
<td></td>
<td>a. Select a device name</td>
</tr>
<tr>
<td></td>
<td>b. Click Move Up or Move Down to change its place in the order.</td>
</tr>
<tr>
<td></td>
<td>c. Click OK to save the current order and close the dialog box or</td>
</tr>
<tr>
<td></td>
<td>Click Cancel to close the dialog box without making any changes.</td>
</tr>
</tbody>
</table>

**Step 15**  Click **Device Order** to view the device order.

The Set Device Order pop-up appears. You can reset the order in which the job should be run on the devices, using the Up and Down arrows.

**Step 16**  Click **Done** after re-ordering the devices.

The pop-up closes.
Support for GOLD Tests

Chapter 13      Generic OnLine Diagnostics (GOLD)

Step 17  Click **Next**

The Job Work Order dialog box appears with information about the job policies, the Job Approval details (if you have enabled Job Approval), the device details, and the task. It also displays details of the CLI commands that will be run on the selected devices as part of this job.

Step 18  Click **Finish** after you review the details of your job in the Job Work Order dialog box.

A notification message appears along with the Job ID. The newly created job appears in the NetConfig Job Browser.

---

**GOLD Tests and LMS Reports**

You can use LMS Custom Reports along with Syslogs to generate GOLD test reports.

Before you generate reports, you need to configure those devices on which GOLD tests are configured, to send Syslog messages to the LMS server.

Each device sends out Syslog messages after running each diagnostic test. You can identify the GOLD Syslog messages, based on their facility names. The facility names for GOLD Syslog messages will consist of DIAG or CONST-DIAG.

You can use the Syslog GOLD Custom report to ascertain the results of the test run on each device.

To generate this custom report, see the Reports Online help. The fields in the generated Syslog GOLD Custom Report are given below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device generating the Syslog message.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name or IP Address of the interface in that device generating the Syslog message.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Time when the Syslog message was generated.</td>
</tr>
</tbody>
</table>

The format used by timestamp is:

```
m 
d yyyy hh:mm:ss
```

where:

- `mmm` represents month
- `dd` represents date
- `yyyy` represents year
- `hh` represents hour
- `mm` represents minute
- `ss` represents second

Example:

```
Nov 18 2008 12:24:36
```
LMS NetShow allows you to generate reports based on various command sets. You can use LMS NetShow to generate:

- Report on Configured GOLD Tests on Each Device
- Detailed Report of All the GOLD Test Results

### Report on Configured GOLD Tests on Each Device

Use LMS NetShow to view the list of GOLD tests configured on each device.

The commandset which is used for this purpose is 
```
show diagnostic content all
show diagnostic schedule module all
show diagnostic schedule switch all
show diagnostic status
show diagnostic bootup level
show diagnostic ondemand settings
show diagnostic content module all
```

### GOLD Tests and LMS NetShow

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility/Sub Facility</td>
<td>Displays the facility or sub-facility codes. A facility is a hardware device, a protocol, or a module of the system software. See System Error Messages in the Cisco IOS Reference manual, for a predefined list of system facility codes. A sub-facility is the sub-facility in the device that generates the Syslog message.</td>
</tr>
<tr>
<td>Severity</td>
<td>Displays the message severity levels. Representations for the severity codes are: 0—Emergencies 1—Alerts 2—Critical 3—Errors 4—Warnings 5—Notifications 6—Informational</td>
</tr>
<tr>
<td>Mnemonics</td>
<td>Codes that uniquely identifies an error message. Example: TEST_RUNNING TEST_OK</td>
</tr>
<tr>
<td>Description</td>
<td>Description of each Syslog message.</td>
</tr>
<tr>
<td>Details</td>
<td>Other details for each Syslog message.</td>
</tr>
</tbody>
</table>
To generate this report:

**Step 1**  
Select **Configuration > NetShow > NetShow Jobs**.  
The NetShow Job Browser window appears.

**Step 2**  
Click **Create**.  
The Select Devices and Commandsets window appears.

**Step 3**  
Select the devices from the Device Type Selector.

**Step 4**  
Select **Show Configured GOLD Tests Info** commandset from the Commandset List.

**Step 5**  
Enter the custom commands in the Custom Commands text area if required.

**Step 6**  
Click **Next** to continue.  
The Set Schedule Options dialog box appears.

**Step 7**  
Enter the following information in the Set Schedule Options dialog box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>Select the frequency at which the job should be run:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs the job immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Once at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>• 6-hourly—Every 6 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>• 12-hourly—Every 12 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Daily—Daily at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly—Weekly on the day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Monthly—Monthly on the day of the month and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Last day of Month—On the last day of the month at the specified time.</td>
</tr>
<tr>
<td></td>
<td>The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete.</td>
</tr>
<tr>
<td></td>
<td>For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.</td>
</tr>
<tr>
<td>Date</td>
<td>Scheduled date and time of the job.</td>
</tr>
<tr>
<td><strong>Job Information</strong></td>
<td></td>
</tr>
<tr>
<td>Job Description</td>
<td>Enter the Job Description. Enter unique descriptions to help you to identify jobs easily. This is mandatory.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter the e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses; separate these addresses by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (<strong>Admin &gt; System &gt; System Preferences</strong>). We recommend that you configure the LMS Server E-mail ID in the View / Edit System Preferences dialog box (<strong>Admin &gt; System &gt; System Preferences</strong>). When the job starts or completes, an e-mail is sent with the LMS Server E-mail ID as the sender's address.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter your comments for the job. Comments appear in the Job Work Order.</td>
</tr>
</tbody>
</table>
Step 8
Click Next.

The View Job Work Order page appears with the Job Work Order. The Job Work Order contains general information on the job and on:
- Job policies.
- Job Approval details (if you have enabled Job Approval).
- Device details.
- Command sets and the commands to be executed.

Step 9
Click Finish after you review the details of your job in the Job Work Order.

A message appears, Job ID created successfully.
The newly created job appears in the NetShow Job Browser.
If your job failed and you want to run the same job, click Retry and perform steps 7 through 9 above.

Step 10
Click on the Job ID to view the results of the NetShow job created.

When a NetShow job is created for the commandset Show Configured GOLD Tests Info, it fails for any kind of devices that are selected. For each device that is selected in the job, only a particular command in the commandset is successful. Other commands fail and hence the job fails.

Example:
The command show diagnostic bootup level will be successful for a Cisco Catalyst 6000 device but will fail for Stack and Non Stack devices.
**Detailed Report of All the GOLD Test Results**

Use LMS NetShow to view a detailed report of the GOLD test results.

The commandset which is used for this purpose is Show GOLD Test Results. This commandset consists of the following two commands:

- `show diagnostic result switch all detail`
- `show diagnostic result all`

To generate this report:

**Step 1** Select **Monitor > Troubleshooting Tools > NetShow > NetShow Jobs**.

The NetShow Job Browser window appears.

**Step 2** Click **Create**.

The Select Devices and Commandsets window appears.

**Step 3** Select the devices from the Device Type Selector.

**Step 4** Select **Show GOLD Test results** commandset from the Commandset List.

**Step 5** Enter Custom Commands in the Custom Commands text area if required.

**Step 6** Click **Next** to continue.

The Set Schedule Options dialog box appears.

**Step 7** Enter the following information in the Set Schedule Options dialog box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td></td>
</tr>
<tr>
<td>Run Type</td>
<td>Select the frequency at which the job should be run:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs the job immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once—Once at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>• 6-hourly—Every 6 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>• 12-hourly—Every 12 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Daily—Daily at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly—Weekly on the day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Monthly—Monthly on the day of the month and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Last day of Month—On the last day of the month at the specified time.</td>
</tr>
<tr>
<td></td>
<td>The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete.</td>
</tr>
<tr>
<td></td>
<td>For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10:00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.</td>
</tr>
<tr>
<td>Date</td>
<td>Scheduled date and time of the job.</td>
</tr>
</tbody>
</table>
### Job Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Description</td>
<td>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter the e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses; separate these addresses by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). We recommend that you configure the LMS Server E-mail ID in the View / Edit System Preferences dialog box (Admin &gt; System &gt; System Preferences). When the job starts or completes, an e-mail is sent with the LMS Server E-mail ID as the sender's address.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter your comments for the job. Comments appear in the Job Work Order.</td>
</tr>
</tbody>
</table>

### Job Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Job Password</td>
<td>If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin &gt; Network &gt; Configuration Job Settings &gt; Config Job Policies) enter the device login user name and password and Device Enable password. If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin &gt; Network &gt; Configuration Job Settings &gt; Config Job Policies) either: - Enter the device login user name and password and Device Enable password. The credentials are for contacting the device and not the DCR credentials. Or - Disable the Job Password option in the Set Schedule Options dialog box.</td>
</tr>
<tr>
<td>Execution</td>
<td>Specify the order in which the job should run on the devices. - Parallel—Allows the job to run on multiple (up to five) devices at the same time. - Sequential—Allows the job to run on only one device at a time.</td>
</tr>
<tr>
<td>Maker Comments</td>
<td>This field appears if you have enabled Job Approval Policies for NetShow. Enter the Maker Comments.</td>
</tr>
<tr>
<td>Maker E-mail</td>
<td>This field appears if you have enabled Job Approval Policies for NetShow. Enter the Maker E-mail address. This is mandatory.</td>
</tr>
</tbody>
</table>
Step 8  Click **Next**.

The View Job Work Order page appears with the Job Work Order.
The Job Work Order contains general information on the job and on the:
- Job policies.
- Job approval details (if you have enabled job approval).
- Device details.
- Command Sets and the commands to be executed.

Step 9  Click **Finish** after you review the details of your job in the Job Work Order.

A message appears, *Job ID created successfully*.

The newly created job appears in the NetShow Job Browser.

If your job failed and you want to run the same job, click **Retry** and perform steps 7 through 9 above.

Step 10  Click on the Job ID to view the results of the NetShow job created.

---

When a NetShow job is created for the commandset **Show GOLD Test Results**, it fails for any kind of devices that are selected. For each device that is selected in the job, only a particular command in the command set is successful. Other commands fail and hence the job fails.

Example:
The command *show diagnostic result switch all detail* will be successful for Stack devices but will fail for Cisco Catalyst 6000 devices and Non Stack devices.

### GOLD Show Commands

See the Configuration Online help for configuring the NetConfig Show Commands job for devices that supports GOLD.

### GOLD Syslogs

See the Reports Online help for the steps to generate GOLD Syslogs report.
Managing IPSLA Devices

This section contains the following topics:

- **Understanding the IPSLA Devices Page**
- **Viewing IPSLA Devices**
- **Automatically Importing DCR Devices**
- **Adding Adhoc Target Devices**
- **Licensing Behavior While Adding Devices**
- **Editing IPSLA Device Attributes**
- **Deleting Devices from IPSLA Monitoring**
Understanding the IPSLA Devices Page

For IPSLA Monitoring function work with devices, you must first add devices to Device Credential Repository (DCR). You can also add adhoc target devices for IPSLA Monitoring.

The devices added for IPSLA Monitoring both from DCR and adhoc target devices, appear on the IPSLA Devices page.

Table 14-1 shows the fields and buttons that are available in IPSLA Devices page.

Table 14-1  IPSLA Devices Page

<table>
<thead>
<tr>
<th>Fields/Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSLA Devices</td>
<td>Lists all devices in LMS. The devices are identified by the Display Name that you have entered while adding devices to Device Credential Repository (DCR).</td>
</tr>
<tr>
<td>Add Adhoc Target</td>
<td>Allows you to add adhoc target devices. For more information, see Adding Adhoc Target Devices.</td>
</tr>
<tr>
<td>Edit Device Attributes</td>
<td>Allows you to edit the device attributes. The device attributes are:</td>
</tr>
<tr>
<td></td>
<td>- SNMP Retry</td>
</tr>
<tr>
<td></td>
<td>- SNMP Timeout</td>
</tr>
<tr>
<td></td>
<td>For more information, see Editing IPSLA Device Attributes.</td>
</tr>
<tr>
<td>Update IPSLA Config</td>
<td>• Allows you to update the IPSLA responder enable or disable status</td>
</tr>
<tr>
<td></td>
<td>• Allows you to save the latest information configured in a device to the database.</td>
</tr>
<tr>
<td>Enable IPSLA Responder</td>
<td>Enables responder for the selected devices.</td>
</tr>
<tr>
<td></td>
<td>You cannot enable IPSLA responder for</td>
</tr>
<tr>
<td></td>
<td>- Devices that is not IPSLA capable</td>
</tr>
<tr>
<td></td>
<td>- Adhoc devices</td>
</tr>
<tr>
<td></td>
<td>- Devices with incorrect Read-Write and Read-Only credentials.</td>
</tr>
<tr>
<td>Delete</td>
<td>Allows you to delete devices from managing IPSLA Monitoring functionality.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Deleting Devices from IPSLA Monitoring.</td>
</tr>
<tr>
<td>Refresh (Icon)</td>
<td>Use this to update the new device count.</td>
</tr>
</tbody>
</table>

Viewing IPSLA Devices

The IPSLA Devices page lists all devices based on Device Type Groups, Responder Enabled Devices, and Adhoc Target devices (Monitor > Performance Settings > IPSLA > Devices).

- All Devices—Lists all DCR devices in the application with their display names. The display names are defined when you add the devices in DCR.
- Device Type Groups—Lists all devices in groups and subgroups based on their MDF type.
Automatically Importing DCR Devices

Whenever you add devices to Device Credential Repository (DCR), the devices are added for IPSLA Monitoring automatically if the Enable Auto Mode option is checked. This option is available under Inventory > Device Administration > Device Allocation Policy.

This option is enabled by default. Hence, the devices get added for IPSLA monitoring automatically after you have added the devices to DCR.

Adding Adhoc Target Devices

You can use this option to add adhoc target devices for IPSLA Monitoring if you want to manage devices from an external source. The Adhoc devices may be either cisco devices or devices with a unique IP address.

The devices added are not included for the device license count.

To add adhoc target devices:

Step 1  Select Monitor > Performance Settings > IPSLA > Devices.

The IPSLA Devices page appears.

Step 2  Click Add Adhoc Target.

The Add Adhoc Devices page appears.

Step 3  Enter the Host Name/IP Address of the target device in the Adhoc Devices field.

Note  Use comma (,) separator to add more than one device.

Step 4  Select the Enable IPSLA Responder check box if IPSLA Responder is enabled on the devices.

Step 5  Click Add to add the adhoc target devices.

A message appears that the devices are added successfully.

Step 6  Click OK.
Licensing Behavior While Adding Devices

Based on the IPSLA device license limit, you can add devices from Device Credential Repository (DCR) either automatically or manually.

Licensing Behavior While Adding Devices Automatically
Select Enable Auto mode option and then either by selecting Managing All devices or Manage by groups option on the Auto Allocation Setting, you can automatically add devices from DCR for IPSLA Monitoring.

Licensing Behavior While Adding Devices Manually
If you do not want to import devices automatically from DCR, then you can import the devices manually from DCR to IPSLA Monitoring.

Editing IPSLA Device Attributes

You can modify the device attributes for single or multiple devices listed in IPSLA Devices page. You cannot modify the adhoc target devices.

The device attributes that you can modify are:

- SNMP Retry—Number of times the system retries to access devices using SNMP options. The default value is 3. The minimum value is 0 and the maximum value is 6.
- SNMP Timeout—Duration of time that the system should wait for a device to respond before it retries to access it again. The default value is 2. The minimum value is 0 and there is no maximum value.

To edit the IPSLA device attributes:

**Step 1** Select Monitor > Performance Settings > IPSLA > Devices from the menu.

The IPSLA Devices page appears.

**Step 2** Select the required devices for which you want to edit the device attributes.

**Step 3** Click Edit Device Attributes.

The Device Attributes Information window appears.

**Step 4** Select the required device from the Devices section.

**Step 5** Modify the following device attributes in the Device Information section:
- SNMP Retry (0-6 count)
- SNMP Timeout (Min 0 Secs)

You can select the Apply to all Devices check box to apply the attributes of one device to all the other devices listed in the Devices section.

**Step 6** Click Modify.

A message appears that the attributes of the selected devices have been modified successfully.

**Step 7** Click OK.
Deleting Devices from IPSLA Monitoring

Whenever you add devices to Device Credential Repository (DCR), the devices are added for IPSLA Monitoring automatically if the **Enable Auto Mode** option is checked. This option is available under **Inventory > Device Administration > Device Allocation Policy**.

This option is enabled by default. Hence, the devices get added for IPSLA monitoring automatically after you have added the devices to DCR.

You cannot delete the devices manually from IPSLA Monitoring.

You can also delete the IPSLA devices using the command line interface command:

```
ipm deletedevice -u admin -p admin -device Display Name
```

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Permission Report (<strong>Reports &gt; System &gt; Users &gt; Permission</strong>) to check if you have the required privileges to perform this task.</td>
</tr>
</tbody>
</table>
Managing Collectors

This section explains how to configure collectors on the source router and gather statistics on availability, latency, and jitter from the network.

It contains the following topics:

- Understanding Collector Management Page
- Working with IPSLA Collectors

Understanding Collector Management Page

This section briefly describes all the collector-related tasks that you can perform on the Collector Management page, and also provides the various collector status and their validation details in Table 15-2.

Table 15-1 outlines the tasks that you can perform from the Collector Management page (Monitor > Performance Settings > IPSLA > Collectors).
### Table 15-1 Collector Management Page

<table>
<thead>
<tr>
<th>Field/Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector Group Selector</td>
<td>Lists all the operation-based (system-defined) and user-defined collector groups in IPSLA Monitoring. The list of operation-based groups are as follows:</td>
</tr>
<tr>
<td></td>
<td>• CallSetupPostDialDelay</td>
</tr>
<tr>
<td></td>
<td>• DHCP</td>
</tr>
<tr>
<td></td>
<td>• DNS</td>
</tr>
<tr>
<td></td>
<td>• Echo</td>
</tr>
<tr>
<td></td>
<td>• EthernetJitter</td>
</tr>
<tr>
<td></td>
<td>• ICMPJitter</td>
</tr>
<tr>
<td></td>
<td>• PathEcho</td>
</tr>
<tr>
<td></td>
<td>• RTP</td>
</tr>
<tr>
<td></td>
<td>• UDPEcho</td>
</tr>
<tr>
<td></td>
<td>• UDPJitter</td>
</tr>
<tr>
<td>List Collectors</td>
<td>Select one or more source devices and click this button to view the collectors associated with the source devices.</td>
</tr>
<tr>
<td>Filter</td>
<td>Filters the list of collectors in IPSLA Monitoring. For more information, see Filtering Collectors.</td>
</tr>
<tr>
<td>View</td>
<td>Allows you to view the collector details. For more information, see Viewing the Collector Details.</td>
</tr>
<tr>
<td>Graph</td>
<td>Allows you to view the collector statistics or compare the latency of collectors based on the granularity. For more information, see Viewing Collector Graphs.</td>
</tr>
<tr>
<td>Edit</td>
<td>Allows you to edit the following collector details:</td>
</tr>
<tr>
<td></td>
<td>• Collector Information such as Name and Description, and Source Interface.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Editing a Collector.</td>
</tr>
</tbody>
</table>
### Table 15-1  
**Collector Management Page**

<table>
<thead>
<tr>
<th>Field/Buttons</th>
<th>Description</th>
</tr>
</thead>
</table>
| Delete        | Deletes collectors from IPSLA Monitoring.  
For more information, see Deleting Collectors. |
| Export        | Exports collector configuration information into a CSV file.  
For more information, see Exporting Collector Configuration Information. |
| Monitor       | Generates real-time graph for a collector in Running status.  
For more information, see Monitoring a Collector. |
| Start         | Starts the stopped collectors.  
For more information, see Starting the Collectors. |
| Stop          | Stops collectors in the Running status.  
For more information, see Stopping the Collectors. |
| Import        | Imports collector configuration information from CSV file into IPSLA Monitoring space.  
For more information, see Importing Collector Configuration Information. |
| Reconfigure   | Allows you to reconfigure Failed state.  
For more information see Reconfiguring Collectors. |
| Create        | Allows you to create collectors for managing IPSLA functionality.  
For more information, see Defining Collectors. |
| Refresh (Icon)| Allows you to refresh the collector list. |

### Collector Status and Validation

Table 15-2 lists the various collector status, their description, and validation of the status with respect to the tasks.

### Table 15-2  
**Collector Status and Validation**

<table>
<thead>
<tr>
<th>Collector Status</th>
<th>Description</th>
<th>Tasks</th>
</tr>
</thead>
</table>
| Scheduled        | Collector is scheduled for a future date and time. | Allows you to edit or delete the collectors.  
You cannot start, stop, or monitor the collectors. |
| Configuring      | Configuration of the collector is in progress. | Allows you to edit or delete the collectors.  
You cannot start, stop, or monitor the collectors. |
| Running          | Collector is configured at the source router and the polling is in progress. | Allows you to stop, monitor, or edit the collectors.  
You cannot start the collectors. |
### Collector Status and Validation

<table>
<thead>
<tr>
<th>Collector Status</th>
<th>Description</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopped</td>
<td>Collectors that are manually stopped and not being polled by IPSLA Monitoring.</td>
<td>Allows you to start, delete, or edit the collectors. You cannot stop or monitor the collectors.</td>
</tr>
<tr>
<td>Completed</td>
<td>Collector has reached its End Time and polling will not be performed again for this collector by IPSLA Monitoring.</td>
<td>Allows you to delete the collectors. You cannot start, stop, edit, or monitor the collectors.</td>
</tr>
</tbody>
</table>
| Config Failed    | Configuration of the collector failed on the source router. This may be caused by one of the following:  
• Low memory allocated for IP SLA on the source router.  
• Source router does not support the operation that you have selected while creating the collector.  
  For example, for ICMP Jitter operation, you must select a source router with IOS version > 12.4. | Allows you to edit or delete the collectors. You cannot start, stop, or monitor the collectors. |
| Dormant          | Collector is inactive on the source device. As a result, IPSLA Monitoring does not poll for the statistical data during this period. | Allows you to edit or stop the collectors. You cannot start, delete, or monitor the collectors. |
| Source Not Responding | Collector will move to this status while configuring/reconfiguring/polling statistics of a collector due to:  
• Invalid credentials  
• Device is not reachable | Allows you to edit or delete the collectors. You cannot start, stop, or monitor the collectors. |
| MEP Missing      | Maintenance End Point Missing. Collector will move to this status when the Maintenance end Point is detected to be missed during polling and reconfiguring (start / edit / device reload). | Allows you to monitor and view the collectors. It also allows you to view graphs for the collectors. You cannot start, stop, export or edit the collectors. MEP missing collectors can be deleted but cannot be monitored. This state is applicable only for Auto IPSLA Ethernet collectors. |
Filtering Collectors

The Filter option available in the IPSLA Collector Management dialog box, allows you to filter the Collectors based on certain fields and value. The filter operation uses “contains” as the default criteria to filter the Collectors based on the string provided in the filter text area. The Collector filter operation is not case sensitive.

You can filter the Collectors based on any of the following fields:

- All
- Collector Name
- Source
- Target
- Operation
- Status
- VRF

Example:
If you want to filter the Collectors based on Collector Name and with value chen:

1. From the Filter Drop down, select Collector Name.
2. In the Filter text area enter chen
3. Click Filter

By default the filter operation uses “contains” to filter the Collectors.

All those Collectors whose names contain the value chen are filtered and provided in the results:

ChenColl
HTTPChenColl

---

Table 15-2 Collector Status and Validation

<table>
<thead>
<tr>
<th>Collector Status</th>
<th>Description</th>
<th>Tasks</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updating</td>
<td>Editing a collector is in progress.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resuming</td>
<td>Intermediate status between Dormant and Running.</td>
<td></td>
<td>You cannot start, stop, or monitor the collectors.</td>
</tr>
<tr>
<td>Stopping</td>
<td>Intermediate status between Running and Stopped.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Completing</td>
<td>Intermediate status between Running and Completed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dormant Pending</td>
<td>Intermediate status between Running and Dormant.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deleting</td>
<td>Collector deletion is in progress.</td>
<td></td>
<td>You cannot the delete the collectors which are running.</td>
</tr>
<tr>
<td></td>
<td>You cannot the delete the collectors which are running.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reconfiguring</td>
<td>Intermediate status between Config Failed and Running.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Or</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>When the collector is missing on the source router.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---
Collector License Information

The number of collectors that you create in IPSLA Monitoring depends on the device license limit. For example, if you have a license for 100 devices, you are allowed to create up to 300 collectors to manage IPSLA Monitoring functionality as shown in Table 15-3.

Table 15-3 Collector License Information

<table>
<thead>
<tr>
<th>Device License</th>
<th>Licensed Number of Collectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>150 Collectors</td>
</tr>
<tr>
<td>100</td>
<td>300 Collectors</td>
</tr>
<tr>
<td>200</td>
<td>300 Collectors</td>
</tr>
<tr>
<td>500</td>
<td>1250 Collectors</td>
</tr>
<tr>
<td>1000</td>
<td>1500 Collectors</td>
</tr>
<tr>
<td>2500</td>
<td>3000 Collectors</td>
</tr>
<tr>
<td>5000</td>
<td>5000 Collectors</td>
</tr>
<tr>
<td>10000</td>
<td>5000 Collectors</td>
</tr>
</tbody>
</table>

Incremental Licenses

| Incremental combination from 250 — 450 device count | 1000 Collectors |
| Incremental combination from 550 — 950 device count | 1250 Collectors |
| Incremental combination from 1050 — 1450 device count | 1500 Collectors |
| Incremental combination from 1500 — 2500 device count | 3000 Collectors |
| Incremental combination from 2500 — 5000 device count | 5000 Collectors |

The IPSLA Monitoring Collector license limit applies only to historical collectors and not to real-time collectors. However, you are allowed to create real-time collectors even after the license limit is reached. There is no limit to the number of real-time collectors that you could create to manage IPSLA Monitoring functionality.

Note

The AutoIPSLA generated collectors are accounted for license.
Working with IPSLA Collectors

A collector is defined as an entity that encompasses a source router, a target device, an operation, and the collector schedule. IPSLA Monitoring allows you to create one or more collectors by selecting one source device, multiple target devices and operations.

The number of collectors you create depends on the device license. For more information on the device license, see Table 15-3.

After you create the collectors, they are configured on the source router by IPSLA Monitoring functionality to collect the network performance statistics.

Creating collectors involves

- Specifying Source Devices
- Specifying Target Devices
- Specifying IPSLA Operations
- Defining Collectors

This section also contains information on:

- Viewing the Collector Page
- Viewing the Collector List
- Viewing the Collector Details
- Editing a Collector
- Deleting Collectors
- Viewing Collector Graphs
- Exporting Collector Configuration Information
- Importing Collector Configuration Information
- Monitoring a Collector
- Stopping the Collectors
- Starting the Collectors
- Reconfiguring Collectors

Note: You cannot start, stop, edit, delete, or monitor AutoIPSLA-generated collectors

Specifying Source Devices

IPSLA Monitoring source is a device from which you initiate operations for measuring network performance statistics. Each source must be IPSLA capable and an SNMP agent.

The following MIBs are used by IPSLA Monitoring to retrieve required information:

- RttMonMIB
- SystemMIB
The source devices are listed under Source Device Selector on the Collector Configuration page. This list contains only IP SLA capable devices under the respective MDF categories and also in “All Devices” folder.

## Specifying Target Devices

IPSLA Monitoring targets are destination devices for which you want to gather network performance statistics. A target can be any IP-addressable device or a Cisco device running the IP SLA Responder on which the source router performs IP SLA operations. Target devices with IP SLA Responder capability provide more accurate measurements than the other target devices.

*Note:* The IP SLA Responder is supported only in Cisco IOS 12.1(2)T or later. We strongly recommend that you use software release 12.1 or later.

## Specifying IPSLA Operations

IP SLA operations are used to create collectors that are configured on the source router to measure network performance statistics. IPSLA supports the following IP SLA operations:

- **Echo Operations**
  - Echo
  - Path Echo
  - UDP Echo
- **Jitter Operations**
  - ICMP Jitter
  - UDP Jitter
- **Services Operations**
  - DNS
  - DHCP
  - HTTP
  - FTP
  - DLSw
  - TCP Connect
- **VoIP-related Operations**
  - Gatekeeper Registration Delay
  - Call Setup Post Dial Delay
  - RTP
- **Metro Ethernet Operations**
  - Ethernet Ping
  - Ethernet Jitter
- Ethernet Ping Auto IP SLA
- Ethernet Jitter Auto IP SLA
- Video Operations

For more information, see Managing Operations.

**Defining Collectors**

IPSLA provides a single wizard-based approach that leads you through the procedure to create multiple collectors. This wizard process involves the following four steps:

- Configuring Collectors
- Selecting Collectors
- Scheduling Collectors
- Viewing the Collector Summary

You must complete all the four tasks in this sequence to create collectors. If you exit the wizard at any stage using Cancel, the details you have specified will be lost and the collectors will not be created.

**Configuring Collectors**

The Collector Configuration page allows you to configure collectors. You can configure collectors by specifying the collector information, a source device, target devices, and operations.

You can also configure collectors by specifying the VRF Name.

The collectors are created, based on the number of target devices and operations that you have selected. If you have selected $M$ target devices and $N$ operations, then $M*N$ collectors are created.

---

**Note**

Target device is not applicable for VoIP Gatekeeper Registration Delay, VoIP Post Dial Delay, Ethernet Ping Auto IPSLA, DHCP, Ethernet Ping, Ethernet Jitter and Ethernet Jitter Auto IP SLA operations. If you select target device a message appears indicating that they do not support target device.

The Maintenance End Point (MEP) number is referred to and considered as the Target device for Ethernet Ping and Ethernet Jitter operations.

The number of historical collectors you create to manage IPSLA Monitoring functionality, depends on your device license. For more information on the license, see Collector License Information.

However, we recommend that you create collectors based on the polling interval for better performance of the IPSLA Monitoring server.
To configure collectors:

**Step 1**  Select **Monitor > Performance Settings > IPSLA > Collectors**.
The Collector Management page appears.

**Step 2**  Click **Create**.
The Collector Configuration page appears.

**Step 3**  Specify the following details in the Collector Info section:
- The collector name in the Collector Name field.
- A brief description of the collector in the Description field.

Though the Collector Name field allows you to enter more than 15 characters, the source device and trap PDUs display only the first 15 characters for IOS versions that are lower than 12.4. However, the IPSLA Monitoring database, contains the complete collector name.

**Step 4**  Select the source device from the Source Devices list.
For more information on selecting Source Device, see Table 15-4.

### Table 15-4  Using Source Device List

<table>
<thead>
<tr>
<th>Folder Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Input</td>
<td>Enter your search expression in this text field. You can enter a single device name or multiple device names in this field. You can enter the following as search inputs to search multiple devices:</td>
</tr>
<tr>
<td></td>
<td>- Comma-separated list of complete device names.</td>
</tr>
<tr>
<td></td>
<td>- Device names with wildcard characters * and ? to search for multiple devices that match the text string entered in this input field.</td>
</tr>
<tr>
<td></td>
<td>- Combination of comma-separated lists of device names, and device names with wildcard characters.</td>
</tr>
<tr>
<td>All</td>
<td>Lists all devices that are available to manage IPSLA Monitoring functionality.</td>
</tr>
<tr>
<td>Selection</td>
<td>Lists all devices that you have selected in the All or Search Results tab or through a combination of both</td>
</tr>
<tr>
<td>Search Results</td>
<td>Displays the Simple search results. From the search result, you can:</td>
</tr>
<tr>
<td></td>
<td>- Select all devices</td>
</tr>
<tr>
<td></td>
<td>- Clear all devices</td>
</tr>
<tr>
<td></td>
<td>- Select a few devices</td>
</tr>
<tr>
<td>All Devices</td>
<td>Lists all devices in the application in alphabetical order of their display names. The display names are defined when you add the devices in DCR.</td>
</tr>
<tr>
<td>Device Type Groups</td>
<td>Lists all devices in groups and subgroups, based on their Device Category, Series, and Model. By default, the device grouping is based on their Device Categories, such as Routers, Switches, and Hubs</td>
</tr>
<tr>
<td>User-defined Groups</td>
<td>Lists IPSLA devices that satisfy the group rules. These group rules are defined by you when you create the User-defined groups.</td>
</tr>
</tbody>
</table>
**Step 5** Select the Use VRF check box to enter Virtual Routing and Forwarding details. When you select the Use VRF check box, the Select VRF button is activated.

**Step 6** Either:
- Enter the VRF details in the VRF field.
  - If you enter an invalid VRF name or a VRF name that does not exist in the selected source, the collectors go to the ConfigFailed state.
  - Or
  - Click **Select VRF** to select the VRF from the existing list of VRFs configured in the device.

When you Select VRF, the VRF List pop-up box appears. The VRF List displayed is based on the Source device that you selected in Step 4.

For more information on selecting the VRF from the VRF List pop-up box, see Table 15-5.

<table>
<thead>
<tr>
<th>Table 15-5 VRF List</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Elements</strong></td>
</tr>
<tr>
<td>Get Latest From Device</td>
</tr>
<tr>
<td>OK</td>
</tr>
<tr>
<td>Cancel</td>
</tr>
</tbody>
</table>

If the VRF List is blank, the VRF List dialog box displays the following message:

*The VRF list is blank. Click Continue to refresh the list from the device.*

You can configure collector using VRF only for the following operations:
- ICMP echo
- UDP echo
- ICMP path echo
- ICMP jitter
- UDP jitter
- TCP Connect
- HTTP
- FTP
- DNS
- Video

**Step 7** Select one or more target devices from the Target Devices list.

For more information on selecting the Target device, see Table 15-6.
Step 8 Select one or more operations from the Operations list.

Step 9 Enter a valid IP address in the Source Interface field.

This is the IP address of the Source Device Interface to which the packets are returned from the destination.

The Source Interface field is an optional field and does not apply to Ethernet operations.

Step 10 Click Next.

The Select Collector page appears.

Table 15-6 Using the Target Devices List

<table>
<thead>
<tr>
<th>Folder Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Input</td>
<td>Enter your search expression in this text field. You can enter a single device name or multiple device names in this field. You can enter the following as search inputs to search multiple devices: • Comma-separated list of complete device names. • Device names with wildcard characters * and ? to search for multiple devices that match the text string you have entered in this input field. • Combination of comma separated list of device names, and device names with wildcard characters.</td>
</tr>
<tr>
<td>All</td>
<td>Lists all devices that are available to manage IPSLA Monitoring functionality.</td>
</tr>
<tr>
<td>Selection</td>
<td>Lists all devices that you have selected in the All or Search Results tab or through a combination of both.</td>
</tr>
<tr>
<td>Search Results</td>
<td>Displays the Simple search results. From the search result, you can: • Select all devices • Clear all devices • Select a few devices</td>
</tr>
<tr>
<td>All Devices</td>
<td>Lists all devices in the application in alphabetical order of their display names. The display names are defined when you add the devices in DCR.</td>
</tr>
<tr>
<td>Device Type Groups</td>
<td>Lists all devices in groups and subgroups based on their Device Category, Series, and Model. By default, the device grouping is based on their Device Categories, such as Routers, Switches, and Hubs.</td>
</tr>
<tr>
<td>User-Defined Groups</td>
<td>Lists IPSLA devices that satisfy the group rules. The group rules are defined by you when you create the User-defined groups</td>
</tr>
<tr>
<td>Subnet Groups</td>
<td>Lists the subnet-based groups.</td>
</tr>
<tr>
<td>Mediantet Endpoint</td>
<td>Lists the group of devices connected Mediantet Endpoints.</td>
</tr>
<tr>
<td>Connected Groups</td>
<td>Lists all responder-enabled Target devices. UDP Jitter operation uses Responder Enabled Target devices.</td>
</tr>
<tr>
<td>Adhoc Target</td>
<td>Lists all external Target devices that are added to manage IPSLA Monitoring functionality.</td>
</tr>
</tbody>
</table>
Selecting Collectors

The Select Collector page allows you to select or deselect collectors that you want to create. By default, all collectors are selected.

A warning appears if the device that you specified on the Collector Configuration page, has wrong credentials or is not reachable.

To select collectors:

**Step 1**
Select the required collectors from the Select Collectors pane that you want to create.

For more information on the Select Collector page, see Table 15-7.

**Table 15-7 Select Collector Page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Details</td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td>IP address of the Source device you have selected.</td>
</tr>
<tr>
<td>IOS Version</td>
<td>IOS version of the Source device.</td>
</tr>
<tr>
<td>Max Collectors</td>
<td>Maximum number of collectors that the Source device supports.</td>
</tr>
<tr>
<td>New Collectors Capacity</td>
<td>Number of collectors you can configure on the Source device.</td>
</tr>
</tbody>
</table>

**Step 2**
Click Next.

The Schedule page appears.

You can also filter the collector list using the Filter field. For more information, see Table 15-8.

**Table 15-8 Filtering Collectors on Select Collector Page**

<table>
<thead>
<tr>
<th>Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Lists all collectors to manage IPSLA Monitoring functionality.</td>
</tr>
<tr>
<td>Collector Name</td>
<td>Enter the complete Collector name or a part of it.</td>
</tr>
<tr>
<td>Target</td>
<td>Enter the complete Target name or a part of it.</td>
</tr>
<tr>
<td>Operation</td>
<td>Enter the complete Operation name or a part of it.</td>
</tr>
</tbody>
</table>
Scheduling Collectors

The Schedule page allows you to specify the collector type, schedule the start and end times for the collectors to configure, and specify the polling time intervals.

To schedule collectors:

**Step 1** Select either of the following from the Collector Type section:

- **Historical/Statistical**—Gathers data and stores it in the IPSLA Monitoring database for future analysis. This is the default setting.

  Or

- **Monitored/Real-time**—Allows you to monitor network performance in real-time. However, the network performance data is not stored in the IPSLA Monitoring database.

If you select **Monitored/Real-time** as the type, the Start Time Details, End Time Details, and Poller Settings fields are disabled.

**Step 2** Define a schedule for the selected collectors in the Start Time Details section. To do this select either:

- **Immediate**—Starts the collector immediately after it is configured. This is the default setting.

  Or

- **Date**—Select this from the Calendar icon. The collector will start at the specified date. The default setting for Date is the current date. That is, the date on which you define the collector.

  The start time of the collector depends on the time defined in the Poller Settings field.

  At the scheduled start time, IPSLA Monitoring configures the collector in the router and the status is reflected in the Collector Management page.

  The Date field is disabled if you have selected **Immediate** as the start time.

**Step 3** Specify the end date for the collector in the End Time Details section. To do this, select any of the following:

- **Forever**—Runs the collector continuously. This is the default setting. To stop the running collector select **Monitor > Performance Settings > IPSLA > Collectors > Stop**.

- **Duration**—Removes the collector from the source router after the specified length of time has expired. The duration is specified in days. You can also specify 0 days as the duration. This is the current date.

  For example, if you specify 0 days with polling time intervals 20:00:00 to 23:30:00, the collector stops polling at 23:30:00 hours.

- **Date**—Select this from the Calendar icon. The collector will stop at the specified date. The default setting for Date is the current date. That is, the date on which you define the collector.

  The end time of the collector depends on the time defined in the Poller Settings field.

  The Duration and Date fields are disabled if you select **Forever** as the end time.
Step 4 Specify the following in the Poller Settings section:

- **Polling Interval**—Specifies the polling frequency from IPSLA Monitoring server to the source router to collect statistics. Select the polling interval from the drop-down list. The default polling interval is 60 minutes. The polling intervals available are 1, 5, 15, and 30, and 60 minutes.

  We recommend that you create collectors based on the polling interval for better performance of the IPSLA Monitoring server.

  - You can generate Minute reports and graphs only if you have set the Polling Interval to any of these: 1, 5, 15, and 30 minutes.
  - You can generate Historical reports and graphs for all Polling Interval such as 1, 5, 15, 30, and 60 minutes.

- **Days of Week**—Select the days of the week when you want the polling to occur.

- **Time**—Specify the From and To time interval for the polling to start. You must specify the time in the format, Hour:Minutes:Seconds. The default From and To times are 00:00:00 and 23:59:59, respectively.

Step 5 Click Next.

The Summary page appears.

---

**Viewing the Collector Summary**

The Summary page provides information on the collector configuration, schedule, and poller settings. It provides the VRF details, if VRF is used while creating Collector. For more information, see Table 15-9.

To view the collector summary:

Step 1 Click Finish.

A message appears that the collectors were created successfully.

Or

Click Back.

This allows you to modify the settings defined in the Collector Configuration, Select Collector, or Schedule pages.

Step 2 Click OK.

The Collector Management page displays the newly-defined collectors.
Working with IPSLA Collectors

Chapter 15  Managing Collectors

Table 15-9  Collector Summary Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector Name</td>
<td>Displays the collector name</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Collector Type</td>
<td>Collector type (such as Historical or Real time).</td>
</tr>
<tr>
<td>Configuration Details</td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td>IP address of the Source device.</td>
</tr>
<tr>
<td>Target Addresses</td>
<td>IP addresses of the Target device.</td>
</tr>
<tr>
<td>Operation Names</td>
<td>Name of the operation.</td>
</tr>
<tr>
<td>VRF Name</td>
<td>Displays the name of the VRF specified while creating collector.</td>
</tr>
<tr>
<td></td>
<td>If you have not specified the VRF details, the field will be displayed as “Not Applicable”.</td>
</tr>
<tr>
<td>Schedule Details</td>
<td></td>
</tr>
<tr>
<td>Start Date</td>
<td>Start date that you specified while creating collectors.</td>
</tr>
<tr>
<td>End Date</td>
<td>End date that you specified while creating collectors.</td>
</tr>
<tr>
<td>Poller Settings</td>
<td></td>
</tr>
<tr>
<td>Polling Interval (mins)</td>
<td>Polling time interval that you specified while creating a collector.</td>
</tr>
<tr>
<td>Polling Time</td>
<td>Start and end times of the polling times that you specified while creating a collector.</td>
</tr>
<tr>
<td>Days of Week Details</td>
<td>Days of the week when polling occurs. These are the days that you specified while creating a collector.</td>
</tr>
</tbody>
</table>

Viewing the Collector Page

The Collector Management page displays collectors. It also displays their details, such as collector name, source, target, operation, start time, end date, collector type, and status.

The Collector Management page has a sliding object selector labelled, Collector Group Selector. Click the red arrow on this selector to maximize or minimize the view of the Collector List.

You can perform the following tasks on this page:

- List Operation-based groups (See Listing Operation-Based (System-Defined) Groups)
  - Lists collectors based on the default operation types.
- List User-defined groups (See Listing User-Defined Groups)
  - Lists collectors based on the groups defined by users in Group Administration.
• Filter the collector list (See Filtering the Collector List)
  Allows you to filter the collector list.
• Sort the collector list (See Sorting the Collector List)
  Allows you to sort the collector list.

**Note**
You can also use a combination of operation-based groups and user-defined groups to list the collectors.

**Listing Operation-Based Groups**
To list collectors, based on Operation-based groups:

**Step 1**
Select Monitor > Performance Settings > IPSLA > Collectors.
The Collector Management page appears, displaying the list of collectors.

**Step 2**
Select the operation you need from the Operation Based Groups folder in the left pane.
For example, to list collectors based on the operation, FTP, select the FTP check box.

**Step 3**
Click List Collectors.
The collector list for the selected operation appears in the right pane.

**Listing User-Defined Groups**
To list collectors based on User-defined groups:

**Step 1**
Select Monitor > Performance Settings > IPSLA > Collectors.
The Collector Management page appears, displaying the list of collectors.

**Step 2**
Select the required User-defined group from the left pane.
For example, to list collectors based on the location, USCollectors, select the USCollectors check box.

**Step 3**
Click List Collectors.
The collector list for the selected User-defined group appears in the right pane.
Filtering the Collector List

To filter the collector list:

**Step 1** Select the filter type from the Filter drop-down list.

**Step 2** Click **Filter**.

The Filter Collector list appears. See **Table 15-10**.

### Table 15-10 Filtering Collector List

<table>
<thead>
<tr>
<th>Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Displays the entire collector list.</td>
</tr>
<tr>
<td>Collector Name</td>
<td>Enter the complete Collector name or a part of it.</td>
</tr>
<tr>
<td>Source</td>
<td>Enter the complete Source device name or a part of it.</td>
</tr>
<tr>
<td>Target</td>
<td>Enter the complete Target device name or a part of it.</td>
</tr>
<tr>
<td>Operation</td>
<td>Enter the complete Operation name or a part of it.</td>
</tr>
<tr>
<td>Status</td>
<td>Enter the complete Status name or a part of it.</td>
</tr>
<tr>
<td>VRF</td>
<td>Enter the complete VRF name.</td>
</tr>
</tbody>
</table>

### Table 15-11 Using Source Devices List

<table>
<thead>
<tr>
<th>Folder Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Input</td>
<td>Enter your search expression in this text field.</td>
</tr>
<tr>
<td></td>
<td>You can enter a single device name or multiple device names in this field.</td>
</tr>
<tr>
<td></td>
<td>You can enter the following as search inputs to search multiple devices:</td>
</tr>
<tr>
<td></td>
<td>• Comma separated list of full device names.</td>
</tr>
<tr>
<td></td>
<td>• Device names with wildcard characters * and ? to search for multiple devices</td>
</tr>
<tr>
<td></td>
<td>• Combination of comma separated list of device names, and device names with</td>
</tr>
<tr>
<td></td>
<td>wildcard characters.</td>
</tr>
<tr>
<td>All</td>
<td>Lists all the devices that are available to manage IPSLA Monitoring function</td>
</tr>
<tr>
<td>Selection</td>
<td>Lists all the devices that you have selected in the All or Search Results tab</td>
</tr>
<tr>
<td>Search Results</td>
<td>Displays the Simple search results. From the search result, you can:</td>
</tr>
<tr>
<td></td>
<td>• Select all devices</td>
</tr>
<tr>
<td></td>
<td>• Clear all devices</td>
</tr>
<tr>
<td></td>
<td>• Select a few devices</td>
</tr>
<tr>
<td>All Devices</td>
<td>Lists all the devices in the application in the alphabetical order of their</td>
</tr>
<tr>
<td></td>
<td>display names. The display names are defined when you have added the devi</td>
</tr>
<tr>
<td></td>
<td>ces in DCR.</td>
</tr>
<tr>
<td>Device Type Groups</td>
<td>Lists all devices in groups and subgroups based on their Device Category, S</td>
</tr>
<tr>
<td></td>
<td>ies, and Model. By default, the device grouping is based on their Device C</td>
</tr>
<tr>
<td></td>
<td>ategories such as Routers, Switches, and Hubs.</td>
</tr>
</tbody>
</table>
Working with IPSLA Collectors

Step 3  Select one or more target devices from the Target Devices list.

For more information on selecting the Target device, see Table 15-12.

Table 15-12  Using the Target Devices List

<table>
<thead>
<tr>
<th>Folder Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Input</td>
<td>Enter your search expression in this text field.</td>
</tr>
<tr>
<td></td>
<td>You can enter a single device name or multiple device names in this field.</td>
</tr>
<tr>
<td></td>
<td>You can enter the following as search inputs to search multiple devices:</td>
</tr>
<tr>
<td></td>
<td>• Comma separated list of full device names</td>
</tr>
<tr>
<td></td>
<td>• Device names with wildcard characters * and ? to search for multiple devices</td>
</tr>
<tr>
<td></td>
<td>• Combination of comma separated list of device names, and device names with</td>
</tr>
<tr>
<td></td>
<td>wildcard characters.</td>
</tr>
<tr>
<td>All</td>
<td>Lists all the devices that are available to manage IPSLA Monitoring functionality.</td>
</tr>
<tr>
<td>Selection</td>
<td>Lists all the devices that you have selected in the All or Search Results tab or through a combination of both.</td>
</tr>
<tr>
<td>Search Results</td>
<td>Displays the Simple search results. From the search result, you can:</td>
</tr>
<tr>
<td></td>
<td>• Select all devices</td>
</tr>
<tr>
<td></td>
<td>• Clear all devices</td>
</tr>
<tr>
<td></td>
<td>• Select a few devices</td>
</tr>
<tr>
<td>All Devices</td>
<td>Lists all the devices in the application in the alphabetical order of their display names. The display names are defined when you have added the devices in DCR.</td>
</tr>
<tr>
<td>Device Type Groups</td>
<td>Lists all devices in groups and subgroups based on their Device Category, Series, and Model. By default, the device grouping is based on their Device Categories such as Routers, Switches, and Hubs.</td>
</tr>
<tr>
<td>User-Defined Groups</td>
<td>Lists IPSLA devices that satisfy the group rules. The group rules are defined by you when you create the User-Defined groups.</td>
</tr>
<tr>
<td>Subnet Groups</td>
<td>Lists Subnet-based groups</td>
</tr>
<tr>
<td>Medianet Endpoint Connected Groups</td>
<td>Lists the group of devices connected with Medianet Endpoints.</td>
</tr>
<tr>
<td>Responder Enabled Devices</td>
<td>Lists all the responder enabled target devices. UDP Jitter operation uses Responder Enabled target devices.</td>
</tr>
<tr>
<td>Adhoc Target</td>
<td>Lists all the external target devices added to manage IPSLA Monitoring functionality.</td>
</tr>
</tbody>
</table>
Working with IPSLA Collectors

The Target List does not apply to the Gatekeeper Registration Delay, Post Dial Delay operations, Ethernet Jitter Auto IP SLA and Ethernet Ping Auto IP SLA, because they do not support Target devices. For Ethernet Jitter and Ethernet Ping the maintenance endpoint ID (MEPID), which is in the operation, is considered as the target.

Step 4  Select one or more operations from the Operations list.
Step 5  Enter a valid IP address in the Source Interface field.
   This is the IP address of the source device interface to which the packets are returned from the destination. The Source Interface field is an optional field.
   The Source Interface field is not applicable for Ethernet operations.
Step 6  Click Next.
   The Select Collector page appears.

Viewing the Collector List

The Collector Management page displays all the operation-based (system-defined) and user-defined collectors, and their details, such as collector name, source, target, operation, start time, end date, collector type, and status.

You can perform the following tasks on this page:

- Listing Operation-Based (System-Defined) Groups
  Lists collectors based on the default operation types. The operation-based groups are also referred to as system-defined groups.
- Listing User-Defined Groups
  Lists collectors based on the groups defined by users in Group Administration.
  For more information, see Creating User-Defined Collector Groups.
- Filtering the Collector List
  Allows you to filter the collector list.
- Sorting the Collector List
  Allows you to sort the collector list.

Note

You can also use a combination of operation-based groups and user-defined groups to list the collectors.

Listing Operation-Based (System-Defined) Groups

To list collectors based on operation-based groups:

Step 1  Select Monitor > Performance Settings > IPSLA > Collectors.
   The Collector Management page appears with the list of collectors.
Step 2  Select the required operation from the Operation Based Groups folder in the left pane.
   For example, to list collectors based on the operation, ‘FTP’, select the FTP check box.
Step 3  Click **List Collectors**.
The collector list for the selected operation appears in the right pane.
You can further filter this list of collectors. For more information, see Filtering the Collector List.

Listing User-Defined Groups
To list collectors based on user-defined groups:

Step 1  Select **Monitor > Performance Settings > IPSLA > Collectors**.
The Collector Management page appears with the list of collectors by default.

Step 2  Select the required user-defined group from the left pane.
For example, to list collectors based on the location, ‘USCollectors’, select the ‘USCollectors’ check box.
For more information on user-defined group, see Managing Collector Groups.

Step 3  Click **List Collectors**.
The collector list for the selected user-defined group appears in the right pane.
You can further filter this list of collectors. For more information, see Filtering the Collector List.

Sorting the Collector List
To sort the collector list, click one of the column titles. By default, the information is sorted based on collector name. Optionally, you can sort the information based on other parameters such as start time, target, or operation type.

Viewing the Collector Details
To view the collector details:

Step 1  Select **Monitor > Performance Settings > IPSLA > Collectors**.
The Collector Management page appears with the list of collectors.

Step 2  Select the collector for which you want to view the details from the Collector List section.

Step 3  Click **View**.
The Collector Details window appears. For more information, see Table 15-13.

Step 4  Click **OK**.
### Table 15-13 Collector Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Collector name specified while defining a collector.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the collector specified while defining a collector.</td>
</tr>
<tr>
<td>Operation Name</td>
<td>The name of the operation while defining a collector.</td>
</tr>
<tr>
<td>Admin Index</td>
<td>Unique number that represents each collector on the device.</td>
</tr>
<tr>
<td>VRF Name</td>
<td>VRF name of the collector.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Source Interface details.</td>
</tr>
<tr>
<td>Last Modified Time</td>
<td>Last modified time of the collector.</td>
</tr>
</tbody>
</table>

**Source Device details obtained when a collector was last configured by IPSLA Monitoring function**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Display name of the device specified while adding the device in DCR.</td>
</tr>
<tr>
<td>IOS Version</td>
<td>Displays the IOS version of the source device.</td>
</tr>
<tr>
<td>IP SLA Version</td>
<td>Displays the IP SLA version of the source device.</td>
</tr>
<tr>
<td>Max Collectors</td>
<td>Maximum number of collectors the source device supports.</td>
</tr>
<tr>
<td>New Collectors Capacity</td>
<td>Number of collectors that you can configure on the source router.</td>
</tr>
<tr>
<td>Last snmp Set Time</td>
<td>Date and time when the source device was last modified while creating or modifying a collector.</td>
</tr>
<tr>
<td>Last reboot Time</td>
<td>Last reboot time of the source device.</td>
</tr>
</tbody>
</table>

**Target Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Display name of the device specified while adding the device in DCR.</td>
</tr>
<tr>
<td>Responder Enabled</td>
<td>Displays whether the target device is Responder Enabled or not.</td>
</tr>
</tbody>
</table>

**Scheduling Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling Type</td>
<td>Displays whether the collector type is Historical or Monitored/Real-time.</td>
</tr>
<tr>
<td>Start Date</td>
<td>Displays the start date specified while creating collectors.</td>
</tr>
<tr>
<td>End Date</td>
<td>Displays the end date specified while creating collectors.</td>
</tr>
</tbody>
</table>

**Polling Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling Interval (mins)</td>
<td>Polling time interval specified while creating a collector.</td>
</tr>
</tbody>
</table>

**Note** If you create a Video collector with polling frequency as 1 minute or 5 minutes, the same statistics will be populated for every 15 minutes in the video_minute_stats table for that collector. This is applicable when you have created a Video operation with default sample interval.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling Time</td>
<td>Start and end time of the polling time specified while creating a collector.</td>
</tr>
<tr>
<td>Days of Week</td>
<td>Displays days of the week when polling happens, specified while creating a collector.</td>
</tr>
</tbody>
</table>
Editing a Collector

You can edit the description and the scheduling details of a collector. You cannot edit the details of a source, target, or operation.

**Note**

You are not allowed to edit individual IPSLA Ethernet auto discovered collectors.

To edit a collector:

**Step 1** Select `Monitor > Performance Settings > IPSLA > Collectors`.

The Collector Management page appears with the list of collectors.

**Step 2** Select the required collector from the Collector List section to edit.

**Step 3** Click *Edit*.

The Collector Configuration page displays the configuration details of the selected collector.

**Step 4** Modify the following fields, if required, in the Collector Info section:

- Collector Name
- Description

**Step 5** Modify the Source Interface field, if required, in the Selected Devices Info section.

You cannot modify the Source Device, Target Device, VRF Name and Operation fields in this section.

**Step 6** Click *Next*.

The Schedule page appears with the scheduling details.

**Step 7** Edit the following fields, if required:

- End Time Details
- Poller Settings

For more information on these fields, see *Scheduling Collectors*.

**Step 8** Click *Next*.

The Summary page appears with the updated information for the selected collector.

For more information on the Summary page, see *Table 15-13*.

**Step 9** Click *Finish*.

A message appears that the selected collector’s information is updated successfully.

**Step 10** Click *OK*.

Deleting Collectors

Using the Delete option, you can delete collectors that you no longer need. When you delete a collector, the collector configured on the source router and the data stored in the database are deleted.
After deleting, the collector remains in the Delete Pending state until the data is completely deleted from the IPSLA Monitoring database. It may take several minutes or more to delete a collector that has a large amount of statistics information stored in the IPSLA Monitoring database. You can delete more than one collector at a time.

If you want to delete a collector in the Running status, you must first move the collector to the Stop status before attempting to delete.

**Note**

You are not allowed to delete individual IPSLA Ethernet auto discovered collectors.

To delete collectors:

**Step 1** Select Monitor > Performance Settings > IPSLA > Collectors.

The Collector Management page appears with the list of collectors.

**Step 2** Select the collectors that you want to delete.

**Step 3** Click Delete.

The Delete Confirmation dialog box appears.

**Step 4** Click OK.

The selected collectors are deleted from IPSLA Monitoring functionality.

---

**Viewing Collector Graphs**

You can use the Graph option to view the collector statistics or compare the latency of the collectors (overlay graphs) based on the granularity and the report period. To generate overlay graphs, you must select collectors in Running, Completed, Dormant, or Stopped status.

**Note**

You cannot view graphs for AutoIPSLA Ethernet collectors.

To view the collector statistics:

**Step 1** Select Monitor > Performance Settings > IPSLA > Collectors.

The Collector Management page appears.

**Step 2** Select the required collectors from the Collector List.

**Step 3** Click Graph.

The Graph Settings window appears.

**Step 4** Select the type of graph from the Type drop-down list.

The available graph types are Availability and Latency.

Based on the collector you select, the report type is added in the drop-down list apart from Availability and Latency.

For example, if you choose RTP collector, RTP report type gets added in the Type drop-down list.
The outage option is not available when you select more than one collector.

When you select more than one collectors, the Graph Type drop-down list is not displayed.

**Step 5**
Select one of the following granularity from the Granularity section:
- Minute
- Hourly
- Daily
- Weekly
- Monthly

**Step 6**
Specify the following in the Report Period section:
- From—Select the start date and time of your report. You can select the date from the calendar icon and the time from the drop-down list.
- To—Select the end date and time of your report. You can select the date from the calendar icon and the time from the drop-down list.
- Outage Option—The outage option is not available when you select more than one collectors.

You can:
- Check the Exclude Planned Outage Periods check box to exclude the outage period details.
- Or
- Uncheck the Exclude Planned Outage Periods check box to include the outage period details.

**Step 7**
Click OK.
A Graph appears displaying the statistics for the selected collector.
- If you have checked the Exclude Planned Outage Period check box, the graph will not display the outage details.
- If you have unchecked the Exclude Planned Outage Period check box, the outage period will be watermarked in the graph and highlighted in red.

To know more about the graphs, see the following sections in Reports Management with Cisco Prime LAN Management Solution 4.1 document:
- Availability Reports and Graphs
- Latency (Round-Trip Time) Reports and Graphs
- UDP Jitter Reports and Graphs
- HTTP Reports and Graphs
- ICMP Jitter Reports and Graphs
- Path Echo Reports and Graphs
- RTP Reports and Graphs
- Ethernet Jitter Reports and Graphs
- Video Jitter Reports and Graphs
To overlay Collector graphs:

**Step 1**  
Select **Monitor > Performance Settings > IPSLA > Collectors**.  
The Collector Management page appears.

**Step 2**  
Select the required collectors from the Collector List.

**Step 3**  
Click **Graph**.  
The Graph Settings window appears.

**Step 4**  
Select the type of graph from the Type drop-down list.  
The available graph types are Availability and Latency.  
Based on the collector you select, the report type is added in the drop-down list apart from Availability and Latency.  
For example, if you choose RTP collector, RTP report type gets added in the Type drop-down list.

**Step 5**  
Select the granularity period from the Granularity section:
- Minute
- Hourly
- Daily
- Weekly
- Monthly

**Step 6**  
Specify the following in the Report Period section:
- From—Select the start date and time of your report. You can select the date from the calendar icon and the time from the drop-down list.
- To—Select the end date and time of your report. You can select the date from the calendar icon and the time from the drop-down list.

**Step 7**  
Click **OK**.  
A Graph appears displaying the latency for the selected collectors, where:
- X-axis represents the range of time period you have selected.
- Y-axis represents the latency of the selected collectors.
  
Each data point has a tooltip that displays the collector name, operation type, date, and time.  
**Figure 15-1** represents a sample overlay graph.
Figure 15-1 Overlay Graphs

There may be instances where the graphs of different collectors may overlap each other. So to view a particular graph curve, you can click on the legends available. This allows you to view only a particular graph corresponding to that selected legend.

Exporting Collector Configuration Information

You can export a list of collectors and their credentials from IPSLA Monitoring User Interface into CSV file. For detailed information on the format of the CSV file, see Format of the CSV File.

Note

You are not allowed to export IPSLA-generated collectors and their credentials.

The exported file is stored at:

Solaris or Soft Appliance:
- `/var/adm/CSCOpx/files/ipm/export/collectors`

Windows:
- `NMSROOT\files\ipm\export\collectors`
To export collector configuration information:

**Step 1**  Select *Monitor > Performance Settings > IPSLA > Collectors.*

The Collector Management page appears with the list of collectors.

**Step 2**  Select the collectors that you want to export.

**Step 3**  Click *Export.*

The Export Collector window appears.

**Step 4**  Specify the file/directory location and the directory content in the Collector File text box.

or

Click the **Browse** hyperlink to select a folder on the IPSLA Monitoring server.

The Server Side File Browser window displays the default file/directory location and the directory contents.

a.  Select the required file/directory location and the directory content on the IPSLA Monitoring server.

b.  Click **OK.**

The Export Collector window appears with the specified information.

**Step 5**  Click **OK.**

A message appears that the selected collectors are exported successfully.

**Step 6**  Click **OK.**
### Sample Exported Collector File

Here are the columns of the file.

- Columns 1, 3, 5, 6, 9-14 are required.
- Columns 2, 7, 8 are optional.
- Column 4 is not applicable for DHCP, GatekeeperRegistrationDelay,
  CallSetupPostDialDelay, EthernetPingAutoIPSLA, EthernetJitterAutoIPSLA
  Operation types and should be left empty.
  For the Operations Ethernetjitter, Ethernetping represents MEPID.

<table>
<thead>
<tr>
<th>Col#</th>
<th>Description</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Col# 1: Collector Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Col# 2: Description of the collector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Col# 3: Source display name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Col# 4: Target display name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Col# 5: Operation name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Col# 6: Operation Type</td>
<td>1 - Echo, 2 - PathEcho, 9 - UDP Jitter, 22 - Video</td>
<td></td>
</tr>
<tr>
<td>Col# 7: Vrf Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Col# 8: Source Interface Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Col# 9: Collector type</td>
<td>1 - Historical, 2 - Realtime</td>
<td></td>
</tr>
<tr>
<td>Col# 10: Start date (must be in MM/DD/YYYY)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Col# 11: End date (must be in MM/DD/YYYY)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Col# 12: Poll Start time (hh:mm:ss)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Col# 13: Poll End time (hh:mm:ss)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Col# 14: Days of week (must be between 1-127)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Col# 15: Poll Interval (must be in milliseconds)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Example for Echo Collector:

```
; test_Echo_Collector, ,10.77.209.9,10.76.90.106-NAM2,Test_Echo_Operation,1,blue,
,1,07/29/2008,01/31/2021,00:00:00,00:00:00,127,3600000
```

#### Example for DHCP Collector:

```
; test_DHCP_collector, ,10.77.209.9,,Test_DHCP_Operation,11,
,1,07/29/2008,01/31/2021,00:00:00,00:00:00,127,3600000
```

#### Here are the rows of data.
Importing Collector Configuration Information

You can import the collector configuration information from an external location within the IPSLA Monitoring server or reuse the exported collector file information.

You can import the collectors with previous versions of IPSLA Monitoring file format. Collectors will be created without VRF details.

For detailed information on the format of the CSV file, see Format of the CSV File.

To import collector configuration information from a CSV file to IPSLA Monitoring:

---

**Step 1** Select Monitor > Performance Settings > IPSLA > Collectors.

The Collector Management page appears with the list of collectors.

**Step 2** Click Import.

The Select Import File window appears.

**Step 3** Specify the file/directory location and the directory content in the Collector File text box.

or

Click the **Browse** hyperlink.

The Server Side File Browser window displays the default file/directory location and the directory contents.

a. Select the required file/directory location and the directory content on the IPSLA Monitoring server.

a. Click **OK**.

The Select Import File window appears with the specified information.

**Step 4** Click **OK**.

A message appears that the selected collectors are imported successfully.

**Step 5** Click **OK**.
Format of the CSV File

The CSV file should have the following fields:

<table>
<thead>
<tr>
<th>Name of the Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector Name</td>
<td>Specify the name of the collector.</td>
<td>echo_coll1_10.77.209.209_echo</td>
</tr>
<tr>
<td>Description</td>
<td>Specify a brief description about the collector. This column is optional.</td>
<td></td>
</tr>
<tr>
<td>Source Display Name</td>
<td>Specify the display name of the source device</td>
<td>10.77.209.3</td>
</tr>
<tr>
<td>Target Display Name</td>
<td>Specify the display name of the target device.</td>
<td>10.77.209.209</td>
</tr>
<tr>
<td></td>
<td>The value of this column should be blank for the following operations:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DHCP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• GatekeeperRegistrationDelay</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CallSetupPostDialDelay</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EthernetPingAutoIPSLA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EthernetJitterAutoIPSLA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the Operation Type is Ethernet Jitter or Ethernet Ping, the value of this column will be MEPID.</td>
<td></td>
</tr>
<tr>
<td>Operation Name</td>
<td>You can specify either the system defined or user-defined operations. The name is case-sensitive.</td>
<td>Echo</td>
</tr>
</tbody>
</table>
### Working with IPSLA Collectors

#### Operation Type
Specify the numeric value associated with the Operation Types. They are:
- **Echo Operations**
  - Echo = 1
  - Path Echo = 2
  - UDP Echo = 5
- **Jitter Operations**
  - UDP Jitter = 9
  - ICMP Jitter = 16
- **Services Operations**
  - DNS = 8
  - DHCP = 11
  - HTTP = 7
  - FTP = 12
  - DLSw = 10
  - TCP Connect = 6
- **VoIP Operations**
  - Call Setup Post Dial Delay = 18
  - Gatekeeper Registration Delay = 19
  - RTP = 14
- **Metro Ethernet Operations**
  - Ethernet Ping = 1019
  - Ethernet Jitter = 1020
  - Ethernet Ping Auto IP SLA = 1119
  - Ethernet Jitter Auto IP SLA = 1120
- **Video Operation** = 22

#### Vrf Name
Specify the VRF name. This column is optional.

#### Source Interface Address
Specify the source interface address. This column is optional.

#### Collector Type
Specify the numeric value associated with the type of collector. It can be:
- Historical = 1
- Real-time = 2

#### Start Date
Specify the start date in the MM/DD/YYYY format.

#### End Date
Specify the end date in the MM/DD/YYYY format.

#### Poll Start Time
Specify the poll start time in the Hour:Minutes:Seconds format.

<table>
<thead>
<tr>
<th>Name of the Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation Type</td>
<td>Specify the numeric value associated with the Operation Types. They are:</td>
<td>1</td>
</tr>
<tr>
<td>Vrf Name</td>
<td>Specify the VRF name. This column is optional.</td>
<td></td>
</tr>
<tr>
<td>Source Interface Address</td>
<td>Specify the source interface address. This column is optional.</td>
<td></td>
</tr>
<tr>
<td>Collector Type</td>
<td>Specify the numeric value associated with the type of collector. It can be:</td>
<td>1</td>
</tr>
<tr>
<td>Start Date</td>
<td>Specify the start date in the MM/DD/YYYY format.</td>
<td>08/27/2009</td>
</tr>
<tr>
<td>End Date</td>
<td>Specify the end date in the MM/DD/YYYY format.</td>
<td>01/31/2021</td>
</tr>
<tr>
<td>Poll Start Time</td>
<td>Specify the poll start time in the Hour:Minutes:Seconds format.</td>
<td>0:00:00</td>
</tr>
</tbody>
</table>
### Monitoring a Collector

You can use the Monitor option to monitor the real-time statistics of a collector in the Running status. The statistical data displayed is not stored in the IPSLA Monitoring database. You can view the real-time graph for both Historical/Statistical and Monitored/Real-Time collectors. You can monitor more than one collector’s statistics in real time.

The sample interval, in the report, indicates the frequency at which the values are plotted on the real-time graph. For example, if the sample interval is 60 seconds, the values in the graphs are plotted every 60 seconds. The sample interval depends on the operation used by the collector.

#### Note

You cannot monitor AutoIPSLA Ethernet collectors.

To monitor a collector:

**Step 1** Select **Monitor > Performance Settings > IPSLA > Collectors**.

The Collector Management page appears with the list of collectors.
Step 2  Select one of the following collectors for monitoring.
- A collector in Running status if the collector type is Historical/Statistical.
- A collector that has the collector type as Monitor/Real-Time.

Step 3  Click Monitor.
A Real-Time graph appears.
To know more about the graphs, see the following sections in Reports Management with Cisco Prime LAN Management Solution 4.1 document:
- Availability Reports and Graphs
- Latency (Round-Trip Time) Reports and Graphs
- UDP Jitter Reports and Graphs
- HTTP Reports and Graphs
- ICMP Jitter Reports and Graphs
- Path Echo Reports and Graphs
- RTP Reports and Graphs
- Ethernet Jitter Reports and Graphs
- Video Jitter Reports and Graphs

Stopping the Collectors

You can use the Stop option to stop the collectors in Running status. As a result of stopping, the collectors become inactive on the source router and the data polling is stopped.

Note  You are not allowed to stop individual IPSLA Ethernet auto discovered collectors.

To stop the collectors:

Step 1  Select Monitor > Performance Settings > IPSLA > Collectors.
The Collector Management page appears with the list of collectors.

Step 2  Select the collectors check box that you want to stop.
The selected collectors must be in the Running status.

Step 3  Click Stop.
The Stop Confirmation dialog box appears.

Step 4  Click OK.
The selected collectors are stopped.
Starting the Collectors

You can use the Start option to start the stopped collectors. As a result of starting, the collector is activated on the source device and IPSLA Monitoring starts polling.

**Note**
You are not allowed to start individual IPSLA Ethernet auto discovered collectors.

To start the collectors:

1. **Step 1** Select Monitor > Performance Settings > IPSLA > Collectors.
   The Collector Management page appears with the list of collectors.
2. **Step 2** Select the collectors in Stopped status.
3. **Step 3** Click **Start** to start the stopped collectors.

Reconfiguring Collectors

You can reconfigure collectors that are in Config Failed state and Source Not Responding State.

To reconfigure collectors:

1. **Step 1** Select Monitor > Performance Settings > IPSLA > Collectors.
   The Collector Management page appears with the list of collectors.
2. **Step 2** Click **Reconfigure** to reconfigure collectors in the Config Failed state and Source Not Responding State.
   The Reconfigure Collectors window appears with the list of Config Failed collectors and Source Not Responding State.

**Note**
The Reconfigure page does not list the collectors that are moved to the Source Not Responding state during polling. This is because these collectors are already configured and running on the device. These collectors will move to Running state during the next polling cycle.

Alternatively, you can select one or more source devices and click this button to view the Config Failed collectors associated with the source devices. Also, you can click **Filter** to filter the collectors based on criteria.

For more information on how to filter collectors, see Filtering Collectors.

3. **Step 3** Check the collectors and click:
   - **Reconfigure**, to reconfigure the collectors.
   - **Delete**, to delete the collectors.

You can also click **Cancel** to revert to the Collector Management window without reconfiguring collectors.
Managing Operations

This chapter provides details on using IPSLA Monitoring to measure latency, jitter, availability, and errors. It contains the following topics:

- Overview of IPSLA Operations
- Understanding the List of IPSLA Operations
- Using IPSLA Operations to Measure Network Performance

Overview of IPSLA Operations

IPSLA is a portfolio of technology embedded in most devices that run Cisco IOS software. This allows you to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce the frequency of network outages.

IPSLA uses active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance.

IPSLA Monitoring supports the following IPSLA operations:

- Echo Operations
  - Echo
  - Path Echo
  - UDP Echo (User Data Protocol)
- Jitter Operations
  - ICMP Jitter (Internet Control Message Protocol)
  - UDP Jitter (User Data Protocol)
- VoIP Operations
  - Call Setup Post Dial Delay
  - Gatekeeper Registration Delay
  - RTP (Real-time Transfer Protocol)
• Operation based on Services
  - DNS (Domain Name System)
  - DHCP (Dynamic Host Configuration Protocol)
  - HTTP (HyperText Transfer Protocol)
  - FTP (File Transfer Protocol)
  - DLSw (Data-link Switching)
  - TCP Connect
• Metro Ethernet Operations
  - Ethernet Ping
  - Ethernet Jitter
  - Ethernet Ping Auto IPSLA
  - Ethernet Jitter Auto IPSLA
• Video Operation

For IPSLA Monitoring operations, the IPSLA Monitoring Request size does not include the size of the headers added by the respective layers. The header size varies according to the type of the IP SLA operation. The overhead added by different layers are as follows:

• TCP Layer - 20 bytes
• UDP Layer - 8 bytes
• IP Layer - 20 to 60 bytes
• ICMP Layer - 8 bytes
• IP SLA - 8 bytes

Predefined IP SLA Operations

When you select to manage IPSLA Monitoring functionality, a group of predefined operations are provided. Table 16-1 describes the predefined operations.

You can define one or more new operations to fit your needs. Although, you cannot modify the default operations, you can use them as templates for creating your own operations.

Note
IPSLA Monitoring does not provide a predefined HTTP, FTP, or RTP operation. Therefore, before you create a HTTP, FTP, or RTP collector, you must first create the respective HTTP, FTP, or RTP operation.

<table>
<thead>
<tr>
<th>Table 16-1 Predefined Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations</td>
</tr>
<tr>
<td>Echo Operations</td>
</tr>
<tr>
<td>Default Echo</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Default Path Echo

Measures hop-by-hop latency in an IP network.

- Packet Priority is set to 0 (no priority)
- Request Payload is set to 64 bytes
- Maximum Paths is set to 5
- Maximum Hops is set to 15
- Sample interval is set to 180 seconds

This operation is denoted as ‘DefaultIpPathEcho’.

Default UDP Echo

Measures end-to-end latency for a UDP datagram. Packet Priority is set to 0 (no priority), Request Payload is set to 64 bytes, and Target Port is set to 7.

This operation is denoted as ‘DefaultUDPEcho’.

Jitter Operations

Default ICMP Jitter

Measures network performance by generating a stream of ICMP packets between a Cisco IOS device (source) and IP device (destination).

You need not use Responder Enabled target device for this jitter operation since this is mainly used for non-Cisco devices.

This operation is denoted as ‘DefaultICMPJitter’.

Default UDP Jitter

Measures round-trip latency, packet loss, and jitter in IP networks by generating synthetic UDP traffic.

You must use Responder Enabled target devices for this operation.

IPSLA Monitoring supports the following default UDP jitter operations:

- Default60ByteVoice
- Default160ByteVoice
- DefaultVPN
- DefaultVideo

Default VOIP Post Dial Delay

Measure your network’s response time for setting up a Voice over IP (VoIP) call.

This operation is denoted as ‘CallSetupPostDialDelay’.

Default VOIP Gatekeeper Registration Delay

Measures the average, median, or aggregated response time (delay) of registration attempts from a VoIP source router to a VoIP gatekeeper device.

This operation is denoted as ‘GatekeeperRegistrationDelay’.

Operations based on services

Default DNS

Measures end-to-end latency for DNS lookups. DNS Name Server is set to the IP address of the DNS server configured on the system on which the IPSLA Monitoring server is running. The DNS Lookup Name is set to the name of the host to look up for the DNS request.

When you create a non-default operation, it is mandatory to specify a DNS Name Server.

This operation is denoted as ‘DefaultDNS’.

<table>
<thead>
<tr>
<th>Table 16-1</th>
<th>Predefined Operations (continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operations</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| Default Path Echo | Measures hop-by-hop latency in an IP network.
- Packet Priority is set to 0 (no priority)
- Request Payload is set to 64 bytes
- Maximum Paths is set to 5
- Maximum Hops is set to 15
- Sample interval is set to 180 seconds
This operation is denoted as ‘DefaultIpPathEcho’.
| Default UDP Echo | Measures end-to-end latency for a UDP datagram. Packet Priority is set to 0 (no priority), Request Payload is set to 64 bytes, and Target Port is set to 7.
This operation is denoted as ‘DefaultUDPEcho’.
| Jitter Operations | |
| Default ICMP Jitter | Measures network performance by generating a stream of ICMP packets between a Cisco IOS device (source) and IP device (destination).
You need not use Responder Enabled target device for this jitter operation since this is mainly used for non-Cisco devices.
This operation is denoted as ‘DefaultICMPJitter’.
| Default UDP Jitter | Measures round-trip latency, packet loss, and jitter in IP networks by generating synthetic UDP traffic.
You must use Responder Enabled target devices for this operation.
IPSLA Monitoring supports the following default UDP jitter operations:
- Default60ByteVoice
- Default160ByteVoice
- DefaultVPN
- DefaultVideo
| Default VOIP Post Dial Delay | Measure your network’s response time for setting up a Voice over IP (VoIP) call.
This operation is denoted as ‘CallSetupPostDialDelay’.
| Default VOIP Gatekeeper Registration Delay | Measures the average, median, or aggregated response time (delay) of registration attempts from a VoIP source router to a VoIP gatekeeper device.
This operation is denoted as ‘GatekeeperRegistrationDelay’.
| Operations based on services | |
| Default DNS | Measures end-to-end latency for DNS lookups. DNS Name Server is set to the IP address of the DNS server configured on the system on which the IPSLA Monitoring server is running. The DNS Lookup Name is set to the name of the host to look up for the DNS request.
When you create a non-default operation, it is mandatory to specify a DNS Name Server.
This operation is denoted as ‘DefaultDNS’.

Understanding the List of IPSLA Operations

This section explains how to manage the IPSLA operations.
It contains the following topics:

- Overview of List of Operations Page
- Viewing the List of Defined Operations
- Creating User-Defined Operations
- Editing User-Defined Operations
- Deleting User-Defined Operations
- Viewing Operation Properties

<table>
<thead>
<tr>
<th>Operations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default DHCP</td>
<td>Measures end-to-end latency for acquiring a new DHCP lease. This operation is denoted as ‘DefaultDHCP’.</td>
</tr>
<tr>
<td>Default DLSw</td>
<td>Measures end-to-end latency in a network which uses DLSw to route SNA traffic over an IP network. Request size is set to 64 and Response Payload is set to 64. This operation is denoted as ‘DefaultDLSw’.</td>
</tr>
</tbody>
</table>
| Default TCP Connect | Measures round-trip latency between a source and any IP-enabled device running TCP services. Latency is computed by measuring the time taken by the source to perform a TCP Connect operation to the target device. IPSLA Monitoring supports the following default TCP Connect operations:  
  - DefaultSMTP  
  - DefaultPOP3  
  - DefaultTELnet  
  - DefaultNNTP |

Table 16-1 Predefined Operations (continued)
Overview of List of Operations Page

The List of Operations page (Table 16-2) lists all the IPSLA Operations (Monitor > Performance Settings > IPSLA > Operations). This page contains the following pane, icon, and buttons:

Table 16-2 List of Operations Page

<table>
<thead>
<tr>
<th>Pane/Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of Operations</td>
<td>Lists all IPSLA operations. The operations are identified by the Operation Name that you have entered while creating them.</td>
</tr>
<tr>
<td>Filter</td>
<td>Filters the list of operations based on the following:</td>
</tr>
<tr>
<td></td>
<td>• All</td>
</tr>
<tr>
<td></td>
<td>• Operation Name</td>
</tr>
<tr>
<td></td>
<td>• Operation Type</td>
</tr>
<tr>
<td></td>
<td>• Create Type</td>
</tr>
<tr>
<td></td>
<td>For more information, see Filtering List of Operations</td>
</tr>
<tr>
<td>Create</td>
<td>Allows you to create a user-defined operation.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Creating User-Defined Operations.</td>
</tr>
<tr>
<td>Edit</td>
<td>Allows you to edit a user-defined operation.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Editing User-Defined Operations.</td>
</tr>
<tr>
<td>Delete</td>
<td>Allows you to delete user-defined operations.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Deleting User-Defined Operations.</td>
</tr>
<tr>
<td>View</td>
<td>Allows you to view the details of a system-defined or user-defined operation.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Viewing Operation Properties.</td>
</tr>
<tr>
<td>Refresh (Icon)</td>
<td>Allows you to refresh the list of operations.</td>
</tr>
</tbody>
</table>
Understanding the List of IPSLA Operations

Viewing the List of Defined Operations

The List of Operations page allows you to view the list of system-defined and user-defined operations and filter the list of operations.

To view the list of defined operations, select **Monitor > Performance Settings > IPSLA > Operations** from the menu.

The List of Operations page appears with the list of system-defined and user-defined operations.

**Filtering List of Operations**

Using the Filter field in the List of Operations page, you can filter the operations. You can filter the operations using one of the following fields and clicking **Filter**. For more information, see Table 16-3.

**Table 16-3 Filtering List of Operations Page**

<table>
<thead>
<tr>
<th>Fields for Filtering</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Displays all operations.</td>
</tr>
<tr>
<td>Operation Name</td>
<td>Enter the complete or a part of the Operation name that you want to display.</td>
</tr>
</tbody>
</table>
### Table 16-3 Filtering List of Operations Page

<table>
<thead>
<tr>
<th>Fields for Filtering</th>
<th>Description</th>
</tr>
</thead>
</table>
| Operation Type       | Enter the complete or a part of the Operation type that you want to display. The operation types available are:  
  - Echo  
  - PathEcho  
  - UDPEcho  
  - ICMPJitter  
  - UDP Jitter  
  - CallSetupPostDialDelay  
  - GatekeeperRegistrationDelay  
  - RTP  
  - DNS  
  - DHCP  
  - HTTP  
  - FTP  
  - DLSw  
  - TCPConnect  
  - EthernetPing  
  - EthernetJitter  
  - EthernetPingAutoIPSLA  
  - EthernetJitterAutoIPSLA  
  - Video |
| Create Type          | Enter the complete or a part of the Create type that you want to display. The Create types available are:  
  - System Defined  
  - User Defined |
Example 1:
If you want to filter the Operations based on Operation Type and with value UDP:
1. From the Filter Drop down, select Operation Type.
2. In the Filter text area enter UDP
3. Click Filter
   By default the filter operation uses “contains” to filter the Operations. All those Operation Types that contain the value UDP are filtered and provided in the results:
   UDPJitter
   UDPEcho

Example 2:
If you want to filter the Operations based on Operation Name and with value Default:
1. From the Filter Drop down, select Operation Name.
2. In the Filter text area enter Default
3. Click Filter
   By default the filter operation uses “contains” to filter the Operations. All those Operation Names that contain the value Default are filtered and provided in the results:
   DefaultVideo
   DefaultVPN
   EchoDefault

Example 3:
Let us say, you want to filter the Operations based on Create Type and with value SYSTEM:
1. From the Filter Drop down, select Create Type.
2. In the Filter text area enter SYSTEM
3. Click Filter
   By default the filter uses “contains” to filter the Operations. All the System Defined operations are filtered and provided in the results.
Creating User-Defined Operations

IPSLA Monitoring function provides a single wizard-based approach that leads you through the procedure to create multiple user-defined operations. While creating these operations, you can use the system-defined operation template and modify only the required parameters for that operation.

This wizard process involves the following four steps:

- General Settings for a User-Defined Operation
- Specific Settings for a User-Defined Operation
- Viewing the Summary of a User-Defined Operation

You must complete all the four tasks in this sequence to create user-defined operations. If you exit the wizard at any stage using Cancel, the details you have specified will be lost and the user-defined operation will not be created.

General Settings for a User-Defined Operation

The General Settings page allows you to define operation details, and threshold, timeout, and miscellaneous settings.

To specify the general settings for a user-defined operation:

**Step 1**
Select Monitor > Performance Settings > IPSLA > Operations from the menu.

The List of Operations page appears.

**Step 2**
Click Create.

The General Settings page appears.

**Step 3**
Specify the following in the General Settings dialog box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter an operation name.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a brief description of the operation, including its purpose.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the operation type from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>For example, if you want to create a Video operation, select Video from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Using IPSLA Operations to Measure Network Performance.</td>
</tr>
</tbody>
</table>
### Table 16-4  General Settings for Operations  (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reaction Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Reaction Type</td>
<td>Select the applicable Reaction types to monitor.</td>
</tr>
<tr>
<td></td>
<td>For example, if you have selected the Operation Type as Video, the following reaction types will be displayed:</td>
</tr>
<tr>
<td></td>
<td>- connectionLoss</td>
</tr>
<tr>
<td></td>
<td>- iaJitterSD</td>
</tr>
<tr>
<td></td>
<td>- jitterSDAvg</td>
</tr>
<tr>
<td></td>
<td>- latencySDAvg</td>
</tr>
<tr>
<td></td>
<td>- packetLossSD</td>
</tr>
<tr>
<td></td>
<td>- timeout</td>
</tr>
<tr>
<td></td>
<td>For more information on Reaction types, see <a href="#">Specifying Reaction Types</a>.</td>
</tr>
<tr>
<td>General Action Event</td>
<td>Select one of threshold violation type for the selected reaction type:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Never</strong>—Do not calculate threshold violations. This is the default setting.</td>
</tr>
<tr>
<td>Action Event Type</td>
<td>Select the action event type as <strong>None</strong> or <strong>SNMP Trap</strong> from the drop-down list</td>
</tr>
<tr>
<td>Rising Threshold (msecs)</td>
<td>Enter a value for rising threshold in milliseconds. The value entered should be greater than the Falling Threshold value.</td>
</tr>
<tr>
<td></td>
<td>Rising and Falling thresholds are disabled for timeout, verifyErrors and connectionLoss reaction types.</td>
</tr>
<tr>
<td>Falling Threshold (msecs)</td>
<td>Enter a value for falling threshold in milliseconds.</td>
</tr>
<tr>
<td></td>
<td>Rising and Falling thresholds are disabled for timeout, verifyErrors and connectionLoss reaction types.</td>
</tr>
<tr>
<td>X</td>
<td>Specify the number of violations that must occur within a specified range.</td>
</tr>
<tr>
<td></td>
<td>The default value is 5. Valid values ranges between 1 and 16.</td>
</tr>
<tr>
<td>Y</td>
<td>Specify the number of operations that must occur within a specified range.</td>
</tr>
<tr>
<td>Add</td>
<td>Click <strong>Add</strong> after selecting a Reaction type and providing the values.</td>
</tr>
<tr>
<td></td>
<td>You can add one or more Reaction types for an Operation.</td>
</tr>
<tr>
<td>Remove</td>
<td>Click <strong>Remove</strong> after selecting one or more Reaction types to remove one or more reaction type for an Operation.</td>
</tr>
</tbody>
</table>
Step 4

Click Next.

The Specific Settings page appears.

---

Table 16-4  General Settings for Operations (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timeout Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Timeout Value (msecs)</td>
<td>Enter the amount of time in milliseconds for the collector to wait for a response to its operation. The default value is 5000 for all operations.</td>
</tr>
<tr>
<td><strong>Miscellaneous Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Threshold (msecs)</td>
<td>Enter the administrative threshold. This value is represented in milliseconds. For all Operations other than UDP Jitter and ICMP jitter with Reaction type rtt, the value set for rising threshold also gets updated for this threshold field. However, you will not be allowed to update this value. For UDP Jitter and ICMP jitter with jitterAvg as the reaction type, the value set for rising threshold also gets updated for this threshold field. However, you will not be allowed to update this value. You will be allowed to update the threshold for all other operation types and reaction values. The default is 5000 msecs.</td>
</tr>
<tr>
<td>Sample Interval (seconds)</td>
<td>Enter the sample interval in seconds. The valid values are 10 seconds to 3600 seconds (1 hour). The default is 60 seconds for all operations except Video. The default is 900 seconds for Video operations. The source router uses the specified value to collect data. Note If you create a Video collector with polling frequency as 1 minute or 5 minutes, the same statistics will be populated for every 15 minutes in the video_minute_stats table for that collector. This is applicable when you have created a Video operation with default sample interval.</td>
</tr>
<tr>
<td>Verify Data</td>
<td>Either:</td>
</tr>
<tr>
<td></td>
<td>• Check this option if you want to verify the data collected by the source router. Or</td>
</tr>
<tr>
<td></td>
<td>• Uncheck this option if you do not want the data collected by the source router to be verified. The default option is unchecked.</td>
</tr>
</tbody>
</table>
Specifying Reaction Types

You can configure IP SLA Operations to react to certain measured network conditions.

You can specify one or more reaction types for a single Operation. The below table lists the Reactions that are applicable for each operation:

<table>
<thead>
<tr>
<th>Table 16-5 Reaction Types for each Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>Echo</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>PathEcho</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>UDP Jitter</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>DNS</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
## Table 16-5 Reaction Types for each Operation (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Reaction Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>- rtt</td>
</tr>
<tr>
<td></td>
<td>- timeout</td>
</tr>
<tr>
<td></td>
<td>- connectionLoss</td>
</tr>
<tr>
<td></td>
<td>- verifyError</td>
</tr>
<tr>
<td>DHCP</td>
<td>- rtt</td>
</tr>
<tr>
<td></td>
<td>- timeout</td>
</tr>
<tr>
<td></td>
<td>- connectionLoss</td>
</tr>
<tr>
<td></td>
<td>- verifyError</td>
</tr>
<tr>
<td>UDP Echo</td>
<td>- rtt</td>
</tr>
<tr>
<td></td>
<td>- timeout</td>
</tr>
<tr>
<td></td>
<td>- connectionLoss</td>
</tr>
<tr>
<td></td>
<td>- verifyError</td>
</tr>
<tr>
<td>HTTP</td>
<td>- rtt</td>
</tr>
<tr>
<td></td>
<td>- timeout</td>
</tr>
<tr>
<td></td>
<td>- connectionLoss</td>
</tr>
<tr>
<td></td>
<td>- verifyError</td>
</tr>
<tr>
<td>TCPConnect</td>
<td>- rtt</td>
</tr>
<tr>
<td></td>
<td>- timeout</td>
</tr>
<tr>
<td></td>
<td>- connectionLoss</td>
</tr>
<tr>
<td></td>
<td>- verifyError</td>
</tr>
<tr>
<td>DLSW</td>
<td>- rtt</td>
</tr>
<tr>
<td></td>
<td>- timeout</td>
</tr>
<tr>
<td></td>
<td>- connectionLoss</td>
</tr>
<tr>
<td></td>
<td>- verifyError</td>
</tr>
</tbody>
</table>
### Table 16-5 Reaction Types for each Operation (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Reaction Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP</td>
<td>• packetLossDS&lt;br&gt;• packetLossSD&lt;br&gt;• packetMIA&lt;br&gt;• iaJitterDS&lt;br&gt;• frameLossDS&lt;br&gt;• mosLQDS&lt;br&gt;• mosCQDS&lt;br&gt;• rFactorDS&lt;br&gt;• iaJitterSD&lt;br&gt;• rFactorSD&lt;br&gt;• mosCQSD&lt;br&gt;• rtt&lt;br&gt;• timeout&lt;br&gt;• connectionLoss&lt;br&gt;• verifyError</td>
</tr>
<tr>
<td>GatekeeperRegistrationDelay</td>
<td>• rtt&lt;br&gt;• timeout&lt;br&gt;• connectionLoss&lt;br&gt;• verifyError</td>
</tr>
<tr>
<td>Operation</td>
<td>Reaction Type</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>ICMP Jitter</td>
<td>• jitterSDAvg</td>
</tr>
<tr>
<td></td>
<td>• jitterDSAvg</td>
</tr>
<tr>
<td></td>
<td>• jitterAvg</td>
</tr>
<tr>
<td></td>
<td>• packetLateArrival</td>
</tr>
<tr>
<td></td>
<td>• packetOutOfSequence</td>
</tr>
<tr>
<td></td>
<td>• maxOfPositiveSD</td>
</tr>
<tr>
<td></td>
<td>• maxOfNegativeSD</td>
</tr>
<tr>
<td></td>
<td>• maxOfPositiveDS</td>
</tr>
<tr>
<td></td>
<td>• maxOfNegativeDS</td>
</tr>
<tr>
<td></td>
<td>• successivePacketLoss</td>
</tr>
<tr>
<td></td>
<td>• maxOfLatencyDS</td>
</tr>
<tr>
<td></td>
<td>• maxOfLatencySD</td>
</tr>
<tr>
<td></td>
<td>• latencyDSAvg</td>
</tr>
<tr>
<td></td>
<td>• latencySDAvg</td>
</tr>
<tr>
<td></td>
<td>• packetLoss</td>
</tr>
<tr>
<td></td>
<td>• rtt</td>
</tr>
<tr>
<td></td>
<td>• timeout</td>
</tr>
<tr>
<td></td>
<td>• connectionLoss</td>
</tr>
<tr>
<td></td>
<td>• verifyError</td>
</tr>
<tr>
<td>CallSetupPostDialDelay</td>
<td>• rtt</td>
</tr>
<tr>
<td></td>
<td>• timeout</td>
</tr>
<tr>
<td></td>
<td>• connectionLoss</td>
</tr>
<tr>
<td></td>
<td>• verifyError</td>
</tr>
<tr>
<td>EthernetPing</td>
<td>• rtt</td>
</tr>
<tr>
<td></td>
<td>• timeout</td>
</tr>
<tr>
<td></td>
<td>• connectionLoss</td>
</tr>
<tr>
<td>EthernetPingAutoIPSLA</td>
<td>• rtt</td>
</tr>
<tr>
<td></td>
<td>• timeout</td>
</tr>
<tr>
<td></td>
<td>• connectionLoss</td>
</tr>
</tbody>
</table>
Table 16-5  Reaction Types for each Operation (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Reaction Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>EthernetJitter</td>
<td>• rtt</td>
</tr>
<tr>
<td></td>
<td>• timeout</td>
</tr>
<tr>
<td></td>
<td>• connectionLoss</td>
</tr>
<tr>
<td></td>
<td>• jitterSDAvg</td>
</tr>
<tr>
<td></td>
<td>• jitterDSAvg</td>
</tr>
<tr>
<td></td>
<td>• jitterAvg</td>
</tr>
<tr>
<td></td>
<td>• maxOfPositiveSD</td>
</tr>
<tr>
<td></td>
<td>• maxOfNegativeSD</td>
</tr>
<tr>
<td></td>
<td>• maxOfPositiveDS</td>
</tr>
<tr>
<td></td>
<td>• maxOfNegativeDS</td>
</tr>
<tr>
<td></td>
<td>• packetLateArrival</td>
</tr>
<tr>
<td></td>
<td>• packetLossDS</td>
</tr>
<tr>
<td></td>
<td>• packetLossSD</td>
</tr>
<tr>
<td></td>
<td>• packetOutOfSequence</td>
</tr>
<tr>
<td></td>
<td>• packetMIA</td>
</tr>
</tbody>
</table>
Table 16-5  Reaction Types for each Operation  (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Reaction Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>EthernetJitterAutoIPSLA</td>
<td>• rtt</td>
</tr>
<tr>
<td></td>
<td>• timeout</td>
</tr>
<tr>
<td></td>
<td>• connectionLoss</td>
</tr>
<tr>
<td></td>
<td>• jitterSDAvg</td>
</tr>
<tr>
<td></td>
<td>• jitterDSAvg</td>
</tr>
<tr>
<td></td>
<td>• jitterAvg</td>
</tr>
<tr>
<td></td>
<td>• maxOfPositiveSD</td>
</tr>
<tr>
<td></td>
<td>• maxOfNegativeSD</td>
</tr>
<tr>
<td></td>
<td>• maxOfPositiveDS</td>
</tr>
<tr>
<td></td>
<td>• maxOfNegativeDS</td>
</tr>
<tr>
<td></td>
<td>• packetLateArrival</td>
</tr>
<tr>
<td></td>
<td>• packetLossDS</td>
</tr>
<tr>
<td></td>
<td>• packetLossSD</td>
</tr>
<tr>
<td></td>
<td>• packetOutOfSequence</td>
</tr>
<tr>
<td></td>
<td>• packetMIA</td>
</tr>
<tr>
<td>Video</td>
<td>• connectionLoss</td>
</tr>
<tr>
<td></td>
<td>• iaJitterSD</td>
</tr>
<tr>
<td></td>
<td>• jitterSDAvg</td>
</tr>
<tr>
<td></td>
<td>• latencySDAvg</td>
</tr>
<tr>
<td></td>
<td>• packetLossSD</td>
</tr>
<tr>
<td></td>
<td>• timeout</td>
</tr>
</tbody>
</table>

For more information on the descriptions for each Reaction, see Descriptions for the Reaction Types.

**Descriptions for the Reaction Types**

Table 16-6  Reaction Type Descriptions

<table>
<thead>
<tr>
<th>Reaction Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connectionLoss</td>
<td>connection lost while moving from source to target and back.</td>
</tr>
<tr>
<td>frameLossDS</td>
<td>Average of the codec frame loss events at the source</td>
</tr>
<tr>
<td>iaJitterDS</td>
<td>Inter Arrival Jitter at the destination.</td>
</tr>
<tr>
<td>iaJitterSD</td>
<td>Inter Arrival Jitter at the source.</td>
</tr>
<tr>
<td>icpif</td>
<td>Calculated Planning Impairment Factor—ICPIF numbers represent predefined combinations of loss and delay.</td>
</tr>
<tr>
<td>jitterAvg</td>
<td>Average Inter-packet delay between any two consecutive data packets sent from the source to target router and back.</td>
</tr>
<tr>
<td>jitterSDAvg</td>
<td>Average Source to Destination jitter.</td>
</tr>
</tbody>
</table>
Understanding the List of IPSLA Operations

Table 16-6 Reaction Type Descriptions

<table>
<thead>
<tr>
<th>Reaction Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jitterDSAvg</td>
<td>Average Destination to Source jitter.</td>
</tr>
<tr>
<td>latencyDSAvg</td>
<td>Average Destination to Source latency.</td>
</tr>
<tr>
<td>latencySDAvg</td>
<td>Average Source to Destination latency.</td>
</tr>
<tr>
<td>maxOfLatencyDS</td>
<td>Maximum Destination to Source latency.</td>
</tr>
<tr>
<td>maxOfLatencySD</td>
<td>Maximum Source to Destination latency.</td>
</tr>
<tr>
<td>maxOfNegativeDS</td>
<td>Maximum Destination to Source negative jitter.</td>
</tr>
<tr>
<td>maxOfNegativeSD</td>
<td>Maximum Source to Destination negative jitter.</td>
</tr>
<tr>
<td>maxOfPositiveDS</td>
<td>Maximum Destination to Source positive jitter.</td>
</tr>
<tr>
<td>maxOfPositiveSD</td>
<td>Maximum Source to Destination positive jitter.</td>
</tr>
<tr>
<td>mos</td>
<td>Mos refers to Mean Opinion Score. It is a numerical measure of the voice quality in the network.</td>
</tr>
<tr>
<td>mosCQDS</td>
<td>Estimated Destination to Source mean opinion score for conversational quality.</td>
</tr>
<tr>
<td>mosCQSD</td>
<td>Estimated Source to Destination mean opinion score for conversational quality.</td>
</tr>
<tr>
<td>mosLQDS</td>
<td>Estimated Destination to Source mean opinion score for listening quality.</td>
</tr>
<tr>
<td>packetLateArrival</td>
<td>Average of the late packets at the source.</td>
</tr>
<tr>
<td>packetLoss</td>
<td>Measures the total number of packets lost while moving from source to target and back.</td>
</tr>
<tr>
<td>packetLossDS</td>
<td>Number of packets lost when sent from destination to source.</td>
</tr>
<tr>
<td>packetLossSD</td>
<td>Number of packets lost when sent from source to destination.</td>
</tr>
<tr>
<td>packetMIA</td>
<td>Number of packets lost whose direction is unknown.</td>
</tr>
<tr>
<td>packetOutOfSequence</td>
<td>Number of packets arrived out of sequence.</td>
</tr>
<tr>
<td>rFactorDS</td>
<td>Estimated R-Factor value at the destination.</td>
</tr>
<tr>
<td>rFactorSD</td>
<td>Estimated R-Factor value at the source.</td>
</tr>
<tr>
<td>rtt</td>
<td>Measures the round-trip time taken to perform an operation.</td>
</tr>
<tr>
<td>successivePacketLoss</td>
<td>Number of packets that are dropped successively.</td>
</tr>
<tr>
<td>timeout</td>
<td>Number of RTT operations timed out.</td>
</tr>
<tr>
<td>verifyError</td>
<td>RTT completions that do not match with the expected data.</td>
</tr>
</tbody>
</table>
Specific Settings for a User-Defined Operation

The Specific Settings page allows you to define the specific settings for an operation. The specific setting differs for each operation type.

To know the specific settings for a particular operation, click the required link. The list of links is given below:

- Measuring Network Performance for DHCP
- Measuring Network Performance for DNS
- Measuring Network Performance for FTP
- Measuring End-to-End Performance for Echo
- Measuring Hop-by-Hop Performance for Path Echo
- Measuring Network Performance for HTTP
- Measuring Network Performance for DLSw
- Measuring Network Performance for UDP Echo
- Measuring Network Performance for UDP Jitter
- Measuring Network Performance for ICMP Jitter
- Measuring Network Performance for Gatekeeper Registration Delay
- Measuring Network Performance for Call Setup Post Dial Delay
- Measuring Network Performance for RTP
- Measuring Network Performance for TCP Connect
- Measuring Network Performance for Ethernet Ping
- Measuring Network Performance for Ethernet Jitter
- Measuring Network Performance for Ethernet Ping Auto IP SLA
- Measuring Network Performance for Ethernet Jitter Auto IP SLA
- Measuring Network Performance for Video
To assign specific settings for a user-defined operation:

**Step 1** Specify the following in the Packet Settings section:
- **IP QoS Type**—Select IP Precedence or DSCP.
- **IP QoS Settings**—Select a value from the drop-down list. The values change based on your IP QoS Type selection.
  - If you have selected IP QoS Type as IP Precedence, select the IP QoS Settings value from the drop-down list. The values range from 0 to 7. The value you select sets the priority for the request packet. The default setting is 0 (no priority). This option sets the ToS bits in the IP packet.
  - If you have selected IP QoS Type as DSCP, select the desired IP QoS Settings value from the drop-down list. The values range from 0 to 63. The value you select defines the packet priority and is based on the DSCP RFC standards.
- **Request Payload (bytes)**—Enter the number of bytes to specify the payload size of the request packet. The default setting is 64 bytes.

**Step 2** Select the Loose Source Routing (LSR) check box to enter LSR Hop Addresses.

**Step 3** Click **Next**.
The Summary page appears with the details of the user-defined operation.

---

**Viewing the Summary of a User-Defined Operation**

The Summary page allows you to view the details of the user-defined operation you have created.

To view the summary of a user-defined operation:

**Step 1** Click **Finish**.
A message appears that the operation is created successfully.

**Step 2** Click **OK**.
The List of Operations page appears.
Or
Click **Back**.
This allows you to modify the general and specific settings of the operation defined in the General Settings and Specific Settings pages.
Editing User-Defined Operations

You can edit all parameters of a user-defined operation except the name and type of operation. You cannot edit the system-defined operations.

**Note**

An error message appears if you try to delete the operation of a running collector.

To edit a user-defined operation:

1. Select **Monitor > Performance Settings > IPSLA > Operations** from the menu. The List of Operations page appears.
2. Select an operation that you want to edit.
3. Click **Edit**. The General Settings page appears.
4. Modify the required fields in the General Settings page.

**Note**

You can modify only the fields in the Threshold Settings, Timeout Settings, and Miscellaneous Settings sections. You cannot modify the Details section.

5. Click **Next**. The Specific Settings page appears.
6. Modify the required fields in the Specific Settings page.

For more information, see **General Settings for a User-Defined Operation**.

7. Click **Next**. The Summary page appears with the details of the operation that you have updated.
8. Click **Finish** to update the changes made.
Deleting User-Defined Operations

You can delete user-defined operations that you no longer need. However, you cannot delete an operation if that operation is currently used by a collector. In that case, you must delete the collector first and then delete the operation. You can delete more than one operation at a time.

Note

You cannot delete the default IPSLA operations.

To delete IPSLA user-defined operations:

Step 1 Select Monitor > Performance Settings > IPSLA > Operations from the menu.
The List of Operations page appears.
Step 2 Select the operations that you want to delete.
Step 3 Click Delete.
The Delete Confirmation dialog box appears.
An error message appears if you try to delete operations that are currently used by a collector.
Step 4 Click OK.
The selected operations are deleted from the IPSLA Monitoring database.

Viewing Operation Properties

The Operation Properties window allows you to view the properties of a defined operation.

To view operation properties:

Step 1 Select Monitor > Performance Settings > IPSLA > Operations from the menu.
The List of Operations page appears.
Step 2 Select an operation for which you want to view the properties.
Step 3  Click View.

The Operation Properties window appears with the information on general settings, threshold settings, timeout settings and specific settings for the selected operation.

For more information on the general settings for each operation, see General Settings for a User-Defined Operation

For more information on the specific settings to define operations see:

- Defining an Echo Operation
- Defining a Path Echo Operation
- Defining a UDP Echo Operation
- Defining an ICMP Jitter Operation
- Defining a UDP Jitter Operation
- Defining an RTP Operation
- Defining a Call Setup Post Dial Delay Operation
- Defining a Gatekeeper Registration Delay Operation
- Defining a DNS Operation
- Defining a DHCP Operation
- Defining an HTTP Operation
- Defining an FTP Operation
- Defining a DLSw Operation
- Defining a TCP Connect Operation
- Defining an Ethernet Ping Operation
- Defining an Ethernet Jitter Operation
- Defining an Ethernet Ping Auto IP SLA Operation
- Defining an Ethernet Jitter Auto IP SLA Operation
Using IPSLA Operations to Measure Network Performance

IPSLA Monitoring allows you to measure the network performance using the following IP SLA operations:

- Measuring Network Performance for IP
- Measuring Network Performance for UDP Echo
- Measuring Network Performance for ICMP Jitter
- Measuring Network Performance for UDP Jitter
- Measuring Network Performance for RTP
- Measuring Network Performance for Call Setup Post Dial Delay
- Measuring Network Performance for Gatekeeper Registration Delay
- Measuring Network Performance for DNS
- Measuring Network Performance for DHCP
- Measuring Network Performance for HTTP
- Measuring Network Performance for FTP
- Measuring Network Performance for DLSw
- Measuring Network Performance for TCP Connect
- Measuring Network Performance for Ethernet Ping
- Measuring Network Performance for Ethernet Jitter
- Measuring Network Performance for Ethernet Ping Auto IP SLA
- Measuring Network Performance for Ethernet Jitter Auto IP SLA
- Measuring Network Performance for Video

Measuring Network Performance for IP

This section explains:

- Measuring End-to-End Performance for Echo
- Defining an Echo Operation
- Measuring Hop-by-Hop Performance for Path Echo
- Defining a Path Echo Operation

In an IP network there are two types of measurements that you can take:

- Echo or Ping Echo—Measures the total round-trip latency from the source to the target device. The IP SLA feature in the source router issues an Internet Control Message Protocol (ICMP) ping to the target device and extracts the latency data from the reply.
  For more information, see Measuring End-to-End Performance for Echo.

- Path Echo or Ping Path Echo—Measures the total round-trip latency as well as the incremental latency for each hop in all paths between the source router and the target device. Path Echo is available only for the IP protocol.
  The IP SLA feature first issues a traceroute command to determine the path through the network from the specified source to the specified target device.
The data returned from the **traceroute** command contains the host name or IP address of each of the routers in the path. IP SLA then issues ICMP pings to each of the routers listed in the traceroute data.

The ICMP ping returns statistics regarding the latency, availability, and errors between the specified source and each of the routers.

For more information, see Measuring Hop-by-Hop Performance for Path Echo.

### Measuring End-to-End Performance for Echo

Echo or Ping Echo operation measures end-to-end performance between a source and any IP-enabled device.

Latency is computed by measuring the time taken between sending an ICMP echo request message to the destination and receiving an ICMP echo reply. The Echo operation also measures availability and errors for IP services.

With an Echo operation, you can determine performance on a specific path by using Loose Source Routing.

Additionally, IPSLA Monitoring provides an option for measuring quality of service (QoS) between endpoints by setting the DSCP and the type of service (ToS) bits on the IP packet.

To measure end-to-end performance for Echo:

---

**Step 1** Define a device as the source device from which to measure performance.
For details on defining a source device, see Specifying Source Devices.

**Step 2** Define a Ping Echo server as a target device.
For details on defining a target device, see Specifying Target Devices.

**Step 3** Define a Ping Echo operation. Use DefaultIPEcho operation or customize a Echo operation.
For details on defining a Ping Echo operation, see Defining an Echo Operation.

**Step 4** Define a collector to measure performance between the source and target.
For details on defining a collector, see Defining Collectors.

**Step 5** Generate the report to view the Echo statistics.
For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.
Defining an Echo Operation

IPSLA Monitoring provides three default Echo operations namely DefaultIpEcho, DefaultIpEchoPri3, DefaultIpEchoPri7 for measuring performance between a source and target. In addition, IPSLA Monitoring provides the option to create, modify, or delete your own Echo operations from the List of Operations page.

To define an Echo operation:

1. **Step 1**
   Select **Monitor > Performance Settings > IPSLA > Operations** from the menu.
   The List of Operations page appears.

2. **Step 2**
   Click **Create**.
   The General Settings page appears.

3. **Step 3**
   Select Echo operation from the Type drop-down list.
   To complete other general setting parameters, see **General Settings for a User-Defined Operation**.

4. **Step 4**
   Click **Next**.
   The Specific Settings page appears.

5. **Step 5**
   Specify the following in the Packet Settings section:
   - **IP QoS Type**—Select the IP QoS Type as IP Precedence or DSCP.
   - **IP QoS Settings**—Select a value from the drop-down list. The values change based on your IP QoS Type selection.
     - If you have selected IP QoS Type as IP Precedence, select the IP QoS Settings value from the drop-down list. The values range from 0 to 7.
     - If you have selected IP QoS Type as DSCP, select the desired IP QoS Settings value from the drop-down list. The values range from 0 to 63.
     The value you select sets the priority for the request packet. The default setting is 0 (no priority). This option sets the QoS bits in the IP packet.
   - **Request Payload (bytes)**—Enter the number of bytes in the Request Payload field to use for the size of the payload of the ICMP echo request packet. The default setting is 64 bytes.

6. **Step 6**
   Enable the Loose Source Routing option to measure performance for a specific path and add the hops for the operation to use. You can enter a maximum of eight hops.

7. **Step 7**
   Click **Finish**.
   The newly defined Echo operation is successfully created.
   An error message appears if the Create operation fails.
Measuring Hop-by-Hop Performance for Path Echo

IPSLA Monitoring’s Path Echo or Ping Path Echo operation determines hop-by-hop performance between a source and target device on the network by discovering the path. Path Echo uses traceroute and then measures performance between the source and each intermittent hop in the path.

If there are multiple equal cost routes between the source and the target, the Path Echo operation can identify the correct path by using Loose Source Routing (if the option is enabled on the intermediate hop devices).

This feature enables IPSLA to discover paths more accurately compared to a regular traceroute. The Path Echo operation also measures availability and errors for IP services.

To measure hop-by-hop performance for Path Echo:

### Step 1
Define a device as the source device from which to measure performance.
For details on defining a source device, see Specifying Source Devices.

### Step 2
Define a device as the target of Path Echo requests from the source device.
For details on defining a target device, see Specifying Target Devices.

### Step 3
Define a Path Echo operation. Use the DefaultIPPathEcho operation or customize a Path Echo operation.
For details on defining a Ping Path Echo operation, see Defining a Path Echo Operation.

### Step 4
Define a collector to measure performance between the source and target.
For details on defining a collector, see Defining Collectors.

### Step 5
Generate the report to view the Path Echo statistics.
For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.

Defining a Path Echo Operation

IPSLA Monitoring provides a default Path Echo operation for measuring performance between a source and target. In addition, IPSLA Monitoring provides the option to create, modify, or delete your own Path Echo operations from the List of Operations page.

To define a Path Echo operation:

### Step 1
Select Monitor > Performance Settings > IPSLA > Operations from the menu.
The List of Operations page appears.

### Step 2
Click Create.
The General Settings page appears.

### Step 3
Select PathEcho operation from the Type drop-down list.
To complete other general setting parameters, see General Settings for a User-Defined Operation.

### Step 4
Click Next.
The Specific Settings page appears.
Step 5 Specify the following in the Packet Settings section:

- IP QoS Type—Select the IP QoS Type as IP Precedence or DSCP.
- IP QoS Settings—Select a value from the drop-down list. The values change based on your IP QoS Type selection.
  - If you have selected IP QoS Type as IP Precedence, select the IP QoS Settings value from the drop-down list. The values range from 0 to 7.
    The value you select sets the priority for the request packet. The default setting is 0 (no priority). This option sets the QoS bits in the IP packet.
  - If you have selected IP QoS Type as DSCP, select the desired IP QoS Settings value from the drop-down list. The values range from 0 to 63.
    The value you select defines the packet priority and is based on the DSCP RFC standards.
- Request Payload (bytes)—Enter the number of bytes in the Request Payload field to use for the size of the payload of the ICMP echo request packet. The default setting is 64 bytes.

Step 6 Specify the following in the Path Settings section:

- Maximum Path—Enter a value to specify the maximum number of paths to discover. The valid range is 1 to 128 paths. The default setting is 5.
  To ensure that you do not miss collecting statistics for relevant paths, set this value to a number slightly higher than the expected number of paths.
- Maximum Hops—Enter a value to specify the maximum number of hops to discover. The valid range is 1 to 25 hops. The default setting is 10 hops.
  To ensure that you do not miss collecting statistics for relevant hops, set this value to a number slightly higher than the expected number of hops.

Step 7 Click Next.
The Summary page appears with the details of the operation created.

Step 8 Click Finish.
The newly defined Path Echo operation is successfully created.
An error message appears if the Create operation fails.

Measuring Network Performance for UDP Echo

IPSLA’s UDP Echo operation measures round-trip latency between a source and any IP-enabled device running UDP services. Latency is computed by measuring the time taken to send a datagram and receive a response from the target device. The UDP operation also measures availability and errors for UDP services.

To measure end-to-end performance for UDP Echo:

Step 1 Define a device as the source device from which to measure performance.
For details on defining a source device, see Specifying Source Devices.

Step 2 Define a device as the target of connection requests from the source device.
For details on defining a target, see Specifying Target Devices.
**Step 3**  Define a UDP operation. Use the DefaultUDPEcho operation or customize a UDP Echo operation. For details on defining an UDP Echo operation, see Defining a UDP Echo Operation.

**Step 4**  Define a collector to measure performance between the source router and target you defined. For details on defining a collector, see Defining Collectors.

**Step 5**  Generate the report to view the UDP Echo statistics. For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.
Defining a UDP Echo Operation

IPSLA Monitoring provides a default UDP Echo operation for measuring performance between a source and target. In addition, IPSLA Monitoring provides the option to create, modify, or delete your own UDP Echo operations from the List of Operations page.

To define a UDP Echo operation:

**Step 1**  
Select **Monitor > Performance Settings > IPSLA > Operations** from the menu.  
The List of Operations page appears.

**Step 2**  
Click **Create**.  
The General Settings page appears.

**Step 3**  
Select UDPEcho operation from the Type drop-down list.  
To complete other general setting parameters, see **General Settings for a User-Defined Operation**.

**Step 4**  
Click **Next**.  
The Specific Settings page appears.

**Step 5**  
Specify the following in the Specific Settings section:

- IP QoS Type—Select the IP QoS Type as IP Precedence or DSCP.

- IP QoS Settings—Select a value from the drop-down list. The values change based on your IP QoS Type selection.
  - If you have selected IP QoS Type as IP Precedence, select the IP QoS Settings value from the drop-down list. The values range from 0 to 7.
    - The value you select sets the priority for the request packet. The default setting is 0 (no priority). This option sets the ToS bits in the IP packet.
  - If you have selected IP QoS Type as DSCP, select the desired IP QoS Settings value from the drop-down list. The values range from 0 to 63.
    - The value you select defines the packet priority and is based on the DSCP RFC standards.

- Request Payload (bytes)—Enter the number of bytes to use for the size of the payload of the request packet. The default setting is 64 bytes.

**Step 6**  
Specify the UDP Echo port number in the Port Settings section.  
The target device uses this port number when sending response packets. Valid values are 7, and 1025 to 65535. The default setting is 7.

- If the target device is a Cisco router running version 12.1 or later of the Cisco IOS software, you can specify any port that is not well known.
  - That is, you can specify any port number greater than 1024 to communicate with the IP SLA Responder, as long as someone is listening on that target port. The only allowed well known port is UDP port 7.

- If the target is not running version 12.1 or later of the Cisco IOS software, whether a Cisco or a non-Cisco IP host, you must specify UDP port 7 as the target port.
Step 7  Click Next.
The Summary page appears with the details of the operation created.

Step 8  Click Finish.
The newly defined UDP operation is successfully created.
An error message appears if the Create operation fails.

Measuring Network Performance for ICMP Jitter

The ICMP Jitter generates a stream of ICMP packets between a Cisco IOS device (source) and any other
IP device (destination) to gather network performance-related statistics namely latency, round-trip time,
jitter (interpacket delay variance), and packet loss.
The destination device can be any network device that supports ICMP such as a server or workstation.
ICMP does not require IP SLA responders to be configured on the destination devices.
ICMP provides:

- End-to-end performance measurements between a Cisco device (source) and any IP device
  (destination) using ICMP.
- Proactive threshold violation monitoring through Simple Network Management Protocol (SNMP)
  trap notifications and syslog messages.

To measure end-to-end performance for ICMP Jitter:

Step 1  Define a device as the source device from which to measure performance.
For details on defining a source device, see Specifying Source Devices.

Step 2  Define a device as the target of discovery requests from the source device.
For details on defining a target, see Specifying Target Devices.

Step 3  Define a ICMP Jitter operation. Use the DefaultICMPJitter operation or customize a ICMP Jitter
operation.
For details on defining an ICMP operation, see Defining an ICMP Jitter Operation.

Step 4  Define a collector to measure performance between the source router and target you defined.
For details on defining a collector, see Defining Collectors.

Step 5  Generate the report to view the ICMP Jitter statistics.
For more information on generating the report, see Reports Management with Cisco Prime LAN
Management Solution 4.1.
Defining an ICMP Jitter Operation

IPSLA Monitoring provides a default ICMP Jitter operation for measuring performance between a source and target. In addition, IPSLA Monitoring provides the option to create, modify, or delete your own ICMP Jitter operations from the List of Operations page.

To define an ICMP Jitter operation:

**Step 1** Select Monitor > Performance Settings > IPSLA > Operations from the menu.

The List of Operations page appears.

**Step 2** Click Create.

The General Settings page appears.

**Step 3** Select ICMPJitter operation from the Type drop-down list.

To complete other general setting parameters, see General Settings for a User-Defined Operation.

**Step 4** Click Next.

The Specific Settings page appears.

**Step 5** Specify the following in the Packet Settings section:

- **IP QoS Type**—Select the IP QoS Type as IP Precedence or DSCP.
- **IP QoS Settings**—Select a value from the drop-down list. The values change based on your IP QoS Type selection.
  - If you have selected IP QoS Type as IP Precedence, select the IP QoS Settings value from the drop-down list. The values range from 0 to 7.
    - The value you select sets the priority for the request packet. The default setting is 0 (no priority). This option sets the ToS bits in the IP packet.
  - If you have selected IP QoS Type as DSCP, select the desired IP QoS Settings value from the drop-down list. The values range from 0 to 63.
    - The value you select defines the packet priority and is based on the DSCP RFC standards.
- **Packet Interval (msecs)**—Enter the number of milliseconds to use for the interpacket delay between packets sent from the source router to the target router. The default setting is 20 milliseconds.
- **Number of Packets**—Enter the number of packets to send to the target to measure latency. The default setting is 10 packets.

**Step 6** Click Next.

The Summary page displays the operation details that you have created.

**Step 7** Click Finish.

The newly defined ICMP Jitter operation is successfully created.

An error message appears if the Create operation fails.
Measuring Network Performance for UDP Jitter

The UDP Jitter operation for Voice over IP measures round-trip latency, packet loss, and jitter in IP networks by generating synthetic UDP traffic. The UDP Jitter operation sends a defined number of packets of a defined size from the source to a target with a defined interpacket delay.

Both the source and the target must be running version 12.1 or later of the Cisco IOS software, and the SA Agent responder must be enabled on the target.

To enable the SA Agent Responder on the target, use the `rtr ressponder` IOS configuration command. The packets sent out to measure jitter contain packet sequence information, as well as sending and receiving timestamps from the source and the Responder.

**Note**
The UDP Jitter operation sends only UDP data traffic, and does not send any voice packets.

The UDP Jitter operation measures the following network performance statistics:

- Round-trip network latency
- Per-direction packet loss
- Per-direction interpacket delay variance (jitter)
- Network availability and errors

The MOS and ICPIF are values that are obtained when collectors are configured with UDP Jitter operations that have codec types other than None. The UDP Jitter with VoIP operation is present only in versions 12.3(14)T and above. The definitions of MOS and ICPIF are given below:

- **MOS**
  Mean Opinion Score provides a numerical measure of the voice quality in the network. It is expressed as a single number in the range 1 to 5, where 1 is lowest perceived quality, and 5 is the highest perceived quality.

- **ICPIF**
  Calculated Planning Impairment Factor loss/delay busyout threshold. The ICPIF numbers represent predefined combinations of loss and delay. Packet loss and delay determine the threshold for initiating the busyout state. Table 16-7 shows the resulting MOS values that will be generated for corresponding ICPIF values.

<table>
<thead>
<tr>
<th>ICPIF Range</th>
<th>MOS</th>
<th>Quality Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 3</td>
<td>5</td>
<td>Best</td>
</tr>
<tr>
<td>4 - 13</td>
<td>4</td>
<td>High</td>
</tr>
<tr>
<td>14 - 23</td>
<td>3</td>
<td>Medium</td>
</tr>
<tr>
<td>24 - 33</td>
<td>2</td>
<td>Low</td>
</tr>
<tr>
<td>34 - 43</td>
<td>1</td>
<td>Poor</td>
</tr>
</tbody>
</table>
To measure end-to-end performance for UDP Jitter:

**Step 1** Define a device as the source device from which to measure performance. For details on defining a source device, see *Specifying Source Devices*.

**Step 2** Define a device as the target of discovery requests from the source device. For details on defining a target, see *Specifying Target Devices*.

**Step 3** Define an UDP Jitter operation. Use one of the default UDP Jitter operations or customize a UDP Jitter operation. For details on defining an UDP Jitter operation, see *Defining a UDP Jitter Operation*.

**Step 4** Define a collector to measure performance between the source router and target you defined. For details on defining a collector, see *Defining Collectors*.

**Step 5** Generate the report to view the UDP Jitter statistics. For more information on generating the report, see *Reports Management with Cisco Prime LAN Management Solution 4.1*.

**Defining a UDP Jitter Operation**

IPSLA Monitoring provides several default UDP Jitter operations for measuring performance between a source and target. In addition, IPSLA Monitoring provides the option to create, modify, or delete your own UDP Jitter operations from the List of Operations page.

To define an UDP operation:

**Step 1** Select *Monitor > Performance Settings > IPSLA > Operations* from the menu. The List of Operations page appears.

**Step 2** Click *Create*. The General Settings page appears.

**Step 3** Select an UDP Jitter operation from the Type drop-down list. To complete other general setting parameters, see *General Settings for a User-Defined Operation*.

**Step 4** Click *Next*. The Specific Settings page appears.
Step 5 Specify the following in the Codec/ICPIF Settings section:

- **Target Port**—Enter the UDP Jitter port number. The target device uses this port number when sending a response packet.
  
  Valid values range from 1 to 65536. The default setting is 16400 for Voice, 2000 for VPN, and 50505 for Video.
  
  The Target Port should be an even number if you have selected the Codec Types g711alaw, g711ulaw, or g729a.

- **Codec Type**—Select the codec type keywords from the drop-down list.
  
  It enables the generation of estimated voice quality scores in the form of Calculated Planning Impairment Factor (ICPIF) and Mean Opinion Score (MOS) values. The codec type should match the encoding algorithm that you are using for VoIP transmissions.
  
  - Codec type g711alaw—The G.711 A-Law codec (64 kbps transmission).
  
  - Codec type g711ulaw—The G.711 muHm-Law codec (64 kbps transmission).
  
  - Codec type g729a—The G.729A codec (8 kbps transmission).
  
  The default codec type is None.

- **Advantage Factor**—Select the advantage factor from the drop-down list. It specifies the expectation factor to be used for ICPIF calculations.
  
  This value is subtracted from the measured impairments to yield the final ICPIF value (and corresponding MOS value). The valid values range from 0 to 20. The default value is 0.
  
  Table 16-8 depicts the Advantage Factor Recommended Maximum values:

<table>
<thead>
<tr>
<th>Communication Service</th>
<th>Advantage/Expectation Factor: Maximum value of A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conventional wire-line (land-line)</td>
<td>0</td>
</tr>
<tr>
<td>Mobility (cellular connections) within a building</td>
<td>5</td>
</tr>
<tr>
<td>Mobility within a Geographical area or moving in a vehicle</td>
<td>10</td>
</tr>
<tr>
<td>Access to hard-to-reach location; (for example, via multi-hop satellite connections)</td>
<td>20</td>
</tr>
</tbody>
</table>
Step 6  Specify the following in the Precision Settings section:
   - Precision Level - Select the precision level as Milliseconds or Microseconds from the listbox.
     - Select Milliseconds to collect the jitter statistics at a precision level of milliseconds. This is the default option.
     - Select Microseconds to collect the jitter statistics at a precision level of microseconds.

Step 7  Specify the following in the Packet Settings section:
   - IP QoS Type—Select the IP QoS Type as IP Precedence or DSCP.
   - IP QoS Settings—Select a value from the drop-down list. The values change based on your IP QoS Type selection.
     - If you have selected IP QoS Type as IP Precedence, select the IP QoS Settings value from the drop-down list. The values range from 0 to 7.
       The value you select sets the priority for the request packet. The default setting is 0 (no priority). This option sets the ToS bits in the IP packet.
     - If you have selected IP QoS Type as DSCP, select the desired IP QoS Settings value from the drop-down list. The values range from 0 to 63.
       The value you select defines the packet priority and is based on the DSCP RFC standards.
   - Request Payload (bytes)—Enter the number of bytes to use for the size of the payload of the UDP request packet. The default setting is one of the following values:
     - 60 bytes for Default60ByteVoice operations
     - 160 bytes for Default160ByteVoice operations
     - 1024 bytes for DefaultVPN and DefaultVideo operations
   - Packet Interval (msecs)—Enter the number of milliseconds to use for the interpacket delay between packets sent from the source router to the target router. The default setting is 20 milliseconds.
   - Number of Packets—Enter the number of packets to send to the target to measure latency. The default setting is 10 packets.

Step 8  Click Next.
The Summary page displays the operation details that you have created.

Step 9  Click Finish.
The newly defined UDP Jitter operation is successfully created.
An error message appears if the Create operation fails.
Measuring Network Performance for RTP

The IP SLA Real-Time Transport Protocol (RTP)-based Voice over IP (VoIP) Operation feature provides the capability to set up and schedule a test call and use Voice source router digital signal processors (DSPs) to gather network performance-related statistics for the call.

Available statistical measurements for VoIP networks include jitter, frame loss, Mean Opinion Score for Conversational Quality (MOS-CQ), and Mean Opinion Score for Listening Quality (MOS-LQ).

The IP SLAs RTP-Based VoIP Operation provides:
- End-to-end performance measurements using DSPs for determining voice quality in VoIP networks.
- Proactive threshold violation monitoring through SNMP trap notifications.

To measure end-to-end performance for RTP:

**Step 1**
Define a device as the source device from which to measure performance.
For details on defining a source device, see Specifying Source Devices.

**Step 2**
Define a device as the target of discovery requests from the source device.
For details on defining a target, see Specifying Target Devices.

**Step 3**
Customize an RTP operation.
For details on defining a RTP operation, see Defining an RTP Operation.

**Step 4**
Define a collector to measure performance between the source router and target you defined.
For details on defining a collector, see Defining Collectors.

**Step 5**
Generate the report to view the RTP statistics.
For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.

Defining an RTP Operation

IPSLA Monitoring provides a default RTP operation to set up and schedule a test call and use Voice source router digital signal processors (DSPs) to gather network performance-related statistics for the call.

In addition, IPSLA Monitoring provides the option to create, modify, or delete your own RTP operations from the List of Operations page.

To define a RTP operation:

**Step 1**
Select Monitor > Performance Settings > IPSLA > Operations from the menu.
The List of Operations page appears.

**Step 2**
Click Create.
The General Settings page appears.

**Step 3**
Select RTP operation from the Type drop-down list.
To complete other general setting parameters, see General Settings for a User-Defined Operation.
Step 4  Click Next.

The Specific Settings page appears.

Step 5  Specify the following in the Settings section:

- Source Voice Port—Specify the source voice port. The source voice port is represented as slot/subunit/port:ds0-group-number, where:
  - slot refers to source slot number.
  - /subunit refers to source submit. A slash must precede this value.
  - /port refers to source port number. A slash must precede this value.
  - :ds0-group-number refers to DS0 group number. A colon must precede this value.

- Codec Type—Enables the generation of estimated voice quality scores in the form of Calculated Planning Impairment Factor (ICPIF) and Mean Opinion Score (MOS) values. The codec type should match the encoding algorithm you are using for VoIP transmissions.
  - Codec type g711alaw—The G.711 A-Law codec (64 kbps transmission).
  - Codec type g711ulaw—The G.711 muLaw-Law codec (64 kbps transmission).
  - Codec type g729a—The G.729A codec (8 kbps transmission).

  The default codec type is g729a codec.

- Call Duration—Specifies the duration of the test call. The valid values range from 20 to 180 seconds. The default value is 20 seconds.

  Collectors move to Config Failed state if the values you specify do not fall between 20 and 180.

- Advantage Factor— Specifies the expectation factor to be used for ICPIF calculations. This value is subtracted from the measured impairments to yield the final ICPIF value (and corresponding MOS value). The valid values range from 0 to 20. The default value is 0.

Step 6  Click Next.

The Summary page appears with the details of the operation created.

Step 7  Click Finish.

The newly defined RTP operation is successfully created.

An error message appears if the Create operation fails.
Measuring Network Performance for Call Setup Post Dial Delay

The Cisco IOS IP Service Level Agreements (SLAs) VoIP Call Setup (Post-Dial Delay) Monitoring feature provides the ability to measure your network’s response time for setting up a Voice over IP (VoIP) call.

Using H.23 or Session Initiation Protocol (SIP), the IP SLAs or VoIP Call setup operation measures the total time taken to send and receive a call message. This measurement provides information if the dialed number rang or the called party answered the call.

In order to use the IP SLAs VoIP call setup functionality, your Cisco IOS software image must support the IP SLAs VoIP test-call application and IP SLAs VoIP Responder application.

To determine if your Cisco IOS software image is configured with these applications, use the show call application voice command in EXEC mode.

For this operation, you need not define a target device for the collector.

To measure end-to-end performance for Call Setup Post Dial Delay:

1. **Step 1** Define a device as the source device from which to measure performance.
   
   For details on defining a source device, see Specifying Source Devices.

2. **Step 2** Customize a Call Setup Post Dial Delay operation.
   
   For details on defining a Call Setup Post Dial Delay operation, see Defining a Call Setup Post Dial Delay Operation.

3. **Step 3** Define a collector to measure the network performance.
   
   For details on defining a collector, see Defining Collectors.

4. **Step 4** Generate the report to view the Call Setup Post Dial Delay statistics.
   
   For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.

Defining a Call Setup Post Dial Delay Operation

Call Setup Post Dial Delay operations measure your network’s response time for setting up a Voice over IP (VoIP) call. In addition, IPSLA Monitoring provides the option to create, modify, or delete your own Call Setup Post Dial Delay operations from the List of Operations page.

If a gatekeeper (GK) or directory gatekeeper (DGK) is involved in the H.323 call signaling, additional messages are sent and received between the originating and terminating gateways before the call message (containing a call number) is actually sent.

The additional time required for these messages is included in the IP SLAs VoIP call setup response time measurement.

Likewise, if a proxy server or redirection server is involved in the SIP call signaling, any additional time required for messages to be sent and received (before sending the call message) is included in the VoIP call setup response time measurement.

A traditional (plain old) telephone service (POTS) IP phone can be set up at the terminating gateway to respond to an IP SLAs VoIP call setup test call. As a convenient alternative to an actual IP phone, you can enable the IP SLAs VoIP Responder application in the terminating gateway.
The IP SLAs VoIP Responder application will respond to incoming call setup messages from the originating gateway using H.323 or SIP.

The IP SLAs VoIP Responder application is different from the IP SLAs Responder (which is configured using the IP SLA monitor Responder command in global configuration mode).

To define a Call Setup Post Dial Delay operation:

---

**Step 1**  
Select **Monitor > Performance Settings > IPSLA > Operations** from the menu.  
The List of Operations page appears.

**Step 2**  
Click **Create**.  
The General Settings page appears.

**Step 3**  
Select **CallSetupPostDialDelay** operation from the Type drop-down list.  
To complete other general setting parameters, see **General Settings for a User-Defined Operation**.

**Step 4**  
Click **Next**.  
The Specific Settings page appears.

**Step 5**  
Specify the following in the Settings section:  
- **Phone Number**—Specifies either the full E.164 telephone number or the dial peer number.  
- **Detect Point**—Sets the Voice over IP call setup operation to measure the response time for the called number to ring. The default value is 6.

**Step 6**  
Click **Next**.  
The Summary page displays the details of the operation that you have created.

**Step 7**  
Click **Finish**.  
The newly defined Call Setup Post Dial Delay operation is successfully created.  
An error message appears if the Create operation fails.
Measuring Network Performance for Gatekeeper Registration Delay

The VoIP (Voice over IP) Gatekeeper Registration Delay operation determines the average, median, or aggregated response time (delay) of registration attempts from a VoIP source router to a VoIP gatekeeper device.

To measure VoIP gatekeeper registration response time, the gatekeeper registration delay operation sends a lightweight Registration Request (RRQ) from an source router to a gatekeeper and records the amount of time taken to receive the Registration Confirmation (RCF) back from the gatekeeper.

For this operation, you need not define a target device for the collector.

To measure end-to-end performance for Gatekeeper Registration Delay:

**Step 1** Define a device as the source device from which to measure performance.
For details on defining a source device, see Specifying Source Devices.

**Step 2** Define a Gatekeeper Registration Delay operation. Use the default Gatekeeper Registration Delay operation or customize a Gatekeeper Registration Delay operation.
For details on defining a Gatekeeper Registration Delay operation, see Defining a Gatekeeper Registration Delay Operation.

**Step 3** Define a collector to measure performance between the source router and target you defined.
For details on defining a collector, see Defining Collectors.

**Step 4** Generate the report to view Gatekeeper Registration Delay statistics.
For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.

### Defining a Gatekeeper Registration Delay Operation

IPS LA Monitoring supports one default VoIP Gatekeeper Registration Delay operation for measuring performance of registration attempts from a VoIP source router to a VoIP gatekeeper.

In addition, IPSLA Monitoring provides the option to create, modify, or delete your own VoIP Gatekeeper Registration Delay operation from the List of Operations page.

To define a Gatekeeper Registration Delay operation:

**Step 1** Select Monitor > Performance Settings > IPSLA > Operations from the menu.
The List of Operations page appears.

**Step 2** Click Create.
The General Settings page appears.

**Step 3** Select GatekeeperRegistrationDelay operation from the Type drop-down list.
To complete other general setting parameters, see General Settings for a User-Defined Operation.

**Note** Ensure that you specify gatekeeper registration response time in the Rising Threshold field.

ClickFor details on defining a source device, see Specifying Source Devices.
Step 4 Define a Gatekeeper Registration Delay operation. Use the default Gatekeeper Registration Delay operation or customize a Gatekeeper Registration Delay operation.
For details on defining an Gatekeeper Registration Delay operation, see Defining a Gatekeeper Registration Delay Operation.

Step 5 Define a collector to measure performance between the source router and target you defined.
For details on defining a collector, see Defining Collectors.

Step 6 Generate the report to view Gatekeeper Registration Delay statistics.
For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.

Defining a Gatekeeper Registration Delay Operation

IPSLA Monitoring supports one default VoIP Gatekeeper Registration Delay operation for measuring performance of registration attempts from a VoIP source router to a VoIP gatekeeper.
In addition, IPSLA Monitoring provides the option to create, modify, or delete your own VoIP Gatekeeper Registration Delay operation from the List of Operations page.
To define a Gatekeeper Registration Delay operation:

Step 1 Select Monitor > Performance Settings > IPSLA > Operations from the menu.
The List of Operations page appears.
Step 2 Click Create.
Step 3 The General Settings page appears. Next.
The Summary page displays the details of the operation that you have created.
Step 4 Click Finish.
The newly defined VoIP Gatekeeper Registration Delay operation is successfully created.
An error message appears if the Create operation fails.

Measuring Network Performance for DNS

DNS operation latency is computed by measuring the time between sending a DNS request and receiving a reply. The operation queries for an IP address if you specify a host name or queries for a host name if you specify an IP address.
The DNS operation also measures availability and errors for DNS services.
To measure end-to-end performance for DNS:

Step 1 Define a device as the source device from which to measure performance.
For details on defining a source device, see Specifying Source Devices.
Step 2 Define a Lookup String (host name or IP address) as a target device.
For details on defining a target device, see Specifying Target Devices.
Step 3 Define a DNS operation. Use the DefaultDNS operation or customize a DNS operation. The DNS server is specified as part of the operation. For details on defining a DNS operation, see Defining a DNS Operation.

Step 4 Define a collector to measure performance between the source router and DNS servers. For details on defining a collector, see Defining Collectors.

Step 5 Generate the report to view the DNS statistics. For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.

---

Defining a DNS Operation

IPSLA Monitoring provides a default DNS operation for measuring performance between a source and a DNS server. In addition, IPSLA Monitoring provides the option to create, modify, or delete your own DNS operations from the List of Operations page.

Note The default DNS operation is available only on Solaris or Soft Appliance platform and not on Windows.

To define a DNS operation:

Step 1 Select Monitor > Performance Settings > IPSLA > Operations from the menu. The List of Operations page appears.

Step 2 Click Create. The General Settings page appears.

Step 3 Select DNS operation from the Type drop-down list. To complete other general setting parameters for the selected operation, see General Settings for a User-Defined Operation.

Step 4 Click Next. The Specific Settings page appears.

Step 5 Enter the host name or IP address for DNS server name in the DNS Server Details section. IPSLA Monitoring automatically creates the Default DNS operation at startup based on the DNS server configuration of the IPSLA Monitoring server.

Step 6 Click Next. The Summary page appears with the details of the operation created.

Step 7 Click Finish. The newly defined DNS operation is successfully created. An error message appears if the Create operation fails.
Measuring Network Performance for DHCP

The DHCP operation measures the round-trip latency time taken to discover a DHCP server and obtain a lease from it. After obtaining an IP address, IP SLA releases the IP address that was leased by the server.

The DHCP operates on two modes:
- By default, the DHCP operation sends discovery packets on every available IP interface on the source router.
- If a specific DHCP server is configured on the router, then discovery packets are sent to only that DHCP server.

The DHCP operation also measures availability and errors for DHCP services.

To measure end-to-end performance for DHCP:

Step 1  Define a device as the source device from which to measure performance.
For details on defining a source device, see Specifying Source Devices.

Step 2  Define a DHCP server as a target device.
For details on defining a target device, see Specifying Target Devices.

Step 3  Define a DHCP operation. Use the Default DHCP operation or customize a DHCP operation.
For details on defining a DHCP operation, see Defining a DHCP Operation.

Step 4  Define a collector to measure performance between the source router and DHCP servers.
For details on defining a collector, see Defining Collectors.

Step 5  Generate the report to view the DHCP statistics.
For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.

Defining a DHCP Operation

IPSLA Monitoring provides a default DHCP operation for measuring performance in leasing an IP address from a DHCP server. In addition, IPSLA Monitoring provides the option to create, edit, or delete your own DHCP operations from the List of Operations page.

To define a DHCP operation:

Step 1  Select Monitor > Performance Settings > IPSLA > Operations from the menu.
The List of Operations page appears.

Step 2  Click Create.
The General Settings page appears.

Step 3  Select DHCP operation from the Type drop-down list.
To complete other general setting parameters for the selected operation, see General Settings for a User-Defined Operation.
Step 4  
Click Next.
The Specific Settings page appears.

Step 5  
Either:
- Check the Enable the DHCP Server option.
  This allows you to enter the DHCP server name or IP address. IPSLA Monitoring will use this
  DHCP server for all those collectors which are configured for DHCP operation.

  Or
- Uncheck the Enable the DHCP Server option.
  If you have not checked Enable DHCP Server option then, the source will broadcast and select any
  of the DHCP servers configured on the network.

Step 6  
Click Next.
The Summary page appears with the details of the operation created.

Step 7  
Click Finish.
The newly defined DHCP operation is successfully created.
An error message appears if the Create operation fails.

---

**Measuring Network Performance for HTTP**

The HTTP operation measures the round-trip latency time required to connect to and access data from
an HTTP server. Three HTTP server response time measurements are made:
- DNS Lookup—Round-trip latency in looking up the domain name.
- TCP Connect—Round-trip latency in performing a TCP connect to the HTTP server.
- HTTP transaction time—Round-trip latency in sending a request to, and receiving a reply from, the
  HTTP server (the probe retrieves the base HTML page only).

The HTTP operation also measures availability and errors for HTTP services.
To measure end-to-end performance for HTTP:

---

**Step 1**  
Define a device as the source device from which to measure performance.
For details on defining a source device, see Specifying Source Devices.

**Step 2**  
Define an HTTP server as a target device.
For details on defining a target device, see Specifying Target Devices.

**Step 3**  
Customize an HTTP operation.
For details on defining an HTTP operation, see Defining an HTTP Operation.
Step 4 Define a collector to measure performance between the source device and the HTTP servers. For details on defining a collector, see Defining Collectors.

Step 5 Generate the report to view the HTTP statistics. For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.

**Defining an HTTP Operation**

The List of Operations page allows you to create, modify, or delete your own HTTP operations for measuring performance in connecting and accessing data from an HTTP server. IPSLA Monitoring does not provide a default HTTP operation.

To define an HTTP operation:

**Step 1** Select Monitor > Performance Settings > IPSLA > Operations from the menu. The List of Operations page appears.

**Step 2** Click Create. The General Settings page appears.

**Step 3** Select HTTP operation from the Type drop-down list.

To complete other general setting parameters, see General Settings for a User-Defined Operation.

**Step 4** Click Next. The Specific Settings page appears.

**Step 5** Specify the following in the Packet Settings section:

- IP QoS Type—Select the IP QoS Type as IP Precedence or DSCP.
- IP QoS Settings—Select a value from the drop-down list. The values change based on your IP QoS Type selection.
  - If you have selected IP QoS Type as IP Precedence, select the IP QoS Settings value from the drop-down list. The value you select sets the priority for the request packet. The default setting is 0 (no priority). This option sets the ToS bits in the IP packet.
  - If you have selected IP QoS Type as DSCP, select the desired IP QoS Settings value from the drop-down list. The value you select defines the packet priority and is based on the DSCP RFC standards.

**Step 6** Specify the following in the Lookup Settings section:

- Use DNS Server Name — Check this check box if you want to enter a name for the DNS server.
- DNS Server Name — Enter a IP Address or hostname for the DNS server. This textbox is activated only if you check the Use DNS Server Name check box.
- URL Relative Path—Enter the URL to use for the HTTP request. IPSLA Monitoring validates the format of the HTTP string that you enter in the URL Lookup String field. The URL that you enter must be in the /path/filename or filename format.

If you specify the path in the URL Relative Path field, the next two characters that follow a ‘%’ should be hexadecimal values. The maximum length of characters that you can specify in the URL Relative Path field is 127.
IPSLA Monitoring displays appropriate error messages if any of the variables you enter in the URL string is incorrect.

- **Port**—Port number should be greater than 0 and less than 65536. The default value is 80.
- **Download URL From Cache**—Select the check box if you want the source to search its cache for the Website and, if it is found, download it instead of querying the Website.
  
  Deselect the check box if you want the router to query the Website for the HTTP request. By default, the check box is not selected.

**Step 7** Specify the following in the Proxy Server Settings section:

- **Use HTTP Proxy Server**—Select the check box to configure IPSLA Monitoring to use a proxy server.
- **Proxy Server**—Enter the name or address of the proxy server to configure IPSLA Monitoring to use a proxy server.

  IPSLA Monitoring will use the proxy server you specify for collectors you have configured for the HTTP operation.

  The default port for the HTTP proxy server would be 80, and the type of proxy server would be HTTP. You can set proxy server settings for IOS versions 12.1(9a) and above. To specify a different proxy port, enter the server name as: `http proxy server: port number`.

**Step 8** Click **Next**.

The Summary page appears with the details of the operation created.

**Step 9** Click **Finish**.

The newly defined HTTP operation is successfully created.

An error message appears if the Create operation fails.

---

**Measuring Network Performance for FTP**

FTP is an application protocol, part of the Transmission Control Protocol (TCP)/IP protocol stack, used for transferring files between network nodes. The FTP operation measures the round-trip latency time required to connect to and access data from an FTP server.

The FTP transaction time server response shows the round-trip latency in sending a request to, and downloading the file from the FTP server.

The FTP operation also measures availability and errors for FTP services.

To measure end-to-end performance for FTP:

**Step 1** Define a device as the source device from which to measure performance.

For details on defining a source device, see **Specifying Source Devices**.

**Step 2** Define a FTP server as a target device.

For details on defining a target device, see **Specifying Target Devices**.

**Step 3** Customize an FTP operation.

For details on customizing an FTP operation, see **Defining an FTP Operation**.
Using IPSLA Operations to Measure Network Performance

### Defining an FTP Operation

Use the List of Operations page to create, modify, or delete your own FTP operations for measuring performance while connecting and accessing data from an FTP server. IPSLA Monitoring does not provide a default FTP operation.

To define an FTP operation:

**Step 1** Select **Monitor > Performance Settings > IPSLA > Operations** from the menu.

The List of Operations page appears.

**Step 2** Click **Create**.

The General Settings page appears.

**Step 3** Select FTP operation from the Type drop-down list.

To complete other general setting parameters, see **General Settings for a User-Defined Operation**.

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

The Specific Settings page appears.

**Step 5** Specify the following in the Packet Settings section:

- **IP QoS Type**—Select IP QoS as IP Precedence or DSCP.
- **IP QoS Settings**—Select a value from the drop-down list. The values change based on your IP QoS Type selection.
  - If you have selected IP QoS Type as IP Precedence, select the IP QoS Settings value from the drop-down list. The values range from 0 to 7. The value you select sets the priority for the request packet. The default setting is 0 (no priority). This option sets the ToS bits in the IP packet.
  - If you have selected IP QoS Type as DSCP, select the desired IP QoS Settings value from the drop-down list. The values range from 0 to 63. The value you select defines the packet priority and is based on the DSCP RFC standards.

**Step 6** Specify the following in the Lookup Settings section:

- Enter the user name and password in the User Name and Password fields to access the FTP server. Use the default values to access an anonymous FTP server.

  IPSLA Monitoring function checks the syntax and also checks whether:
  - The username contains only alphanumerical characters, safe characters ($',*,.-:',:+), and extra characters (',",',0x27,0x28,0x29).
  - The password contains only alphanumerical characters, safe characters, extra characters, and ' %'.

---

**Step 4** Define a collector to measure performance between the source device and the FTP servers.

For details on defining a collector, see **Defining Collectors**.

**Step 5** Generate the report to view the FTP statistics.

For more information on generating the report, see **Reports Management with Cisco Prime LAN Management Solution 4.1**.
• Enter the file location in the File Location field. Use the following guidelines to enter a file location:
  - To select a relative path use /, this will look for the file in the User’s Home Directory
    Example
    /Documents and Settings/<username>/myfile.sh
    Where myfile.sh is the name of the file and /Documents and Settings/<username> is the User’s Home Directory.
    Specifying single slash will assume that the relative path is considered.
  - To select an absolute path use //, this will look for the file in the absolute path not relative to the User’s Home directory.
    Example
    //opt/CSCOpx/bin/myfile.sh
    Where myfile.sh is the name of the file
  - IPSLA Monitoring function checks the syntax and also checks whether:
  The path, dir/file, contains only alphanumerical characters, safe characters, extra characters, reserved characters ("?','@','&','=','.'), ' ' and '%'
• Select the mode of FTP session from the drop-down list.
  - In Active FTP, the client opens a control connection on port 21 to the server, and whenever the client requests data from the server, the server opens a TCP session on port 20.
  - In Passive FTP, the client opens the data sessions, using a port number supplied by the server. This is the default FTP mode.

**Step 7** Click **Next**.
The Summary page appears with the details of the operation created.
**Step 8** Click **Finish**.
The newly defined FTP operation is successfully created.
An error message appears if the Create operation fails.

---

**Measuring Network Performance for DLSw**

DLSw+ is the enhanced Cisco version of DSCP RFC 1795. DLSw+ tunnels SNA traffic over IP backbones using TCP. The routers performing the tunneling of SNA traffic onto TCP/IP are referred to as DLSw peers.
The DLSw operation measures the DLSw+ protocol stack and round-trip latency between DLSw peers. Normally DLSw peers communicate through TCP port 2065.
To successfully run the DLSw operation you must have a connected DLSw+ peer between the source and destination Cisco devices. On the source DLSw+ device, an operation can be defined for a DLSw+ partner peer. The DLSw operation also measures availability and errors for DLSw services.
To measure the round-trip latency between two DLSw peers, the IP address that you define as the source router must be one of the DLSw peers. Also, the IP address that you define as the target router must be configured as the DLSw peer to the source router.
To measure end-to-end performance for DLSW:

**Step 1** Define a device as the source device from which to measure performance.
For details on defining a source device, see Specifying Source Devices.

**Step 2** Define a device as the target of discovery requests from the source device.
For details on defining a target, see Specifying Target Devices.

**Step 3** Define a DLSw operation. Use the DefaultDLSw operation or customize a DLSw operation.
For details on defining an DLSW operation, see Defining a DLSw Operation.

**Step 4** Define a collector to measure performance between the source router and target you defined.
For details on defining a collector, see Defining Collectors.

**Step 5** Generate the report to view the DLSW statistics.
For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.

---

### Defining a DLSw Operation

IPSLA Monitoring provides a default DLSw operation for measuring performance between a source and target. In addition, IPSLA Monitoring provides the option to create, modify, or delete your own DLSw operations from the List of Operations page.

To define a DLSw operation:

**Step 1** Select **Monitor > Performance Settings > IPSLA > Operations** from the menu.
The List of Operations page appears.

**Step 2** Click **Create**.
The General Settings page appears.

**Step 3** Select DLSW operation from the Type drop-down list.
To complete other general setting parameters, see General Settings for a User-Defined Operation.

**Step 4** Click **Next**.
The Specific Settings page appears.

**Step 5** Enter the number of bytes to use for the size of the payload of the request packet in the Request Payload.
The values can be less than or equal to 16384. The default value is 64 bytes.

**Step 6** Click **Next**.
The Summary page displays the operation details that you have created.

**Step 7** Click **Finish**.
The newly defined DLSw operation is successfully created.
An error message appears if the Create operation fails.
Measuring Network Performance for TCP Connect

The TCP Connect operation in IPSLA Monitoring measures round-trip latency between a source and any IP-enabled device running TCP services. Latency is computed by measuring the time taken by the source to perform a TCP Connect operation to the target device.

This operation is useful for simulating Telnet or HTTP connection times. The TCP operation also measures availability and errors for TCP services.

You can specify any port number, well known or otherwise, on any IP host, Cisco or non-Cisco, as long as someone is listening on that port on the target. A well known port is a port number less than or equal to 1024 (for example, 21 for FTP, 23 for Telnet, and 80 for HTTP).

IPSLA Monitoring provides default TCP Connection operations for several of these common TCP services.

To measure end-to-end latency for TCP Connect:

**Step 1** Define a device as the source device from which to measure performance.
For details on defining a source device, see Specifying Source Devices.

**Step 2** Define a device as the target of connection requests from the source device.
For details on defining a target, see Specifying Target Devices.

**Step 3** Define a TCP operation. Use one of the default operations for TCP or customize a TCP operation.
For details on defining a TCP operation, see Defining a TCP Connect Operation.

**Step 4** Define a collector to measure performance between the source router and target you defined.
For details on defining a collector, see Defining Collectors.

**Step 5** Generate the report to view the TCP Connect statistics.
For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.

Defining a TCP Connect Operation

IPSLA Monitoring provides several default TCP operations for measuring performance between a source and target. In addition, IPSLA Monitoring provides the option to create, modify, or delete your own TCP operations from the List of Operations page.

To define a TCP Connect operation:

**Step 1** Select Monitor > Performance Settings > IPSLA > Operations from the menu.
The List of Operations page appears.

**Step 2** Click Create.
The General Settings page appears.

**Step 3** Select TCPConnect operation from the Type drop-down list.
To complete other general setting parameters, see General Settings for a User-Defined Operation.

**Step 4** Click Next.
The Specific Settings page appears.
Step 5  Specify the following in the Packet Settings section:

- **IP QoS Type**—Select the IP QoS Type as IP Precedence or DSCP.
- **IP QoS Settings**—Select a value from the drop-down list. The values change based on your IP QoS Type selection.
  - If you have selected IP QoS Type as IP Precedence, select the IP QoS Settings value from the drop-down list. The values range from 0 to 7. The value you select sets the priority for the request packet. The default setting is 0 (no priority). This option sets the ToS bits in the IP packet.
  - If you have selected IP QoS Type as DSCP, select the desired IP QoS Settings value from the drop-down list. The values range from 0 to 63. The value you select defines the packet priority and is based on the DSCP RFC standards.

Step 6  Specify the following in the Other Settings section:

- **Target Port**—Enter the TCP port number. The target device uses the specified port number when sending a response to a connection request. Valid values range from 1 to 65535. The default setting is 3000. You can specify any port number, known or unknown, on any IP host, Cisco or non-Cisco, as long as someone is listening on that target port.
  - If the port number specified is less than 1024, then your target device can be a Cisco Responder or any IP reachable device.
  - If the port number specified is greater than 1024, then your target device must be a Cisco IP SLA Responder enabled device.
- **Control Enable**—Select True or False from the drop-down list. The value you select depends on the value specified for the target port.
  - If you have specified a known port (such as less than 1024), then you have to select False from the drop-down list.
  - If you have specified an unknown port (such as greater than 1024), then you have to select True from the drop-down list.

Step 7  Click Next.

The Summary page appears with the details of the operation created.

Step 8  Click Finish.

The newly defined TCP Connect operation is successfully created. An error message appears if the Create operation fails.
Measuring Network Performance for Ethernet Ping

IPSLA Ethernet Ping operation measures the Round-trip time latency and Errors by sending frames to a Maintenance End Point (MEP). To measure end-to-end performance for Ethernet Ping:

**Step 1** Define a device as the source device from which to measure performance.
For details on defining a source device, see [Specifying Source Devices](#).

**Step 2** Define an Ethernet Ping operation.
For details on defining an Ethernet Ping operation, see [Defining an Ethernet Ping Operation](#).

**Step 3** Define a collector to measure performance between the source router and maintenance endpoint (MEP) you defined.
For details on defining a collector, see [Defining Collectors](#).

**Step 4** Generate the report to view the Ethernet Ping statistics.
For more information on generating the report, see [Reports Management with Cisco Prime LAN Management Solution 4.1](#).

Defining an Ethernet Ping Operation

IPSLA Monitoring allows you to create, modify, or delete your own Ethernet Ping operations from the List of Operations page for measuring Round-trip time latency and Errors between a source and MEP.

To define an Ethernet Ping operation:

**Step 1** Select **Monitor > Performance Settings > IPSLA > Operations** from the menu.
The List of Operations page appears.

**Step 2** Click **Create**.
The General Settings page appears.

**Step 3** Select **EthernetPing** from the Type drop-down list.
To complete other general setting parameters, see [General Settings for a User-Defined Operation](#).

**Step 4** Click **Next**.
The Specific Settings page appears.
Step 5 Specify the following in the Specific Settings section:
   - **Probe Settings**
     - MPID—Specify the MEP ID between 1 to 8191. For example, 1,2,6,9-10
     - Domain Name—Specify the domain name. For example, PROVIDER_DOMAIN
     - VLAN ID—Specify the VLAN ID between 1 to 4095.
   - **Other Settings**
     - Class of Service—Specify the class of service between 0 to 7.
     - Packet Request Size—Specify the packet request size between 0 to 1400.

Step 6 Click *Next*.
The Summary page appears with the details of the operation created.

Step 7 Click *Finish*.
The newly defined Ethernet Ping operation is successfully created.
An error message appears if the Create operation fails.

---

**Measuring Network Performance for Ethernet Jitter**

IPSLA Ethernet Jitter operation measures the following statistics by sending and receiving Ethernet data frames between a source MEP and a destination MEP:
   - Jitter (source-to-destination and destination-to-source)
   - Round-trip time latency
   - Unprocessed packets
   - Packet loss (source-to-destination and destination-to-source)
   - Out-of-sequence, tail-dropped, and late packets

To measure end-to-end performance for Ethernet Jitter:

---

**Step 1** Define a device as the source device from which to measure performance.
For details on defining a source device, see *Specifying Source Devices*.

**Step 2** Define an Ethernet Jitter operation.
For details on defining a Ethernet Jitter operation, see *Defining an Ethernet Jitter Operation*.

**Step 3** Define a collector to measure performance between the source router and MEP you defined.
For details on defining a collector, see *Defining Collectors*.

**Step 4** Generate the report to view the Ethernet Jitter statistics.
For more information on generating the report, see *Reports Management with Cisco Prime LAN Management Solution 4.1*. 
Defining an Ethernet Jitter Operation

IPSLA Monitoring provides the option to create, modify, or delete your own Ethernet Jitter operations from the List of Operations page for measuring performance between a source and MEP.

To define a Ethernet Jitter operation:

**Step 1**
Select **Monitor > Performance Settings > IPSLA > Operations** from the menu.

The List of Operations page appears.

**Step 2**
Click **Create**.

The General Settings page appears.

**Step 3**
Select **EthernetJitter** from the Type drop-down list.

To complete other general setting parameters, see **General Settings for a User-Defined Operation**.

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

The Specific Settings page appears.

**Step 5**
Specify the following in the Specific Settings section:

- **Probe Settings**
  - MPID—Specify the MEP ID between 1 to 8191. For example, 1,2,6,9-10
  - Domain Name—Specify the domain name. For example, PROVIDERDOMAIN
  - VLAN ID—Specify the VLAN ID between 1 to 4095.

- **Frame Settings**
  - Frame Interval—Specify the interval between 1 to 60000.
  - No. of Frames—Specify the number of frames between 1 to 60000.

- **Other Settings**
  - Class of Service—Specify the class of service between 0 to 7.
  - Packet Request Size—Specify the packet request size between 0 to 1400.

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

The Summary page appears with the details of the operation created.

**Step 7**
Click **Finish**.

The newly defined Ethernet Jitter operation is successfully created.

An error message appears if the Create operation fails.
Measuring Network Performance for Ethernet Ping Auto IP SLA

You can use Ethernet Ping Auto IP SLA feature to create individual Ethernet Ping operations. You can do this by querying the Ethernet Connectivity Fault Management (CFM) database based on the MEPs discovered in a maintenance domain and VLAN.

Ethernet Ping Auto IP SLA measures the following statistics:
- Round-trip time latency
- Errors

To measure end-to-end performance for Ethernet Ping Auto IP SLA:

Step 1 Define a device as the source device from which to measure performance.
For details on defining a source device, see Specifying Source Devices.

Step 2 Define an Ethernet Ping Auto IP SLA operation.
For details on defining a Ethernet Ping Auto IP SLA operation, see Defining an Ethernet Ping Auto IP SLA Operation.

Step 3 Define a collector to measure performance between the source router and target you defined.
For details on defining a collector, see Defining Collectors.

Step 4 Generate the report to view the Ethernet Ping Auto IP SLA statistics.
For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.

Defining an Ethernet Ping Auto IP SLA Operation

IPSLA Monitoring allows you to create, modify, or delete your own Ethernet Ping Auto IP SLA operations from the List of Operations page for measuring performance between a source and an MEP.

To define a Ethernet Ping Auto IP SLA operation:

Step 1 Select Monitor > Performance Settings > IPSLA > Operations from the menu.
The List of Operations page appears.

Step 2 Click Create.
The General Settings page appears.

Step 3 Select EthernetPingAutoIPSLA from the Type drop-down list.
To complete other general setting parameters, see General Settings for a User-Defined Operation.

Step 4 Click Next.
The Specific Settings page appears.
**Step 5** Specify the following in the Specific Settings section:
- **Probe Settings**
  - Domain Name—Specify the domain name. For example, PROVIDER_DOMAIN
  - VLAN ID—Specify the VLAN ID between 1 to 4095.
  - Schedule Period—Specify the schedule for Auto IP SLA (value in seconds).
  - Exclude MPID—The MEP IDs entered will be excluded for Auto IP SLA. Specify the MEP ID between 1 to 8191. For example, 1,2,6,9-10
- **Other Settings**
  - Class of Service—Specify the class of service between 0 to 7.
  - Packet Request Size—Specify the packet request size between 0 to 1400.

**Step 6** Click **Next**.
The Summary page appears with the details of the operation created.

**Step 7** Click **Finish**.
The newly defined Ethernet Ping Auto IP SLA operation is successfully created. An error message appears if the Create operation fails.

---

**Measuring Network Performance for Ethernet Jitter Auto IP SLA**

Ethernet Jitter Auto IP SLA operation can be used to automatically create individual Ethernet Jitter operations. This is done by querying the Ethernet CFM database based on the MEPs discovered in a maintenance domain and VLAN.

Ethernet Jitter Auto IP SLA measures the following statistics:
- Jitter (source-to-destination and destination-to-source)
- Round-trip time latency
- Unprocessed packets
- Packet loss (source-to-destination and destination-to-source)
- Out-of-sequence, tail-dropped, and late packets

To measure end-to-end performance for Ethernet Jitter Auto IP SLA:

**Step 1** Define a device as the source device from which to measure performance.
For details on defining a source device, see [Specifying Source Devices](#).

**Step 2** Define an Ethernet Jitter Auto IP SLA operation.
For details on defining a Ethernet Jitter Auto IP SLA operation, see [Defining an Ethernet Jitter Auto IP SLA Operation](#).

**Step 3** Define a collector to measure performance between the source router and the target you defined.
For details on defining a collector, see [Defining Collectors](#).
**Defining an Ethernet Jitter Auto IP SLA Operation**

IPSLA Monitoring provides the option to create, modify, or delete your own Ethernet Jitter Auto IP SLA operations from the List of Operations page for measuring performance between a source and an MEP.

To define an Ethernet Jitter Auto IP SLA operation:

**Step 1** Select **Monitor > Performance Settings > IPSLA > Operations** from the menu.

The List of Operations page appears.

**Step 2** Click **Create**.

The General Settings page appears.

**Step 3** Select **EthernetJitterAutoIPSLA** from the Type drop-down list.

To complete other general setting parameters, see General Settings for a User-Defined Operation.

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

The Specific Settings page appears.

**Step 5** Specify the following in the Specific Settings section:

- **Probe Settings**
  - Domain Name—Specify the domain name. For example, PROVIDER_DOMAIN
  - VLAN ID—Specify the VLAN ID between 1 to 4095.
  - Schedule Period—Specify the schedule for Auto IP SLA between 1 to 604800 (value in seconds).
  - Exclude MPID—The MEP IDs entered will be excluded for Auto IP SLA. Specify the MEP ID between 1 to 8191. For example, 1,2,6,9-10

- **Frame Settings**
  - Frame Interval—Specify the interval between 1 to 60000.
  - No. of Frames—Specify the number of frames between 1 to 60000.

- **Other Settings**
  - Class of Service—Specify the class of service between 0 to 7.
  - Packet Request Size—Specify the packet request size between 0 to 1400.

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

The Summary page appears with the details of the operation created.

**Step 7** Click **Finish**.

The newly defined Ethernet Jitter Auto IP SLA operation is successfully created. An error message appears if the Create operation fails.
Measuring Network Performance for Video

The platform-independent IP SLA software feature in Cisco IOS software is incapable of generating the high data rates, 4 to 16 Mbps, which are typical for video applications. To eliminate the protocol overhead and the process scheduling delays that contribute to the limitations of the earlier IP SLAs software to generate video traffic, the Cisco IP SLAs Video Operation feature makes the traffic generation and transmission routines platform dependent.

This section explains:
- Prerequisites for IPSLA Video Operations
- Restrictions for IPSLA Video Operations
- Video Operation-specific MIBs
- Procedure for measuring end-to-end performance for Video

Prerequisites for IPSLA Video Operations
The following are the prerequisites for IPSLA Video Operations:
- Your networking device must be running Cisco IOS 12.2(58)SE or a later release.
- Both the source and responder devices for the IP SLAs video operation must be capable of providing platform-assisted video traffic generation and reflection.
- Time synchronization provided by Network Time Protocol (NTP) is required between the source and the responder device to provide accurate one-way delay (latency) measurements.

Restrictions for IPSLA Video Operations
The following are the restrictions for IPSLA Video Operations:
- This feature is supported only on Cisco devices that are capable of generating platform-assisted video traffic and reflection, such as Cisco Catalyst 3560-X, 3750, 3750-E, 3750-X, 3650, and 3650-E Series switches.
- IP SLAs video operations do not support Round Trip Time (RTT) traffic.
- Because IP SLAs video operations support only one-way traffic, an operation and a responder must be configured on both the source and responder and both devices must support SNMP access.
- IP SLAs video operations are supported in IPv4 networks only.

Video Operation-specific MIBs
Following are the MIBs are used for storing and configuring the Video operations:
- CISCO-IPSLA-VIDEO-MIB
- CISCO-RTTMON-MIB
- CISCO-RTTMON-TC-MIB
Procedure for measuring end-to-end performance for Video

To measure end-to-end performance for Video:

---

**Step 1** Define a device as the source device from which performance is to be measured.
For details on defining a source device, see Specifying Source Devices.

**Step 2** Define a device as the target of discovery requests from the source device.
For details on defining a target, see Specifying Target Devices.

**Step 3** Customize a Video operation.
For details on defining a Video operation, see Defining a Video Operation.

**Step 4** Define a collector to measure performance between the source router and target you defined.
For details on defining a collector, see Defining Collectors.

**Step 5** Generate the report to view the Video statistics.
For more information on generating the report, see Reports Management with Cisco Prime LAN Management Solution 4.1.

---

### Defining a Video Operation

To define a Video operation:

---

**Step 1** Select Monitor > Performance Settings > IPSLA > Operations from the menu.
The List of Operations page appears.

**Step 2** Click Create.
The General Settings page appears.

**Step 3** Select Video operation from the Type drop-down list.
To complete other general setting parameters, see General Settings for a User-Defined Operation.

**Step 4** Click Next.
The Specific Settings page appears.

**Step 5** Specify the following in the Video Operation section:

- Source Port — Enter a value for Source port number ranging from 1 to 65535. Default value is 1.
- Target Port — Enter a value for Target port number ranging from 1 to 65535. Default value is 1
- Call Duration — Enter a value for Source port number ranging from 1 to 600 seconds. Default duration is 20 seconds
- Profile Name — Select a type of the video traffic from the drop-down list.
The available video profiles are:
  - IPTV
  - IPVSC
  - Telepresence

**Step 6** Click Next.
The Summary page appears with the details of the operation created.

**Step 7**  
Click **Finish**.

The newly defined Video operation is successfully created.  
An error message appears if the Create operation fails.

---

**Bandwidth Limitations on Video Operations**

When you create video probes on the device with different video profiles and varying operation frequencies, the latest operation return code for some probes can be Busy / Timeout. The statistics may not be generated. This may be because of the large number of video probes created on the device.

Hence, there is a limitation in the number of video probes that can be created on the device and it depends on the bandwidth of the device.

Following is the bandwidth for each video profile:

- **IPTV** — IP television traffic (2.6 Mbps)
- **IPVSC** — IP video surveillance camera traffic (2.2 Mbps)
- **Telepresence** — Cisco TelePresence 1080P traffic (6.6Mbps)

**Example:**

If the bandwidth of the device is 20Mbps, you can create the following number of video probes for video endpoints.

- **IPTV** — 8 Video probe sessions
- **IPVSC** — 9 Video probe sessions
- **Telepresence** — 3 Video probe sessions
Managing Outage Details

Outages or downtime refers to the time span when the network fails to provide its primary function. This chapter explains how you can create, edit, and delete planned outage. The feature provides support to configure Network planned outage details in IPSLA Monitoring device function. It also gives details of completed planned outages.

This section contains the following topics:

- Understanding Planned Outage
- Creating Planned Outage
- Editing Planned Outage
- Deleting Planned Outage
- Viewing Completed Planned Outages

Understanding Planned Outage

IPSLA Monitoring device function has been enhanced to support planned network outage intervals for existing collectors.

The Planned network outage details will be utilized for the Availability hourly report during the report generation to render water mark on the availability hourly chart.

However, the hourly daily availability consolidation will exclude the availability statistics collected for the planned network outage period.

By default, the outage period data is excluded while generating the IPSLA Summarized Reports.

Note
Outage configuration is applicable only for Historical collectors and not Real-time collectors.

To navigate to the Outage screen, go to Monitor > Performance Settings > IPSLA > Outage Settings. The Outage Settings are listed in Table 17-1.

<table>
<thead>
<tr>
<th>Table 17-1 Outage Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fields</strong></td>
</tr>
<tr>
<td>Outage Name</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>
Creating Planned Outage

You can create Planned outage for once, weekly, or monthly period.

To create Planned outage:

Step 1 Select Monitor > Performance Settings > IPSLA > Outage Settings.
   The Outage Settings page appears.

Step 2 Click Create.
   The Select Collectors page is displayed with the following details:
   • Collectors
   • Source
   • Target
   • Operation
   • Start date
   • End date
   • Status

Note The completed collectors, config failed and Auto IPSLA parent collectors are not included during outage creation.

Step 3 Select atleast a collector and click Next.
   The Outage Configuration page appears.

### Table 17-1 Outage Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>Time when the outage is scheduled to begin.</td>
</tr>
<tr>
<td>End Time</td>
<td>Time when the outage is scheduled to end.</td>
</tr>
<tr>
<td>Recurrence Type</td>
<td>Type of recurrence that is selected such as once, weekly or monthly.</td>
</tr>
<tr>
<td>Recurrence On</td>
<td>The day when the outage re-occurs.</td>
</tr>
<tr>
<td>Collectors Affected</td>
<td>Lists the number of collectors affected during the outage period.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the outage such as Active, Schedule.</td>
</tr>
</tbody>
</table>

Note The Outages that are in Complete state are moved to Completed Outage page and do not appear in the status column.
Step 4 Enter the Outage Configuration details:

- Outage Details:
  - Outage Name — Enter the outage name in the Outage Name field.
  - Description— Enter the description of the outage name in the Description field.
- Recurrence Type — Can be Once, Weekly, or Monthly.

If you select Once:

   a. Specify the start date and time of the outage.
   b. Specify the end date and time of the outage.
   c. Select the date by clicking the calendar icon
   d. Select the time from the drop-down list.

Note You can configure an outage period report if the time interval is at least one hour.

If you select Weekly:

   a. Select the start time and end time from the drop-down list
   b. Select the weekdays from the check box displayed. However, by default all days are selected.

If you select Monthly:

   a. Select the start time and end time from the drop-down list.
   b. Select the day of every month from the day drop-down list.

Note While selecting either Weekly or Monthly option, you cannot schedule an outage spanning two days (For example from 23:00 hrs to 01:00 hrs)
However, if you have selected once, then you can schedule an outage spanning across two days.

Step 5 Click Next

The Outage Summary page appears.

You can view the Outage summary details such as the description, type and the configuration details.

Step 6 Click Finish and the Outage Settings page appears.
Editing Planned Outage

You can edit only scheduled outages. You cannot edit completed or active outages and the recurrence Type.

To edit a Planned outage:

**Step 1** Select Monitor > Performance Settings > IPSLA > Outage Settings.
The Outage Settings page appears.

**Step 2** Select an outage from the Outage Settings screen.

**Step 3** Click Edit
The Select Collectors page appears.
You can select or deselect the number of collectors for which outages are created.

**Step 4** Click Next.
The Outage Configuration page appears where you can edit the details.

**Step 5** Click Next.
The Outage Summary page appears with the updated details.

**Step 6** Click Finish.
The Outage Settings page appears with the edited outage.

Deleting Planned Outage

You can delete only scheduled outages. You cannot delete Completed or Active outages.
If all the collectors associated with the outage is deleted, then the outage will also be deleted automatically.
The completed outages that are in the hourly purging period are also deleted.

To delete a Planned outage:

**Step 1** Select Monitor > Performance Settings > IPSLA > Outage Settings.
The Outage Settings page appears.

**Step 2** Select an outage from the Outage Settings page.

**Step 3** Click Delete.
The Delete Confirmation dialog box appears.

**Step 4** Click OK to delete the outage for the selected collector.
Or

**Step 5** Click Cancel to return to the Outages Details screen.
Viewing Completed Planned Outages

You can also view Completed Planned outage details.
To view Completed Planned outages:

**Step 1** Select Monitor > Performance Settings > IPSLA > Outage Settings.
The Outage Settings page appears.

**Step 2** Click Completed Outages.
The Completed Outages report page appears.
You can view the report details such as outage name, description, start date, end date, recurrence type and affected collectors.

**Step 3** Click Close to return to the Outage Settings page
This section describes the command line interface (CLI) commands that you can use to manage LMS Performance Monitor application.

The commands described in this section are:

- `ipm -help`
- `ipm addadhoctarget`
- `ipm baseline`
- `ipm deletedevice`
- `ipm export`
- `ipm exportstats`
- `ipm importcollector`
- `ipm controlcollector`
- `ipm deletereports`
- `ipm generatereports`
- `ipm listcollectors`
- `ipm -v`
- `ipm enableipslaresponder`

Some IPSLA Device Management commands are run only by the root user while the others are run by the root user and also by members of the casusers group.

This section contains:

- Using CLI Command
- Arguments
- IPSLA Monitoring CLI Commands
Using CLI Command

In addition to using the graphical-based device configuration functions, you can use the `ipm` command-line utility to perform tasks on the devices, collectors, or on both.

For more details, see these topics:

- Setting CWCLIFILE Environment Variable
- Running IPSLA Monitoring CLI Commands

On all supported platforms, the files that are created by IPSLA Monitoring are owned by casuser. They belong to the same group as the user (casuser) who created the files, and have read-write access for both casuser and the group.

---

**Note**

Your login determines whether you can use this argument.

---

Setting CWCLIFILE Environment Variable

You can store your username and password in a file and set an environment variable `CWCLIFILE` which points to the file, if you want to avoid the `-p` argument which will reveal the password in clear text in CLI.

You should maintain this file and control access permissions to prevent unauthorized access. If `CWCLIFILE` is set only to filename instead of full path, IPSLA Monitoring framework looks for the current working directory.

If you use the `-p` argument, even after setting the `CWCLIFILE` variable, the password is taken from the command line instead of `CWCLIFILE`. This is not secure and usage of this argument is not recommended.

The password must be provided in the file in the following format:

```
username password
```

Where username and password are the LMS login credentials. The delimiter between the username and password is a single space.

You must enter a comma as the delimiter if the password is blank. Otherwise, IPSLA Monitoring framework cannot validate the password.

**Example**

To run the `ipm` command with the `CWCLIFILE` file on Windows, enter the following at the command prompt:

```
C:\Program Files\CSCOpx\bin>set CWCLIFILE=D:\ciscoworks\password.txt
```

Where the file, `password.txt` contains the username and password for LMS server.
Running IPSLA Monitoring CLI Commands

The `ipm` command is located in the following directories, where install_dir is the directory in which LMS is installed:

- On Solaris or Soft Appliance systems: `/opt/CSCOpx/bin`
- On Windows systems: `install_dir\CSCOpx\bin`

The default install directory is `C:\Program Files`.

If you install LMS on Windows on an NTFS partition, only users in the administrator or casuser group can access LMS.

Users with read-write access to the `CSCOpx\files\archive` directory and the directories under that can also use LMS.

Examples of `ipm` Commands

1. `ipm exportstats`
   ```
   ipm exportstats -u admin -p admin -m user@domain.com -coll C3_DHCP -start '2006-12-29 01:47:37.000' -end '2006-12-30 01:47:37.000' -granularity h -reportType a
   ```
   **Output**
   Successful: `ipm` exportstats: 
   This result occurs when the collector statistics is successfully exported.

2. `ipm deletedevice`
   ```
   ipm deletedevice -u admin -p admin -device 255.255.255.255
   ```
   **Output**
   <ipm> INFO - Done with the execution of the command. 
   This result occurs when the device is successfully deleted.

Arguments

Many of the arguments are common to all commands. These arguments can be broadly classified as those that are expected by every command (function independent) and those that are specific to the context of a command.

This section explains:

- Mandatory Arguments
- Function-independent Arguments
- Function-dependent Arguments
- Function-specific Arguments
- Input List File Format
Mandatory Arguments

You must use the following arguments with all commands.

- **u userid**

  Specifies the LMS username. You must define an environment variable ipm CWCLIFILE with value set to a filename, which will contain the corresponding password.

  You should maintain the file. You can control the access permissions of this file to prevent unauthorized access. ipm looks for current working directory if ipm CWCLIFILE is set to only file name instead of full path.

  If -u argument is used along with -p argument, the password is taken from the command line instead of ipm CWCLIFILE. This is not secure and we recommend that you do not use this argument.

  The password must be provided in the file in the following format:

      username password

  Where username is the LMS user name given in command line. The delimiter between username and password is single blank space.

  You must provide the delimiter if the password is blank. Otherwise, ipm will not validate the password. The password file can contain multiple entries with different user names. The password of the first match is considered in case of duplicate entries.

  For more information, see Setting CWCLIFILE Environment Variable.

Function-independent Arguments

You can use the following arguments without any commands:

- **-help**

  When you run the -help argument, ipm displays a list of all supported commands and a one-line description of the command.

- **-v**

  When you run the -v argument, ipm displays the ipm CLI version.

Function-dependent Arguments

You can use the following arguments only with commands:

- **-p password**

  Specifies the password for the LMS username.

  **Warning** If -p password is not used, the password is read from the command ipm CW CLIFILE. This is highly insecure and *not* recommended. See -u argument for more details. For more information, see Setting CWCLIFILE Environment Variable.

- **-m mailbox**

  Mails the results of the ipm command to the specified e-mail address.
Function-specific Arguments

You can use the following arguments only with specific commands:

- `-coll`—Used with `stop`, `start`, `delete`, `controlcollector` functions.
- `-start`—Used with `controlcollector` function.
- `-end`—Used with `exportstats` function.

Example 1

```
ipm controlcollector -u userid -p password -start -coll collector name
```

Use the above command to start the stopped collectors.

Example 2

```
ipm exportstats -u userid -p password [-m email] [-delimiter delimiter] [-coll
collectorname] {-start starttime} {-end endtime} {-granularity d|w|m|h|min}{-reportType
a|l|h|i|p|r|e|v}
```

Use the above command to export collectors.

- `delimiter`—Separates the fields in the exported file. By default, `,'` is used as a delimiter, where
the exported file is in .xls format.
- `coll`—Specify the name of the collectors separated by comma.
- `start`—Specify the Start Time of your report.
- `end`—Specify the End Time of your report.
- `granularity`—Specify the granularity for the report. The granularity available are
  - `min`-Minute,
  - `h`-Hourly,
  - `d`-Daily,
  - `w`-Weekly, and
  - `m`-Monthly.
- `reportType`—Specify the report type. The report types available are
  - `a`-Availability,
  - `l`-Latency,
  - `j`-Jitter,
  - `h`-HTTP,
  - `i`-ICMP,
  - `p`-PathEcho,
  - `r`-RTP,
  - `e`-EthernetJitter, and
  - `v`-Video.

Input List File Format

You can create Input List File Format for entering a list of arguments and its parameters.

The contents of the input list file are a sequence of lines. Each line specifies command arguments and
the input parameters. The arguments must be specific to the function. You can include comments in the
input list file by starting the each commented line with `#`.

In LMS, you can use input list file format in the following commands:

- `ipm export`
- `ipm exportstats`
- `ipm deletedevice`
- `ipm controlcollector`
- `ipm addadhoctarget`
- `ipm importcollector`
- `ipm enableipslacollector`
Syntax for command using Input File System

```
ipm addadhoctarget -u userid -p password -input file
input file—Contains [-m email] [-device deviceip | hostname] information.
```

**Note**

In the above syntax, ensure that the hostname you provide is DNS resolvable from the LMS server. If the hostname is not DNS resolvable, the command may fail.

Example for command using Input File System

```
ipm addadhoctarget -u admin -p admin -input C:/filename.csv
```

where `C:/filename.csv` contains:

```
-device testdevice1, testdevice2, 10.77.200.200
```

<ipm> INFO - Done with the execution of the command.
Successful: ipm addadhoctarget
This result occurs when the adhoc devices mentioned in the input file are successfully added.

**IPSLA Monitoring CLI Commands**

The section describes the command line interface (CLI) commands that you use for IPSLA Monitoring.

- Viewing IPSLA Monitoring CLI Help
- Managing Collectors
- Listing Collectors
- Importing Collectors
- Exporting Collector Components and Collector Statistics
- Managing System Reports
- Adding Adhoc Devices
- Deleting Devices
- Baseline
- Viewing IPSLA Monitoring CLI Version
- Enabling IPSLA Responder

**Viewing IPSLA Monitoring CLI Help**

This section explains how to view all the IPSLA Monitoring CLI commands and view help for a specific command. It also explains how to list the commands and subcommands for LMS.

```
ipm -help
ipm <command> -help
ipm ?
```

`Command`

```
ipm -help
```
Use this command to view all the IPSLA Monitoring CLI commands.

**Syntax Description**

```plaintext
ipm -help
```

`help`—Allows you to view the list of all IPSLA Monitoring supported CLI commands.
**IPSLA Monitoring CLI Commands**

**Command**

```plaintext
ipm command -help
```

Use this command to view help for a specific command.

**Syntax Description**

```plaintext
ipm command -help
```

*help*—Allows you to view the help for the command you have specified.

*command*—Specify the command.

**Example**

```plaintext
ipm controlcollector -help
```

- **controlcollector**: To stop or start or delete for given collector.

**Usage**

```plaintext
ipm controlcollector -u userid -p password [-m email] 
{-start | -stop | -delete} {-coll collectorname} [-input argumentFile]
```

- **-u**: specifies the CiscoWorks user name
- **-p**: specifies the password for the CiscoWorks user name
- **-m**: specifies an email address to send the results
- **-start**: To start collector
- **-stop**: To stop collector
- **-delete**: To delete collector
- **-coll**: Collector names
- **-input**: text file containing arguments to the command

**Command**

```plaintext
ipm ?
```

Use this command to list the commands and subcommands for IPSLA Monitoring.

**Note**

You cannot use this command for Solaris or Soft Appliance as it does not accept wildcard characters (*?).

**Syntax Description**

```plaintext
ipm ?
```

*?*—Lists the commands and subcommands for IPSLA Monitoring.

**Example 1**

```plaintext
ipm ?
```

- **addadhoctarget**
- **baseline**
- **controlcollector**
- **deletedevice**
- **deletereports**
- **export**
- **exportstats**
- **generatereports**
- **help**
- importcollector
- listcollectors
- enableipslaresponder

This result occurs when there are commands and subcommands for IPSLA Monitoring.

Example 2

ipm baseline ?
<iipm> - No valid commands or sub-commands found.

This results when there are no commands and subcommands for IPSLA Monitoring baseline.
Managing Collectors

Use the following command to start, stop, or delete collectors.

Ethernet Jitter and Ethernet Ping collectors created by an Auto IP SLA collector cannot be started, stopped, or deleted individually. You need to start, stop, or delete the Auto IP SLA group collector to automatically start, stop, or delete its Ethernet Jitter and Ethernet Ping collectors.

Command

ipm controlcollector

Syntax Description

ipm controlcollector -u userid -p password [-m email] [-start | -stop | -delete] [-coll collectorname] | [-coll all -deleteAllInSource] [-input argumentFile]

- start— Starts the stopped collectors.
- stop— Stops the collectors in Running status.
- delete— Deletes the collectors in Stopped status.
- coll— Specify the collector name.
- deleteAllInSource— Deletes all collectors from all the source in LMS.
- input— Text file that contains arguments for the command.

• Stopping Collectors

ipm controlcollector -u admin -p admin -stop -coll Coll4_Default_IPECHO

<ipm> INFO - Done with the execution of the command.
Successful: ipm controlcollector

This result occurs when the collector is stopped successfully.

• Starting Collectors

ipm controlcollector -u admin -p admin -start -coll findpath_10.77.203.159_DefaultIpPathEcho

<ipm> INFO - Done with the execution of the command.
Successful: ipm controlcollector

This result occurs when the collector is started successfully.

• Deleting Collectors

ipm controlcollector -u admin -p admin -delete -coll findpath_10.77.203.159_DefaultIpPathEcho

INFO - Done with the execution of the command.
Successful: ipm controlcollector

This result occurs when the collector is deleted successfully.

• Deleting all Collectors from all the source in LMS

ipm controlcollector -u admin -p admin -coll all -deleteAllInSource

Successful: ipm controlcollector: - Deletion of all probes in source devices.
Listing Collectors

Use the following command to list the collectors.

Command
ipm listcollectors

Syntax Description
ipm listcollectors -u userid -p password

Example
ipm listcollectors -u admin -p admin
<ipm> INFO - Done with the execution of the command.
This result occurs when the collectors are listed successfully.

Importing Collectors

Use the following command to import collectors for IPSLA Monitoring functionality.

Command
ipm importcollector

Syntax Description
ipm importcollector -u userid -p password {-m email} {-file filename} {-source (sourceDisplayNames|All)} {-oper (operationRttTypeName|All)} [-input argumentFile]

- u—Specifies the LMS user name.
- p—Specifies the password for the LMS user name.
- m—Specifies an email address to send the results.
- file—Contains the details of the collector to be imported.
- source—Specifies one or more source display names separated by comma.
- oper—Specifies one or more operation names of RttType separated by comma.
- input—Text file that contains arguments for the command.

Note
If you import a collector using file, only the Auto IP SLA collector is imported and not its individual Ethernet Jitter and Ethernet Ping collectors.

Example
ipm importcollector -u admin -p admin -file
'/var/adm/CSCOpx/files/ipm/export/collection_Fri_Jan_05_21:31:08_IST_2007.csv'
Successful: ipm importcollector: Successfully imported the collectors.
This result occurs when the collector is imported successfully.
File format for Importing a collector using File option

Note
The lines starting with ; (semicolon) are considered as comments and the examples given below are the information about each column.

;  Here are the columns of the file.
;  Columns 1, 3, 5, 6, 9-14 are required.
;  Columns 2, 7, 8 are optional.
;  Column 4 is not applicable for DHCP, GatekeeperRegistrationDelay,
;  CallSetupPostDialDelay, EthernetPingAutoIPSLA, EthernetJitterAutoIPSLA
;  Operation types and should be left empty.
;  For the Operations Ethernetjitter, Ethernetping represents MEPID.
;  Col# = 1: Collector Name
;  Col# = 2: Description of the collector
;  Col# = 3: Source display name
;  Col# = 4: Target display name
;  Col# = 5: Operation name
;  Col# = 6: Operation Type [1 - Echo, 2 - PathEcho, 9 - UDP Jitter, 22 - Video]
;  Col# = 7: Vrf Name
;  Col# = 8: Source Interface Address
;  Col# = 9: Collector type [1 - Historical, 2 - Realtime]
;  Col# = 10: Start date (must be in MM/DD/YYYY)
;  Col# = 11: End date (must be in MM/DD/YYYY)
;  Col# = 12: Poll Start time (hh:mm:ss)
;  Col# = 13: Poll End time (hh:mm:ss)
;  Col# = 14: Days of week (must be between 1-127)
;  Col# = 15: Poll Interval (must be in milliseconds)

;  Example for Echo Collector:

; test_Echo_Collector, ,1.7.20.9,1.7.9.106-NAM2,Test_Echo_Operation,1,blue,
; ,1,07/29/2008,01/31/2021,00:00:00,00:00:00,127,3600000

;  Example for DHCP Collector:

; test_DHCP_collector, ,1.7.20.9, ,Test_DHCP_Operation,11, ,
; ,1,07/29/2008,01/31/2021,00:00:00,00:00:00,127,3600000

; Here are the rows of data.

; test_Echo_Collector, ,1.7.20.9,1.7.9.106-NAM2,Test_Echo_Operation,1,blue,
; ,1,07/29/2008,01/31/2021,00:00:00,00:00:00,127,3600000

test_DHCP_collector, ,1.7.20.9, ,Test_DHCP_Operation,11, ,
,1,07/29/2008,01/31/2021,00:00:00,00:00:00,127,3600000

If you exceed the license limit, the imported collectors are considered as real-time collectors and not as historical collectors. This applies only to collectors imported from a device and not file.
Importing a collector from the source device

To import all collectors from the source devices 1.1.1.1 and 2.2.2.2 of the Operation type Echo use the following command:

```
ipm importcollector -u userid -p password -source 1.1.1.1,2.2.2.2 -oper Echo
```

This will import all the collectors from the source devices 1.1.1.1 and 2.2.2.2 of the Operation type Echo.

To import all the below given operation types, use the following command:

```
ipm importcollector -u userid -p password -source 1.1.1.1,2.2.2.2 -oper All
```

You can use any of the following operation name as input to -oper

- Echo — To Import Echo Operations
- PathEcho— To Import PathEcho Operations
- UDPEcho— To Import UDPEcho Operations
- TCPConnect— To Import TCPConnect Operations
- UDPJitter— To Import UDPJitter Operations
- DLSW— To Import DLSW Operations
- DHCP— To Import DHCP Operations
- FTP — To Import FTP Operations
- VOIP— To Import GatekeeperRegistrationDelay and CallSetupPostDialDelay Operations
- RTP— To Import RTP Operations
- ICMPJitter— To Import ICMPJitter Operations
- EthernetPing— To Import EthernetPing Operations
- EthernetPingAutoIPSLA— To Import EthernetPingAutoIPSLA Operations
- EthernetJitter— To Import EthernetJitter Operations
- EthernetJitterAutoIPSLA— To Import EthernetJitterAutoIPSLA Operations
- HTTP— To Import HTTP Operations
- DNS— To Import DNS Operations
- Video—To Import Video Operations

For example, find below a sample report:

- Total Number of Collectors Imported: 24
- Total Number of Collectors Not Imported: 3
- Total Number of Collectors Filtered: 1
- Total Number of New Adhoc devices (Target) added: 15

Table 18-1 lists the sample report details.
Note

If you exceed the license limit, the imported collectors are considered as real-time collectors and
not as historical collectors. This applies only to collectors imported from a device and not file.

Exporting Collector Components and Collector Statistics

This section explains how to export collector components and collector statistics using CLI commands.

- Exporting Collector Components
- Exporting Collector Statistics

Exporting Collector Components

Use the following command to export IPSLA collectors, target devices, source devices, or operations to
a CSV file. They are exported in the .xls format by default.

The exported file is stored at the following location:

- Solaris or Soft Appliance
  - /var/adm/CSCOpx/files/ipm/export/collectors
  - /var/adm/CSCOpx/files/ipm/export/source
  - /var/adm/CSCOpx/files/ipm/export/target
  - /var/adm/CSCOpx/files/ipm/export/operations

- Windows
  - <NMSROOT>/CSCOpx/files/ipm/export/collectors
  - <NMSROOT>/CSCOpx/files/ipm/export/source
  - <NMSROOT>/CSCOpx/files/ipm/export/target
  - <NMSROOT>/CSCOpx/files/ipm/export/operations

Command

ipm export

Syntax Description

```
ipm export -u userid -p password [-m email] [-delimiter delimiter] [-file filename] [-coll (collectorname|all)] [-source (sourceDisplayNames|all)] [-target (targetDisplayName|all)] [-oper (operationNames|all)] [-input argumentFile]
```
- **delimiter**—Separates the fields in the exported file. By default, ',' is used as delimiter, where the exported file is in .xls format.
- **coll**—Specify the name of the collectors separated by comma. To export all collectors, specify *all*.
- **source**—Specify the source devices display name separated by comma.
- **target**—Specify the target devices display name separated by comma.
- **oper**—Specify the operation names separated by comma.
- **file**—Specify a filename to export the data. This option is not applicable for exporting operations.
- **input**—Text file that contains arguments for the command.

It is mandatory to specify at least one value for arguments collector, source, target, or operation.

**Note**

To export all collectors, source devices, target devices, and operations, give *all* as the input for the argument. Example: To export all the source devices, give [**-source (all)**]

### Examples for Exporting Collectors

This section consists of examples.

**Example 1: Exporting Collectors**

```
ipm export -u admin -p admin -coll C3_DHCP
```

Successful: `ipm export: /var/adm/CSCOpx/files/ipm/export/collectors/collector_Fri_Jan_05_21:31:08_IST_2007.csv is exported successfully`

This result occurs when the collectors are exported successfully.

**Note**

If you export a collector by file, only the Auto IP SLA collector is exported and not its individual Ethernet Jitter and Ethernet Ping collectors.

**Example 2: Exporting Target Devices**

```
ipm export -u admin -p admin -target 10.77.203.87
```

Successful: `ipm export: /var/adm/CSCOpx/files/ipm/export/target/target_Fri_Jan_05_21:33:42_IST_2007.csv is exported successfully`

This result occurs when the target devices are exported successfully.

**Example 3: Exporting Source Devices**

```
ipm export -u admin -p admin -source 10.77.203.87
```

Successful: `ipm export: /var/adm/CSCOpx/files/ipm/export/source/source_Fri_Jan_05_21:33:42_IST_2007.csv is exported successfully`

This result occurs when the source device is exported successfully.
Example 4: Exporting Operations

ipm export -u admin -p admin -operation DefaultSMTP

Successful: ipm export:
/var/adm/CSCOpx/files/ipm/export/source/source_Fri_Jan_05_21:33:42_IST_2007.csv is exported successfully

This result occurs when the operations are exported successfully.

Example 5: Exporting Collectors in .txt format

ipm export -u admin -p admin -coll C3_DHCP -delimiter '~'

Successful: ipm export:
/var/adm/CSCOpx/files/ipm/export/collectors/collector_Fri_Jan_05_21:31:49_IST_2007.txt is exported successfully

This result occurs when the collectors is exported successfully.
Exporting Collector Statistics

Use the following command to export collector statistics to a CSV file. The exported file is in .xls format by default. If you want the exported file in .txt format specify the delimiter. Example: ‘~’.

The exported file is stored at the following location:
- Solaris or Soft Appliance: /var/adm/CSCOpx/files/ipm/export/statistics
- Windows: C:/Program Files/CSCOpx/files/ipm/export/statistics

Command
```
ipm exportstats
```

Syntax Description
```
```

- **delimiter**—Separates the fields in the exported file. By default, ‘,’ is used as delimiter, where the exported file is in .xls format.
- **coll**—Specify the name of the collectors separated by comma.
- **start**—Specify the Start Time of your report in this yyyy-mm-dd format.
- **end**—Specify the End Time of your report in this yyyy-mm-dd format.

**Note**
For more accurate report details, give the start and end in “yyyy-mm-dd hh:mm:ss” and “yyyy-mm-dd hh:mm:ss” format.

- **granularity**—Specify the granularity for the report. The granularity available are min-Minute, h-Hourly, d-Daily, w-Weekly, and m-Monthly.
- **reportType**—Specify the report type. The report types available are a-Availability, l-Latency, j-Jitter, h-HTTP, i-ICMP, p-PathEcho, r-RTP, e-EthernetJitter, and v-Video.
- **input**—Text file that contains arguments for the command.
- **excludeOutage**—Exclude statistic information on outage period.

Example 1
```
ipm exportstats -u admin -p admin -m user@domain.com -coll C3_DHCP -start “2006-12-29 01:47:37.000” -end “2006-12-30 01:47:37.000” -granularity h -reportType a
```
Successful: ipm exportstats:

This result occurs when the collector statistics are successfully exported.

Example 2
```
ipm exportstats -u admin -p admin -m user@domain.com -coll C3_DHCP -start “2006-12-29 01:47:37.000” -end “2006-12-30 01:47:37.000” -granularity h -reportType a -excludeOutage.
```
This will exclude the outage period data.
Managing System Reports

This section explains how to manage the system reports using CLI commands.

- Generating System Reports
- Deleting System Reports

Generating System Reports

Use the following command to generate the system reports for all report types and all granularities.

**Command**

```
ipm generatereports
```

**Syntax Description**

```
ipm generatereports -u userid -p password
```

**Example**

```
ipm generatereports -u admin -p admin
```

Successful: ipm generatereports: Successfully generated reports.

This result occurs when the system reports are generated successfully.

Deleting System Reports

Use the following command to delete the system reports.

**Command**

```
ipm deletereports
```

**Syntax Description**

```
ipm deletereports -u userid -p password {-noofdays no_of_days} [-input argumentFile]
```

- `noofdays`—Specify the number of days for which you want to save the report.
- `input`—Text file that contains arguments for the command.

**Example**

```
ipm deletereports -u admin -p admin - noofdays 4
```

Successful: ipm deletereports: Successfully deleted reports.

This result occurs when the system reports are deleted successfully.
Adding Adhoc Devices

Use the following command to add external target devices for IPSLA Monitoring.

Command

ipm addadhoctarget

Syntax Description

ipm addadhoctarget -u userid -p password [-m email] {-device deviceip | hostname} [-input argumentFile]

device—Specify the display name or IP address of the device.
input—Text file that contains arguments for the command.

Example 1

ipm addadhoctarget -u admin -p admin -device abc
<ipm> INFO - Done with the execution of the command.
Successful: ipm addadhoctarget
This result occurs when the adhoc device is successfully added.

Example 2

ipm addadhoctarget -u admin -p admin -device abcd
The following target(s) already exist abcd
<ipm> INFO - Done with the execution of the command.
This result occurs when you try to add an existing adhoc target device.

Example 3

ipm addadhoctarget -u admin -p admin -input C:/filename.csv
where C:/filename.csv contains:
-device testdevice1, testdevice2, 10.77.200.200

<ipm> INFO - Done with the execution of the command.
Successful: ipm addadhoctarget
This result occurs when the adhoc devices mentioned in the input file are successfully added.

Deleting Devices

Use the following command to delete the devices from IPSLA Monitoring.

Command

ipm deletedevice

Syntax Description

ipm deletedevice -u userid -p password [-m email] {-device displayname} [-input argumentFile]
device—Specify the display name of the device.
input—Text file that contains arguments for the command.

Example 1
ipm deletedevice -u admin -p admin -device 255.255.255.255
<i>ipm> INFO - Done with the execution of the command.
This result occurs when the device is successfully deleted.

Example 2
ipm deletedevice -u admin -p admin -device abc
<i>ipm> ERROR - Device abc does not exist
This result occurs when you are not able to delete the device.

Baseline

Use the following command to modify the default Rising Threshold value for all collectors that is associated with the specified operation.

For example, if the current average latency is 100 milliseconds and you specify a baseline of 50, the new rising threshold is 150 milliseconds (50% above the current average latency), and the falling threshold is 50 ms (50% below the current average latency).

Command
ipm baseline

Syntax Description
ipm baseline -u userid -p password [-m email] [-percentage value] [-input argumentFile]
percentage—Allows you to modify the Rising Threshold value.
input—Text file that contains arguments for the command.

Example
ipm baseline -u admin -p admin -percentage 90
<i>ipm> INFO - Baseline value updated successfully
<i>ipm> INFO - Done with the execution of the command.
This result occurs when the Rising Threshold value is updated successfully.

Viewing IPSLA Monitoring CLI Version

Use the following command to view the ipm command line framework interface version.

Command
ipm -v

Syntax Description
ipm -v
v—Allows you to view the ipm CLI version details
Enabling IPSLA Responder

Use the following command to enable the IPSLA responder for the selected devices.

Command

ipm enableipslaresponder
This chapter provides you the following information for Cisco Prime LMS:

- Frequently Asked Questions
- Troubleshooting LMS

Frequently Asked Questions

This sections contains the Frequently Asked Questions (FAQs) for the following modules:

- Performance Management
- NetShow
- Fault Management
- General
- IPSLA Devices
- Operations
- Collectors
- CLI Commands
- IPSLA Monitoring
- Device Management
- VRF-Lite

Performance Management

This section lists the frequently asked questions about LMS Performance Management.

- How many MIB objects can LMS monitor?
- What polling intervals does LMS support?
- What MIBs does LMS uses to query the device?
- What parameters can LMS monitor in a device?
- How can I stop a Poller from polling the devices?
• Can I create my own custom templates and poll the devices using it?
• What does Transient and Permanent failures mean?
• What are Missed Cycles?
• Can I export a template from LMS to a directory location?
• Can I use an external MIB file in LMS?
• How can I create a threshold for a MIB variable?
• Can I receive alerts or notifications when a threshold rule is violated?
• Can I view the complete details of a device from a single report?
• Can I configure LMS to send the PDF format of reports as an E-mail?
• Can I configure LMS to publish PDF format of reports to a directory location?
• Can I set log levels for individual application modules? Where are these log files stored?
• Can I change the frequency of Quick Report generation?
• Can I enable or disable any quick report?
• Can I generate a report in LMS to view the last 24 hour data? If so, which report should I choose?
• Can I compare two MIB variables in LMS?
• Can I generate a report based on templates added in a given Poller?
• Can I generate a report in LMS based on MIB variables added in a Poller?
• Can I configure the SNMP Poll Settings in LMS?
• What type of SNMP support does LMS provide?
• Why is the Report Job failing when I select the Add Full Report option?
• Why are my Report Jobs taking longer time to run?
• Why am I not able to load a new MIB file into LMS?
• What type of notifications are supported in LMS in case of violations?
• Can I do capacity planning with the help of LMS?
• Why is the data purge job taking a long time to complete?

Q. What polling intervals does LMS support?
A. The following polling intervals are supported in LMS: 1 minute, 5 minutes, 15 minutes, 30 minutes, 60 minutes, 120 minutes, 240 minutes, and 480 minutes.

Q. How many MIB objects can LMS monitor?
A. Cisco Prime LMS can monitor up to 100,000 MIB objects. LMS can monitor 40,000 MIB objects for one minute polling and 100,000 MIB objects for five minutes polling.
Q. What MIBs does LMS uses to query the device?
A. LMS supports the following Cisco MIBs, by default:
   - CISCO-ENHANCED-MEMPOOL-MIB
   - CISCO-ENVMON-MIB
   - CISCO-MEMORY-POOL-MIB
   - CISCO-PROCESS-MIB
   - ENTITY-MIB
   - OLD-CISCO-CHASSIS-MIB
   - RFC1213-MIB
   - IF-MIB
   - CISCO-POWER-ETHERNET-EXT-MIB
   - POWER-ETHERNET-MIB
   - CISCO-RTMON-MIB
   
   However, you can also compile and use other MIB files into LMS that support Cisco devices. See Load MIB files in Administration of Cisco Prime LMS 4.1 User Guide.

Q. What parameters can LMS monitor in a device?
A. LMS can monitor the CPU utilization, memory utilization, interface utilization, interface availability, device availability, interface error rate and environmental temperature in a device using System-defined templates.

Q. How can I stop a Poller from polling the devices?
A. You can use the Deactivate feature in the Poller Management page to stop a Poller from polling the devices. In this case, the license count on the number of devices to poll is not reduced when you deactivate a Poller.

Q. Can I create my own custom templates and poll the devices using it?
A. Yes. LMS allows you to create user-defined templates by leveraging MIB variables from an existing System-defined template, or by grouping MIB variables from a compiled MIB file. You can use the templates to poll all Cisco devices that support the specific MIB.

Q. What does Transient and Permanent failures mean?
A. Transient is a failure status displayed if the device is down, the SNMP credentials are incorrect, or the SNMP request times out. Permanent is a failure status displayed if the polled MIB variables or instances are not available.

Q. What are Missed Cycles?
A. Missed Cycle occurs if a Poller takes more than the required time to complete polling and miss the scheduled polling cycle.

For instance, if the Polling Interval for a Poller is set as 15 minutes and the first polling cycle starts at 10:00 a.m., the next polling cycle is scheduled to start at 10:15 a.m.

If the polling cycle that started at 10:00 a.m. does not complete before 10:15 a.m., then the next polling cycle will start only at 10:30 a.m. The polling cycle missed at 10:15 is called Missed Cycle.
Q. Can I export a template from LMS to a directory location?
A. Yes. You can export a template to a directory location where the LMS application is installed. The exported file is in XML format. You can export both System-defined templates and User-defined templates.

Q. Can I use an external MIB file in LMS?
A. Yes. You can use the Load MIB option in LMS to load an external MIB file. LMS compiles this new MIB file. You can use the new MIB file to create user-defined templates.

Q. How can I create a threshold for a MIB variable?
A. Threshold is an optimal value set for a MIB variable by the user or the system. You can create and set threshold rules for all devices that are selected for polling.

Threshold rules are set for one MIB variable at a time and you can set many thresholds for each MIB variable.

Q. Can I receive alerts or notifications when a threshold rule is violated?
A. Yes. LMS supports triggering of user-specified external commands or scripts against threshold violations. It also provides E-mail, Traps or Syslog notifications when a threshold rule is violated.

Q. Can I view the complete details of a device from a single report?
A. Yes. Device Dashboard report displays the complete details of the device polled using the System-defined and user-defined templates.

Q. Can I configure LMS to send the PDF format of reports as an E-mail?
A. Yes. You can configure LMS to send the PDF format of the report as an E-mail attachment.

You need to enable the E-mail Attachment checkbox and specify the Maximum Attachment size in the System Preferences dialog box (Admin > System > System Preferences) to send the PDF as an E-mail.

If the PDF file size exceeds the Maximum Attachment size, the URL link of the report is sent as an e-mail. You can click the URL link to view the report.

Q. Can I configure LMS to publish PDF format of reports to a directory location?
A. Yes. You can configure a default report publish path to which PDF format of the reports are published.

Q. Can I set log levels for individual application modules? Where are these log files stored?
A. Yes. You can set log levels for all LMS modules. Log files are stored at these locations:

- On Windows: \NMSROOT\log, where \NMSROOT is the LMS installation directory.
- On Solaris or Soft Appliance: /var/adm/CSCOpx/log/

Report specific logs are stored under LMSReportJobs under the log directory.

Q. Can I change the frequency of Quick Report generation?
A. Yes. You can change the frequency and the time of generating Quick Reports from Reports > Report Job Browser > Quick Report Schedule. By default, Quick Reports are generated every hour.
Q. Can I enable or disable any quick report?
A. User Configurable Quick Reports allows you to enable or disable generating any Quick Report and also to change the frequency of report generation. By default, reports are generated every hour and all Quick Reports are enabled.

Q. Can I generate a report in LMS to view the last 24 hour data? If so, which report should I choose?
A. Yes. You can use the Quick Reports option in LMS to view the reports on the data of the last 24 hours.

Q. Can I compare two MIB variables in LMS?
A. Yes. LMS allows you to compare the historical trending of two MIB variables in the form of overlay graphs in Quick Reports. Reports that support overlay graph are Interface Error report, Interface Utilization report, and PoE Port Utilization report.

Q. Can I generate a report based on templates added in a given Poller?
A. Yes. You can use the Poller Reports option to generate reports based on templates added in a given Poller.

Q. Can I generate a report in LMS based on MIB variables added in a Poller?
A. Yes. You can use the Custom Reports option to generate reports on MIB variables added in a Poller.

Q. Can I configure the SNMP Poll Settings in LMS?
A. Yes. LMS allows you to configure polling settings using the Poll Settings option. You can configure the SNMP time-out and SNMP retries based on the device and the network response time.

Q. What type of SNMP support does LMS provide?
A. LMS supports SNMP v1, SNMP v2 and SNMP v3 (authPriv, authNoPriv and noAuthNoPriv modes). The support of SNMP is decided based on the SNMP credentials configured in the DCR. The choice of using SNMP v3/v2/v1 is decided during instance query.

The support of SNMP v3 authPriv mode is available from LMS 3.0.1.

Q. Why is the Report Job failing when I select the Add Full Report option?
A. If you have selected large number of instances to create a full report (includes graphs), the job might fail because of insufficient memory. You can reduce the number of instances and then try creating the report.

Q. Why are my Report Jobs taking longer time to run?
A. If you have added large number of instances and have also selected the Add Full Report option, the report job will generate graphs for each of the selected instances, which will take long time to generate the report. Either you must reduce the number of instances selected or disable the Add Full Report option.

Q. Why am I not able to load a new MIB file into LMS?
A. Either you have tried to load an invalid or corrupted MIB file, or the dependent MIB files are not available in the directory path. Before you load a MIB file, you need to ensure that the MIB file is valid and all the dependent MIB files are available in the same directory path. To view the list of dependent MIB files go to: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2
Q. What type of notifications are supported in LMS in case of violations?
A. LMS supports E-mails, Traps and Syslog notifications in case there are any Threshold or TrendWatch violations.

Q. Can I do capacity planning with the help of LMS?
A. The TrendWatch feature in LMS ensures that the capacity, performance or utilization of critical resources remains within the defined service level. It also helps in capacity planning. You can configure TrendWatches through LMS by setting up rules for each MIB variable or on thresholds, for a specific time period. You can schedule TrendWatches (Immediate, Once, Daily, Weekly, or Monthly) as jobs and you can configure them to send notifications through e-mail, traps and Syslogs.

Q. Why is the data purge job taking a long time to complete?
A. If the LMS view in LMS Portal is opened and the data purge job is running in parallel, then the data purge job will take longer time to complete. This is because the portlets in the LMS Portal page gets refreshed at frequent intervals which uses a lot of memory. It is recommended to close the LMS view in LMS Portal when data purge job is running.

NetShow

This section provides the FAQs and troubleshooting information for the NetShow application:

- How can I add an adhoc command to only one particular device category in a command set?
- How do I mask the credentials shown in NetShow job output?
- Why am I not able to delete some adhoc commands?
- What are the valid adhoc commands that I can enter?
- Why are the system-defined command sets not displayed in the assign command sets flow?
- What do I enter in the custom commands field during job creation?
- Why are the system-defined commands inside a command set, not shown based on device category?
- How do I view the consolidated output of all the devices and the commands executed on these devices?
- What is Output Archive?
- When is the output of a command archived?
- When I delete a job, does the corresponding archive also get deleted?
- In the Output Archive page, what does Success = and Fail = under the heading Status mean?
- Why do devices show Fail status in NetShow jobs?

Q. How can I add an adhoc command to only one particular device category in a command set?
A. You need to choose that particular device category while creating the command and enter the adhoc command.
Q. How do I mask the credentials shown in NetShow job output?
A. You need to update the properties file

```
NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nmrmeng\config\netshow\NSCredCmds.properties file
```

with the command for which the credentials are displayed.

We recommend that you enter the complete command in the file. For example, you must enter `show running-config`, not `show run`.

Q. Why am I not able to delete some adhoc commands?
A. You can delete adhoc commands only if they are not part of any command set. So in the Edit flow, you need to remove the command from the selected commands list and click Finish. Then you can edit the command set again and try deleting the adhoc command.

Q. What are the valid adhoc commands that I can enter?
A. `show`, `version`, `where`, `ping`, `traceroute`, and `?`. You can use the short forms of these commands. For example you can use `sh` for `show`.

Q. Why are the system-defined command sets not displayed in the assign command sets flow?
A. System-defined command sets are by default assigned to all. Since the system-defined command sets are already assigned to all users, they will not appear in the assign command sets flow.

Q. What do I enter in the custom commands field during job creation?
A. Enter the adhoc commands. These adhoc commands are downloaded on all devices even if a particular device does not support the command.

Q. Why are the system-defined commands inside a command set, not shown based on device category?
A. The system-defined commands do not map to a particular device category inside a command set. When you run a job, these commands will be downloaded on all applicable devices.

Q. How do I view the consolidated output of all the devices and the commands executed on these devices?
A. You can view the output of all the commands for all the devices by clicking the Print button on the top right hand corner of the NetShow Job Details page.

Q. What is Output Archive?
A. The Output Archive feature in NetShow helps you archive and access the stored output that is created from a NetShow job. The Output Archive will not display the Job Summary and Work Order details.

Q. When is the output of a command archived?
A. The command output is archived only if the job was executed completely. Cancelled jobs are not archived.

Q. When I delete a job, does the corresponding archive also get deleted?
A. No. If you want to delete an archive, you can do so from the Output Archive page.
**Frequently Asked Questions**

**Q.** In the Output Archive page, what does *Success* = and *Fail* = under the heading *Status* mean?

**A.** It indicates the number of devices on which a particular command execution was successful and the number of devices on which it failed.

**Q.** Why do devices show *Fail* status in NetShow jobs?

**A.** A device will show *Fail* status if it is unreachable or if a single command execution fails.

**Fault Management**

The following section lists the frequently asked questions about Fault Management:

- What are the OIDs polled by Fault Management for card status?
- Where can I find the log and rps files of Incharge/Smarts?
- Why are devices with SysObjID 1.3.6.1.4.1.311.1.1.3.1.2 or 1.3.6.1.4.1.311.1.1.3.1.3 not managed by Fault Management?
- Why does Fault Management display false Card Down events?
- How can I collect Mibwalk for a device?
- Can I have HPOV/Netview installed in one drive, for example C: and DFM HPOV/Netview Adapters in another drive, D:?
- In the Search Results, the selected devices are not displayed as selected. They are displayed as selected only in All Devices group. Why?
- How can I avoid Fault Management generating Unresponsive alerts when the devices are in Natted Environment?
- How can I get rid of alerts for a device that has been deleted?
- Why HighUtilization on interface gets generated by Fault Management?
- Why does a device go into Unsupported state although it is Supported?
- What is the difference between Snmp Raw Trap Forwarding and Processed Snmp Trap alert/event Trap Forwarding? Does Fault Management support both of these methods?
- How does Fault Management detect Trunk and Access ports?
- What is the meaning of different discovery percentages?
- How can I troubleshoot device discovery stuck at 10%?
- How can I troubleshoot device discovery stuck at 40%?
- How can I troubleshoot device discovery stuck at 90%?
- How can I stop nGenius RealTimeMonitoring in Solaris or Soft Appliance?
- How can I perform rediscovery of devices in LMS through CLI?
- How can I manage or unmanage ports and interfaces from CLI?
- How can I import devices into DCR through CLI?
- How can I enable CAM logs for debugging ACS Configuration?
- How can I create a link to the Java Plug-in in Mozilla?
- How does LMS react to a Cisco ISR with Inline POE switch module when there is no -48V power supply installed?
Chapter 19  Troubleshooting and FAQs in LMS Monitoring and Troubleshooting

Frequently Asked Questions

- What happens when VG200 Routers have an ISDN PRI carrying voice traffic?
- I am unable to sort Cleared Alerts in LMS. Why?

Q. What are the OIDs polled by Fault Management for card status?
A. The following OIDs are polled to monitor the cards:
  - In EntityFRU:
    - 1.3.6.1.4.1.9.9.117.1.2.1.1.1
    - 1.3.6.1.4.1.9.9.117.1.2.1.1.2
  - In OLD-CISCO-CHASSIS-MIB: 1.3.6.1.4.1.9.3.6.11.1.9.0
  - In CISCO-STACK-MIB: 1.3.6.1.4.1.9.5.1.3.1.1.10

Q. Where can I find the log and rps files of Incharge/Smarts?
A. The log and rps files of Incharge/Smarts can be found at the following locations:
  - log files: NMSROOT/objects/smarts/local/logs
  - rps files: NMSROOT/objects/smarts/local/repos/icf
  - broker.rps files: \CSCOpx\objects\smarts\local\repos\broker

You need to send all these files for debugging if there is a problem with Incharge.

Q. Why are devices with SysObjID 1.3.6.1.4.1.311.1.1.3.1.2 or .1.3.6.1.4.1.311.1.1.3.1.3 not managed by Fault Management?
A. Devices with SysObjID 1.3.6.1.4.1.311.1.1.3.1.2 or .1.3.6.1.4.1.311.1.1.3.1.3 on Windows 2000 are not discovered by Fault Management. This could be because CDP MIB does not respond on the devices. For a device to be managed by Fault Management, it should respond to CDP MIB.

Q. Why does Fault Management display false Card Down events?
A. For all ARTG routers that can hold VWIC2-xMFT cards, you may see Card Down events. There is a bug (CSCsj58422) on the agent side. You may need to upgrade to the latest IOS Version to resolve this problem. Please refer to the case ID 607434565 and 607553227 for more details.
Q. How can I collect Mibwalk for a device?
A. To collect the Mibwalk for a device, do the following:

**Step 1**
Go to `NMSROOT/objects/smarts/bin`.

**Step 2**
Enter the following command for:

- **Snmp v1 and snmp v2 devices:**
  - For Solaris or Soft Appliance: `./sm_snmpwalk --community= deviceIp`
    
    For eg: `./sm_snmpwalk --community=cisco 4.1.1.1`
  
  - For Windows: `sm_snmpwalk --community= deviceIp`
    
    For eg: `sm_snmpwalk --community=cisco 4.1.1.1`

- **Snmp v3 devices:**
  - For Solaris or Soft Appliance: `./sm_snmpwalk --snmp=3 --user=desuser --auth=MD5 --authPass=changeme --priv=DES --privPass=despass --authengine=8000000903000019563F8338 bq-gwhsrp.lss.emc.com`
  
  - For Windows: `sm_snmpwalk --snmp=3 --user=desuser --auth=MD5 --authPass=changeme --priv=DES --privPass=despass --authengine=8000000903000019563F8338 bq-gwhsrp.lss.emc.com`

The above command will generate three files, `xxxxx.walk`, `xxxxx.mimic`, and `xxxxx.snap` files [where `xxxxx` is the device IP] in the same location, that is in `NMSROOT/objects/smarts/bin`. You can zip the 3 generated files.

Q. Can I have HPOV/Netview installed in one drive, for example C: and DFM HPOV/Netview Adapters in another drive, D:?  
A. No. It is recommended to install both HPOV/Netview and Fault Management HPOV/Netview Adapters in the same drive. For more information, see:  

Q. In the Search Results, the selected devices are not displayed as selected. They are displayed as selected only in All Devices group. Why?  
A. This is the default behavior of HOSTree. The devices will be displayed as selected only in All Devices group, and not wherever the devices are listed.

Q. How can I avoid Fault Management generating Unresponsive alerts when the devices are in Natted Enviroment?  
A. Based on the solution offered by the case 60634 2543, Fault Management may have walked the `ipAddrTable` for these Natted devices and got back the untranslated IP address. If you try to poll that IP address it will not work. In such a case, you can disable polling for selected IP addresses from the Alerts and Activities display screen.

To disable polling:

**Step 1**
From the Alerts and Activities display, start the view that contains your device.

Unmanaged devices will be in the Suspended Devices view.

The DDV opens. Depending upon the managed state of the device, either the Suspend or the Resume button is shown.
**Step 2**  
Click **Suspend** to change the device’s current managed state to Suspended.  
Fault Management no longer polls any device components, nor does it process any traps. All alerts and activities change to the Cleared state, and the device is moved to the Suspended Devices view.  
Subsequent events (including traps) are ignored and no longer processed.

---

**Q.** How can I get rid of alerts for a device that has been deleted?  
**A.** To get rid of the alerts of a deleted device, you have to cleanup the database and re-initialize the Fault Management databases using `dbRestoreOrig.pl`.

---

**Step 1**  
Go to the command prompt and stop the daemon manager by entering **net stop crmdmgtd**  
**Step 2**  
Go to `C:Program Files\CSCOpx\bin`  
**Step 3**  
Reinitialize the Fault Management databases by entering:  
- `perl dbRestoreOrig.pl dsn=dfmInv dmprefix=INV`  
- `perl dbRestoreOrig.pl dsn=dfmFh dmprefix=FH`  
- `perl db RestoreOrig.pl dsn=dfmEpm dmprefix=EPM`  
**Step 4**  
Restart the daemon managers by entering **net start crmdmgtd**  
After a few minutes, all processes will restart.

---

**Q.** Why HighUtilization on interface gets generated by Fault Management?  
**A.** The reason could be a bug at the agent side. The agent side bug for MSFC is CSCdy46229. It was fixed in 12.2(15) and later versions. The agent side bug for VG248 device is CSCsj51190.

**Q.** Why does a device go into Unsupported state although it is Supported?  
**A.** Some devices, in spite of being supported, go to Unsupported state because CDP is not enabled on them. Fault Management manages such devices only when CDP is enabled on them. Examples of such devices are CCC and CPA.

**Q.** What is the difference between Snmp Raw Trap Forwarding and Processed Snmp Trap alert/event Trap Forwarding? Does Fault Management support both of these methods?  
**A.** Yes, Fault Management supports both ways of Trap forwarding.  
Raw Trap is forwarded by the Device to Fault Management and Fault Management has to process it. To configure Raw Trap Forwarding, go to **Monitor > Fault Settings > SNMP Traps > Forwarding**.  
When Fault Management receives certain SNMP traps, it analyzes the data found in fields such as Enterprise/Generic trap identifier, Specific Trap identifier, and variable-bindings of each SNMP trap message.  
If needed, Fault Management changes the property value of the object property. These are Processed Traps. This configuration can also send trap notifications if there is a threshold violation in the Fault Management managed devices.
Q. How does Fault Management detect Trunk and Access ports?
A. If a port is connected to a system interface, the PortType is labelled as ACCESS and if the port is connected to another port, it is labelled as TRUNK.

To verify the PortType in Incharge, check the NeighboringSystems attribute under the port. This attribute indicates whether the port is connected to a switch, router, or a host interface. If the discovered port has no connection, then the default PortType is ACCESS.

To find the NeighboringSystem attribute, go to dmctl and enter `get Port::PORT-<Port Name>`.

Q. What is the meaning of different discovery percentages?
A. The following list explains the different discovery percentages:

- 10% — Startup, where devices have not been handed over to Incharge processes yet
- 40% — Devices have been successfully handed over to Incharge processes
- 70% — Incharge processes have successfully discovered devices and handed the information over to Cisco code
- 90% — Discovered devices must be placed in appropriate groups. Device information has been sent to Grouping Services and group information from Grouping Services is awaited.

Q. How can I troubleshoot device discovery stuck at 10%?
A. If device discovery is stuck at 10%, it means that devices to be discovered have not been communicated to Incharge processes yet. To troubleshoot device discovery stuck at 10%:

- On Solaris or Soft Appliance:

  **Step 1** Enter the `pdshow` command to check if DfmServer and DfmBroker processes are running.
  
  **Step 2** Check if there are multiple instances of brstart and sm_server.
  
  The name of binary for DfmBroker is brstart and for DfmServer, it is sm_server.
  
  **Step 3** Enter the following commandline:
  
  `/usr/ucb/ps -auxww | grep brstart`
  `/usr/ucb/ps -auxww | grep sm_server`
  
  For example:
  ```
  marver-sol-daily# /usr/ucb/ps -auxww | grep brstart
  root 11751 0.1 0.1 984 648 pts/7 S 11:34:49 0:00 grep brstart
  casuser 11577 0.0 0.42465613496 ? S 09:42:38 0:00 brstart --output --port=9002
  ---user=casuser
  ```

  If you see more than one instance of each process, enter the command `ptree` to get all related process.
  
  For example:
  ```
  marver-sol-daily# ptree 11577
  11461 /opt/CSCOpx/objects/dmgt/dmgtd.sol
  11577 brstart --output --port=9002 ---user=casuser
  11588 /opt/CSCOpx/objects/smarts/bin/system/sm_logerror 131
  11604 /opt/CSCOpx/objects/smarts/bin/system/sm_authority
  11605 /opt/CSCOpx/objects/smarts/bin/system/sm_logerror 136
  ```

  **Step 4** Except for dmgtd.sol, manually terminate all processes found in the `ptree` command by entering the command: `kill -9`.


Step 5  Stop the daemon manager by entering `net stop crmdmgtd`.
Wait for five minutes.

Step 6  Enter `netstat -a | grep 9002` to make sure that port 9002 is not in listening state or timed wait state.

Step 7  Enter `netstat -a | grep 435` to make sure that ports 43501 to port 43508 are not in listening or timed wait state.

If the ports are in listening state, use the Unix utility to find the process that owns the ports and terminate that process.

Step 8  Start the daemon manager by entering `net start crmdmgtd`.

Step 9  Enter the following command: `/objects/smarts/bin/brcontrol`
The following is an example of the output:

```
Broker is located at: localhost:9002
Domain Host Name Port Proc ID State Last Chg Time
DFM marver-sol-daily 50449 11589 RUNNING Oct 26 09:42:58 2005
```

Step 10 Check whether the displayed host name is the host name in DNS or `/etc/hosts`

- On Windows:

Step 1  Download the tools from the following location: http://www.sysinternals.com/Utilities/PsTools.html

Step 2  Unzip it into a directory.

Step 3  Enter `pdshow DfmServer` `pdshow DfmBroker` to check whether the processes DfmServer and DfmBroker are running.

Step 4  Enter `/objects/smarts/bin/brcontrol`

Step 5  Check whether the host name is the same as in DNS.

Step 6  Check whether there are multiple instances of brstart and sm_server
You can use the downloaded Pstool to see one branch each of brstart and sm_server.
For example:

```
pplist -t
brstart 5708 8 1 16 8476 1104 264
brstart 5880 8 7 86 32720 11240 9664
sm_authority 6452 8 1 52 14376 3616 1528
sm_server 6332 8 1 16 8476 1104 264
sm_server 6416 8 124 678 212696 58784 56812
sm_authority 6444 8 1 47 14376 3572 1528
```

There should be only one branch. You need to terminate any extra branches.

Step 7  Stop the daemon manager by entering `net stop crmdmgtd`.
Wait for five minutes.

Step 8  Enter `netstat -a -n -p tcp` to make sure that ports 9002 and 43501 to 43508 are not in listening state or timed wait state.

Step 9  Start the daemon manager by entering `net start crmdmgtd`. 
How can I troubleshoot device discovery stuck at 40%?

To troubleshoot device discovery stuck at 40%:

Step 1 Make sure that the device under question is responding to ping messages.

Step 2 Make sure that the device responds to snmpwalk by entering:

```
(objects/smarts/bin/sm_snmp -c --dest=walk
```

Step 3 Enable discovery logging in incharge process by entering:

```
(objects/smarts/bin/dmct1 -s DFM
```

Note In some cases, you need to enter your UserID and Password.

Step 4 From dmct1 prompt, enter:

```
ICF-TopologyManager::ICF-TopologyManager::DebugEnabled TRUE
```

Step 5 Exit out of dmct1

Step 6 Trigger the rediscovery of the device

The log file from the location /objects/smarts/local/logs/DFM.log will have discovery information in detail. It will provide the root cause for the failing device discovery.

Step 7 Restore debug to False.

How can I troubleshoot device discovery stuck at 90%?

To troubleshoot devices stuck at 90% discovery:

Step 1 Increase the log level for Inventory Service to debug.

Step 2 Stop the daemon manager by entering `net stop crmdmgtd`

Step 3 Take a backup of the following file:

```
/MDC/tomcat/webapps/triveni/WEB-INF/classes/log4j-ogs.properties
```

Step 4 Replace the string FATAL by string DEBUG

Step 5 Start the daemon manager by entering `net start crmdmgtd`

Step 6 Collect the contents of /log/dfmLogs/TIS file by entering:

- On Solaris or Soft Appliance:
  ```
  /var/adm/CSCIpx/log/DFMServer.log
  ```
- On Windows:
  ```
  /log/DFMServer.log
  ```

How can I stop nGenius RealTimeMonitoring in Solaris or Soft Appliance?

If nGenius RealTimeMonitoring is not getting uninstalled, stop it before LMS installation and do not restart it manually.

Enter `/opt/NetScout/rtm/bin/stop1` to stop it. It will get started again when the system is rebooted.
Q. How can I perform rediscovery of devices in LMS through CLI?
A. To perform a rediscovery of:
   - All devices:
     Enter `dmctl -s DFM invoke ICF_TopologyManager::ICF-TopologyManager discoverAll`
   - A specific device:
     Enter `dmctl -s DFM invoke ICF_TopologyManager::ICF-TopologyManager ::`

Q. How can I manage or unmanage ports and interfaces from CLI?
A. To manage or unmanage ports and interfaces from CLI, enter
   `dmctl -s=DFM invoke class::instance op [arg1 ...]`
   The following is the list of examples:
   - `dmctl> invoke Port::PORT-5.1.2.2/10123 manage`
   - `dmctl> invoke Interface::IF-5.1.3.2/1 manage`
   - `dmctl> invoke Port::PORT-5.1.2.2/10123 unmanage`

Q. How can I import devices into DCR through CLI?
A. To import devices into DCR through CLI:
   
   **Step 1** Run the command `dcrecli -u admin` with the LMS username as the argument.
   
   **Step 2** Enter the LMS password when prompted.
   
   **Step 3** At the `dcrecli` prompt, enter `dcrecli> impFile fn="path to csv import file" ft=csv`

Q. How can I enable CAM logs for debugging ACS Configuration?
A. To enable CAM logs:
   
   **Step 1** Go to the command prompt and enter `/opt/CSCOpx/MDC/bin/ccraccess -updateLog Core cam DEBUG`
   
   **Step 2** Restart the daemon manager after enabling logs.
   
   The logs will be under `NMSROOT/MDC/log`

Q. How can I create a link to the Java Plug-in in Mozilla?
A. Create a symbolic link to the Java Plug-in `libjavaplugin_oji.so` file in the Mozilla Plugins directory.
   To create the link, go to the command prompt and enter:
   
   **Step 1** `cd /plugins`
   
   **Step 2** `ln -s /plugin/sparc/ns610/libjavaplugin_oji.so .`

   Include the period at the end.

   Restart your browser.
Frequently Asked Questions

Q. How does LMS react to a Cisco ISR with Inline POE switch module when there is no -48V power supply installed?

A. When there is no -48V power supply installed, the device Cisco ISR with Inline POE switch module shows up in SNMP as being in a Critical state. There is no option to unmanage it from the GUI. You need to perform a command line edit of the database whenever the device is added or re-added to LMS.

Enter the following command to edit the database:

Step 1
Find out to which LMS domain the device belongs.
From the command prompt, enter:
NMSROOT/objects/smarts/bin/

Step 2
Enter
dmctl -s DFM geti ICIM_UnitaryComputerSystem
and
dmctl -s DFM1 geti ICIM_UnitaryComputerSystem
The list of devices managed by LMS domains are listed.

Step 3
Enter dmctl -s Domain Name
For example, if you find the device listed under LMS domain, enter: dmctl -s DFM
Your login will be successful and you will see the prompt dmctl>

Step 4
From Detailed Device View (DDV), get the power component name of the device
Or
Enter dmctl>geti PowerSupply to list the power components of the devices:
The power components are listed.

Step 5
Enter dmctl>get PowerSupply::componentname::IsManaged to check the management status of the component.
For example, if PWR-fl-69-69-9-45.dyn.embarqhsd.net/2 is the power component, enter
dmctl>get PowerSupply::PWR-fl-69-69-9-45.dyn.embarqhsd.net/2::IsManaged
If it returns TRUE, set it to False.

Step 6
Enter:
    dmctl>invoke PowerSupply::PWR-fl-69-69-9-45.dyn.embarqhsd.net/2 unmanage

Step 7
Run Step 5 again to check if the management state is set as FALSE

Step 8
To apply the changes, enter:
    dmctl>invoke ICF_PolicyManager::ICF-PolicyManager reconfigure

Q. What happens when VG200 Routers have an ISDN PRI carrying voice traffic?

A. When VG200 Routers have an ISDN PRI carrying voice traffic, by default, LMS generates a Warning alert whenever a phone call uses a B-channel. For every ISDNBCHANNEL, set the Managed State as False in Device Detailed View. They are then listed with the Backup Mode.

However, removing the Backup Interface Support Settings is not a workaround since that will cause LMS to report an error whenever any B-channel is not in use.
Q. I am unable to sort Cleared Alerts in LMS. Why?

A. Alerts are moved to Cleared state when their last active event has been in the Cleared state for 20 minutes. Cleared alerts remain in that state for twenty minutes. After that time it is removed from the Alerts and Activities Display. So, whenever the Status column is sorted, the Cleared alerts remain only in the end of the Status column. Sorting is not available for Cleared alerts.

**General**

This section provides the general FAQs for IPSLA Monitoring:

- What are the supported NAM versions? What happens if an unsupported NAM version is configured in LMS?
- What is IPSLA Monitoring?
- How can I access the IPSLA functionality?
- What are the Cisco IOS software releases that support IP SLA operations?
- What are the network performance statistics that I can measure using IPSLA Monitoring?
- Does IPSLA Monitoring require a dedicated hardware probe to measure and monitor network performance statistics?
- What are the MIBs used by IPSLA Monitoring?
- What network protocols does IPSLA Monitoring support?
- How frequently I can take network performance measurements?
- Is the data averaged or summarized when IPSLA Monitoring collects the data from IP SLA using SNMP?
- Does IPSLA Monitoring support data export?
- What is the difference between Active and Passive FTP session modes?
- Does IPSLA Monitoring receive traps?
- Do I run a Cisco IOS software release with the IP SLA feature on all my routers to get hop-by-hop performance statistics?
- Does IPSLA Monitorings support SNMPV3?
- Does IPSLA Monitoring take measurements from the management workstation?
- How does IPSLA Monitoring interact with IP SLA operations of Cisco IOS software?

Q. What are the supported NAM versions? What happens if an unsupported NAM version is configured in LMS?
A. Only NAM 4.1 is supported.
   If you configure NAM 5.0 or higher version, this portlet displays HTTP 500 error.

Q. What is IPSLA Monitoring?
A. IPSLA Monitoring is a network management functionality that allows you to monitor the performance of multi-protocol networks.
   IPSLA Monitoring monitors the network performance by configuring collectors on IP SLA (IP Service Level Agreement) capable source devices (routers) and collects the performance-related statistics from these devices.

Q. How can I access the IPSLA functionality?
A. You can access IPSLA functionality using:
   - Web-based Cisco Prime LMS User Interface.
   - IPSLA CLI scripts by logging on to LMS server using Telnet or SSH.

Q. What are the Cisco IOS software releases that support IP SLA operations?
A. Table 19-1 maps the Cisco IOS releases to IP SLA operations.

<table>
<thead>
<tr>
<th>IP SLA Operations</th>
<th>Cisco IOS Software Releases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Echo</td>
<td>12.3(14)T</td>
</tr>
<tr>
<td>Path Echo</td>
<td>12.3(14)T</td>
</tr>
<tr>
<td>UDP Jitter</td>
<td>12.3(14)T</td>
</tr>
<tr>
<td>DNS</td>
<td>12.3(14)T</td>
</tr>
<tr>
<td>FTP</td>
<td>12.3(14)T</td>
</tr>
<tr>
<td>DHCP</td>
<td>12.3(14)T</td>
</tr>
<tr>
<td>UDP Echo</td>
<td>12.3(14)T</td>
</tr>
<tr>
<td>HTTP</td>
<td>12.3(14)T</td>
</tr>
<tr>
<td>TCP Connect</td>
<td>12.3(14)T</td>
</tr>
<tr>
<td>DLSw</td>
<td>12.3(14)T</td>
</tr>
<tr>
<td>RTP</td>
<td>12.4(4)T</td>
</tr>
<tr>
<td>VoIP Gatekeeper Registration Delay</td>
<td>12.3(14)T</td>
</tr>
<tr>
<td>ICMP Jitter</td>
<td>12.4(6)T</td>
</tr>
<tr>
<td>VoIP Call Setup Post Dial Delay</td>
<td>12.3(14)T</td>
</tr>
<tr>
<td>Ethernet Jitter / Ethernet Jitter Auto IPSLA</td>
<td>12.2(44)SE</td>
</tr>
<tr>
<td>Ethernet Ping / Ethernet Ping Auto IPSLA</td>
<td>12.2(44)SE</td>
</tr>
</tbody>
</table>
Q. What are the network performance statistics that I can measure using IPSLA Monitoring?

A. You can measure the following network statistics using IPSLA Monitoring:
   - Latency
   - Availability
   - Jitter
   - Packet Loss
   - Errors
   - Mean Opinion Score (MOS)
   - Calculated Planning Impairment Factor (ICPIF)

Q. Does IPSLA Monitoring require a dedicated hardware probe to measure and monitor network performance statistics?

A. No. IPSLA Monitoring uses the IP SLA probes embedded in the Cisco IOS software.

Q. What are the MIBs used by IPSLA Monitoring?

A. IPSLA Monitoring extensively uses CISCO-RTTMON-MIB, which is a part of IP SLA in the Cisco IOS software. Almost all tables in CISCO RTTMON-MIB are queried by IPSLA Monitoring. The SYSTEM-MIB is used minimally. IPSLA Monitoring uses MPLS -VPN -MIB to query for VRF details. IPSLA Monitoring also uses Ethernet MIB and VRF MIB.

Q. What network protocols does IPSLA Monitoring support?

A. IPSLA Monitoring supports IP monitoring. It also supports high-level IP protocols including:
   - DHCP
   - DLSw
   - DNS
   - HTTP
   - FTP
   - TCP Connect
   - UDP Echo
   - UDP Jitter
   - Echo
   - Path Echo
   - RTP
   - Gatekeeper Registration Delay
   - Call Setup Post Dial Delay
   - ICMP Jitter
   - Ethernet Operations
**Frequently Asked Questions**

**Q.** How frequently can I take network performance measurements?

**A.** IP SLA generates several measurements every hour. IPSLA Monitoring polls the router once every hour and collects the summarized statistics for that period.

You can set the sampling interval for IP SLA for as often as every 10 seconds, but for optimal performance, we recommend a sample interval of at least 60 seconds (1 minute). This is the default value.

You can view the latest real-time statistics in the Real Time Statistics window as IP SLA gathers the data from the collector. However, IPSLA Monitoring does not store the real-time data in the IP SLA database. IPSLA Monitoring stores only the hourly summarized data in the IPSLA database.

**Q.** Is the data averaged or summarized when IPSLA Monitoring collects the data from IP SLA using SNMP?

**A.** The data is summarized and averaged in many ways. IPSLA Monitoring displays the data in the Historical Statistics window in hourly, daily, weekly, and monthly increments.

IPSLA Monitoring also displays average, minimum, and maximum calculations of the data over the monitoring period. IPSLA Monitoring also provides consolidation facility for purging and summarizing older data.

**Q.** Does IPSLA Monitoring support data export?

**A.** Yes. IPSLA Monitoring CLI allows you to export files with user-defined delimiters.

**Q.** What is the difference between Active and Passive FTP session modes?

**A.** The File Transfer Protocol (FTP) has multiple modes of operation that can affect its operation and, as a result, the security of your network.

These modes of operation determine whether the FTP server or FTP client initiates the TCP connections that send information from the server to the client. The FTP protocol supports two modes of operation:

- **Active Mode**
- **Passive Mode**

**Active Mode**

In Active FTP, the client opens a control connection on port 21 to the server. Whenever the client requests data from the server, the server opens a TCP session on port 20.

The Active mode of operation is less secure than the Passive mode. This mode of operation complicates the construction of firewalls, because the firewall must anticipate the connection from the FTP server back to the client program.

The steps in the Active mode are:

1. The client opens a control channel (port 21) to the server and informs the server which port number it should respond to. This port number is a randomly determined port that is greater than 1023.

2. The server receives this information and sends the client an acknowledgement. The client and server exchange commands on this control connection.

When the user requests a directory listing or initiates sending or receiving a file, the client software sends a `PORT` command. This command includes a port number that is greater than 1023. This is the port number that the client wants the server to use for the data connection.

3. The server opens a data connection from port 20 to the client's port number. This is the number given in the `PORT` command.
Passive Mode

In Passive FTP, the client opens the data sessions, using a port number supplied by the server. This mode of operation is assumed to be more secure because all the connections are being initiated from the client, so there is less chance that the connection will be compromised.

It is called Passive because the server performs a “passive open”.

The steps in the Passive mode are:

1. In Passive FTP, the client opens a control connection on port 21 to the server, and then requests the Passive mode by using the PASV command.
2. The server agrees to this mode, and then selects a random port number (greater than 1023). It sends this port number to the client for data transfer.
3. The client receives this information and opens a data channel to the server assigned port.

Q. Does IPSLA Monitoring receive traps?
A. No. IPSLA Monitoring does not receive traps. You can configure IPSLA Monitoring to raise a trap when a threshold violation or timeout occurs. However, you should configure a separate NMS (Network Management Station) to receive and process these traps.

Q. Do I run a Cisco IOS software release with the IP SLA feature on all my routers to get hop-by-hop performance statistics?
A. No. Only routers sourcing the network performance measurements or routers defined as Targets for UDP Jitter measurements must run the IP SLA feature.

Q. Does IPSLA Monitoring support SNMPV3?
A. Yes. IPSLA Monitoring supports SNMPV3 in AuthNoPriv as well as AuthPriv mode. That is, you can configure the source router with SNMPV3 AuthNoPriv/AuthPriv and add it into IPSLA Monitoring to create collectors. While creating collectors, the communication to the device occurs using V3.

Q. Does IPSLA Monitoring take measurements from the management workstation?
A. No. IPSLA Monitoring configures IP SLA operations in Cisco IOS software to take measurements. These measurements are taken within the network instead of from the management workstation.

Q. How does IPSLA Monitoring interact with IP SLA operations of Cisco IOS software?
A. IPSLA Monitoring uses SNMP to configure IP SLA in Cisco IOS software to gather network performance statistics. IPSLA Monitoring uses SNMP to collect the statistics from IP SLA and stores the information in a database for future reference and analysis.

IPSLA Devices

This section provides the following FAQs on the IPSLA Device Management.

- Are adhoc target devices included for device license count?
- What are the device attributes that I can edit?
- Can I edit adhoc target device attributes?
- What does Responder Enabled target device mean?
- Does a target device need to be a router that supports IP SLA?
Frequently Asked Questions

- **Why Responder enable devices are not displayed below Responder Category?**
- **Q.** Are adhoc target devices included for device license count?
  - **A.** No. Only DCR devices are included for the device license count.
- **Q.** What are the device attributes that I can edit?
  - **A.** You can edit the device information, such as SNMP Retry and SNMP Timeout, but you cannot modify the device name.
- **Q.** Can I edit adhoc target device attributes?
  - **A.** No. You can edit only DCR device attributes.
- **Q.** What does Responder Enabled target device mean?
  - **A.** This is a component embedded in a Target Cisco device running version 12.1 or later of the Cisco IOS software. It responds to IP SLA request packets from a Source device and provides accurate results.
- **Q.** Does a target device need to be a router that supports IP SLA?
  - **A.** No. IPSLA Monitoring supports target devices as long as they are reachable through IP. These target devices can be Web servers, PCs, printers, routers, switches, network devices, or any other device with an IP address. However, if you are measuring UDP Jitter statistics for applications such as Voice over IP or VPN monitoring, the target devices must be a Cisco router running a release of the Cisco IOS software that supports the IP SLA Responder feature Cisco IOS version 12.1(2)T or later. We recommend version 12.1 or later.
- **Q.** Why Responder enable devices are not displayed below Responder Category?
  - **A.** Check if the device is IPSLA responder. If not, Enable IPSLA responder on the device. Then go to Monitor > Performance Settings > IPSLA > Devices and select the device and click Update IPSLA config.

Operations

This section provides the following FAQs on the Operation Management module in IPSLA Monitoring.
- **What is IOS IP SLA?**
- **What is a sample interval?**
- **Does IPSLA Monitoring provide predefined operations for all IP SLA operations?**
- **What port numbers does IPSLA Monitoring support for UDP operations?**
- **Can I delete the default operations?**
- **Where do I specify the DNS Lookup Name in IPSLA Monitoring?**
- **Where do I specify the HTTP server in IPSLA Monitoring?**
- **Where do I specify the FTP server in IPSLA Monitoring?**
- **When should the target port number be an even number?**
- **Is the DefaultDNS operation available in Windows platform?**
• Why do collectors created with ICMP Jitter operation move to Config Failed state?
• Why I am unable to see the MOS and ICPIF values for UDP Jitter collectors?
• Is target device required for operation types, namely VOIPCallSetup, VOIP Registration delay?
• What is the DNS server address for defaultDNS operation after restore?

Q. What is IOS IP SLA?
A. IP SLA (formerly known as SAA) is a feature built into Cisco Internetwork Operating System (IOS), used by most Cisco routers and IOS switches. IP SLA has been available since IOS version 11.2.

Q. What is a sample interval?
A. This is a frequency with which IPSLA Monitoring source device polls the target device to retrieve the statistics. These statistics are based on the IP SLA operations configured by you.

Q. Does IPSLA Monitoring provide predefined operations for all IP SLA operations?
A. No. IPSLA Monitoring does not provide a predefined operation for HTTP, FTP, or RTP. Therefore, before you create a HTTP, FTP, or RTP collector, you must first create the respective HTTP, FTP, or RTP, CallSetupPostDailaDelay, EthernetPing, EthernetPingautoIPSLA, EthernetJitter, and EthernetJitterAutoIPSLA operation.
Frequently Asked Questions

Q. What port numbers does IPSLA Monitoring support for UDP operations?
A. For UDP connections, the valid port numbers are 7, and 1025 to 65535.
   If the target device is a Cisco router running version 12.1 or later of the Cisco IOS software, you can specify any port. That is, you can specify any port number greater than 1024 to communicate with the IP SLA Responder, as long as some process is listening on that Target port.
   The only known port allowed is UDP port 7.
   If the target device, whether a Cisco or a non-Cisco IP host, is not running version 12.1 or later of the Cisco IOS software, you must specify UDP port 7 as the Target port.

Q. Can I delete the default operations?
A. No. You can delete only user-defined operations.

Q. Where do I specify the DNS Lookup Name in IPSLA Monitoring?
A. As the workflow has changed in IPSLA Monitoring, you must specify the DNS Lookup Name while creating collectors as part of the Target.

Q. Where do I specify the HTTP server in IPSLA Monitoring?
A. As the workflow has changed in IPSLA Monitoring, you must specify the HTTP server while creating collectors as part of the Target.

Q. Where do I specify the FTP server in IPSLA Monitoring?
A. As the workflow has changed in IPSLA Monitoring, you must specify the FTP server while creating collectors as part of the Target.

Q. When should the target port number be an even number?
A. If you have specified the codec type as 1, 2, or 3 while defining a UDP Jitter.

Q. Is the DefaultDNS operation available in Windows platform?
A. No. After installing IPSLA Monitoring, the DefaultDNS operation is not available for Windows platform. It is available only in Solaris or Soft Appliance platforms, because for Solaris or Soft Appliance platforms the DNS servers are stored under /etc/resolve.conf. In case of Windows, there is similar file where you can find the DNS server. Hence, DefaultDNS is supported only on Solaris or Soft Appliance platforms. However, you can customize the DNS operation and configure it with DNS servers as targets on Windows platform.

Q. Why do collectors created with ICMP Jitter operation move to Config Failed state?
A. ICMP Jitter is supported only from IOS versions 12.4(6)T. Hence, you cannot configure collectors on source devices with ICMP Jitter versions less than 12.4(6)T. If you try to configure them, the collectors move to the Config Failed state.

Q. Why am I unable to see the MOS and ICPIF values for UDP Jitter collectors?
A. You cannot view the MOS and ICPIF values if you have defined a collector with default UDP Jitter operations such as default60ByteVoice or default160ByteVoice. This is because the codec type is ‘0’ for these operations.
   To view the values of MOS and ICPIF, you should define collectors with customized UDP Jitter with appropriate codec type values such as 1, 2, or 3.
Q. Is target device required for operation types, namely VOIPCallSetup, VOIP Registration delay?
A. No. You need not specify the target device for these operation types because the Target refers to the called number.

Q. What is the DNS server address for defaultDNS operation after restore?
A. After the Restore operation (same version Backup-Restore), the defaultDNS operation points to the DNS server which was available in the backup archive. Hence, after Restore, you need to add the restored server to the DNS server in the backup. If you do not add the server, all the collectors configured with that DNS server in backup become invalid. That is, they will not generate statistics or skewed statistics based on whether the DNS server is reachable or not. Hence, you need to add the restored server into the DNS server available in the backup or you must customize the DNS operation with newly available DNS server and create collectors for that.

Collectors

This section provides the following FAQs on the Collector Management module in IPSLA Monitoring.

- Can I configure collectors that use IP SLA targets and NNTP, POP3, or SMTP operations?
- What does Historical or Statistical collector type mean?
- What does Monitored or Real-time collector type mean?
- What is a polling interval?
- Do minute (1, 5, 15, 30) based collectors poll every hour also?
- Why is the Poller Settings section disabled in the Collector Configuration wizard when I select the Monitored or Real-time option?
- Can collectors in Config Failed status move back to Running status?
- What are Outages?
- Is Outage applicable for all type of reports?
- Is Outage period data included for IPSLA Summarized reports?
- Is it possible to schedule outage which runs on last day of every month?
- Can you modify the outage details?
- Is it possible to create outage for all collectors?
- What will happen if I delete all collectors associated with the outage?
- Can I edit the recurrence type of the scheduled outage while editing the outage?
- What will happen if the complete outage falls in the purging period?
- Can you view the completed outage details?
- What is a Syslog?

Q. Is the target device a must for creating collectors?
A. No. The target device is not required for operations, such as Gatekeeper Registration Delay, Call Setup Post Dial Delay, and RTP.

Q. Can I configure collectors that use IP SLA targets and NNTP, POP3, or SMTP operations?
A. No. IP SLA targets are routers, and routers cannot perform NNTP, POP3, or SMTP services.

If you configure a collector with an IP SLA target and an NNTP, POP3, or SMTP TCP Connect operation (such as DefaultNNTP, DefaultPOP3, or DefaultSMTP), IPSLA Monitoring displays No Connection error messages and does not collect data.

Q. What does Historical or Statistical collector type mean?
A. The collector type specified while creating a collector. This collector type archives the collector statistics in the IPSLA database to generate custom reports.

Q. What does Monitored or Real-time collector type mean?
A. The collector type specified while creating a collector to view the collector statistics in real time. The real-time statistics are not stored in the IPSLA database.

Q. What is a polling interval?
A. The frequency with which the LMS server polls the source router to retrieve the statistics and update the IPSLA database. IPSLA Monitoring also supports 1, 5, 15, and 30 minutes polling frequencies to the fixed 60 minutes polling frequency.

Q. Do minute (1, 5, 15, 30) based collectors poll every hour also?
A. Yes, apart from polling during the specified polling intervals (such as 1, 5, 15, or 30 minutes), it is also polled every 60 minutes. As the consolidation of statistical data into daily, weekly, and monthly tables are done only from hourly collection tables.

Hence, you must populate the hourly tables, as well. However, for a collector with polling interval 60 minutes, the polling is done only every 60 minutes.

Q. Why is the Poller Settings section disabled in the Collector Configuration wizard when I select the Monitored or Real-time option?
A. The real-time collectors will not poll automatically. They are only configured on the source router based on the Start and End Time details that you have specified.

Hence to view the real-time collectors statistics, click the Monitor button on the Collector Management page. The statistics of the collectors are displayed as a graph. The real-time statistics are not stored in the database.
Q. Can collectors in Config Failed status move back to Running status?
A. Yes. It can happen in the following scenarios:
   • When the IPSLA processes are restarted, all the collectors in Config Failed status are reconfigured. During this process, the collectors are moved to Running status if the conditions for creating collectors are satisfied.
   • When a device associated with a collector is rebooted, all the collectors are reconfigured. Hence the collectors can move from Config Failed to Running status if the conditions for creating collectors are satisfied.

The conditions for creating collectors successfully are:
   • Device should be reachable while configuring the collectors.
   • Device should be reachable through SNMP.
   • Device should support the operations.

Q. What are Outages?
A. Outages or downtime are the period of time when the network fails to provide the primary function

Q. Is Outage applicable for all type of reports?
A. No. Outage configuration is applicable only for Historical collectors and not for Real time collectors.

Q. Is Outage period data included for IPSLA Summarized reports?
A. No. The Outage period data is excluded during IPSLA Summarized report generation.

Q. Is it possible to schedule outage which runs on last day of every month?
A. Yes. It is possible to schedule outage which runs on the last day of every month.

Q. Can you modify the outage details?
A. You can modify only the Schedule Outage details. However, you can edit or modify completed or active outage details.

Q. Is it possible to create outage for all collectors?
A. Yes. It is possible to create outages for all collectors.

Q. What will happen if I delete all collectors associated with the outage?
A. The outage will be deleted along with the collectors.

Q. Can I edit the recurrence type of the scheduled outage while editing the outage?
A. No. You cannot edit the recurrence type of the scheduled outage while editing the outage.

Q. What will happen if the complete outage falls in the purging period?
A. Purging for the collectors will be based on the collector status.

Q. Can you view the completed outage details?
A. Yes. You can click the Completed Outage button to navigate to the completed outage reports page.
Frequently Asked Questions

Q. What is a Syslog?
A. Syslog is a trap message that is sent from the device if any changes occur to the device.

CLI Commands

This section provides following FAQs on IPSLA CLI reference.

- What is the command to list IPSLA CLI commands?
- Does IPSLA CLI require LMS authentication?

Q. What is the command to list IPSLA CLI commands?
A. To view the list of IPSLA CLI commands, go to NMSROOT/bin and enter `ipm -help`.

Q. Does IPSLA CLI require LMS authentication?
A. Yes. IPSLA CLI requires LMS authentication.

For more information, type `ipm -help` at NMSROOT/bin on any LMS 4.1 server.

IPSLA Monitoring

This section provides the following troubleshooting tips for IPSLA Monitoring.

- I have problems while migrating the IPSLA data. What should I do?
- I am unable to migrate the customized operations properly. What should I do?
- I am not able to migrate the collectors. What should I do?
- Why are the collectors not moved to a Running state?
- The devices are not migrated? What should I do?
- What if I accidentally create a collector that uses all remaining memory in the source router?
- What should I do when all DHCP IP Address leases are exhausted?
- When I attempt to generate reports, I get an error message, No data available for the selected time period. What should I do?
- When does the system consolidation happen?
Q. I have problems while migrating the IPSLA data. What should I do?
A. Check the following log files for information:
   - restorebackup.log
   - migration.log
   - ipmclient.log
   - ipmsserver.log

Q. I am unable to migrate the customized operations properly. What should I do?
A. Check whether:
   - IPSLA backed up DB contains custom operations.
   - Predefined or custom SNA Operations are migrated.
   - Alerts of NMVT type are changed to None.
   - Alerts of NMVT and SNMP trap are changed to snmp trap.

Q. I am not able to migrate the collectors. What should I do?
A. Make sure that:
   - Source devices, target devices, and operations are migrated properly.
   - Collectors configured with SNA operations are migrated.

Q. Why are the collectors not moved to a Running state?
A. Check whether:
   - The devices are SNMP reachable from LMS.
   - There is sufficient memory in the router to configure probes. If not, remove some probes on the router CLI.

Q. The devices are not migrated? What should I do?
A. Make sure that the IPSLA backed up database contains source and target devices.

Q. What if I accidentally create a collector that uses all remaining memory in the source router?
A. The IP SLA in IOS 12.1 or later provides a low watermark feature to prevent collectors from using all the memory in the source router. Low watermark memory is a memory on the source router.

Q. What should I do when all DHCP IP Address leases are exhausted?
A. When you use DHCP operations with certain DHCP servers, all DHCP IP address leases on the servers can be exhausted. To reduce the likelihood of this problem occurring:
   - Reduce IP address lease times on your DHCP servers. Long lease times increase the likelihood of this problem occurring.
   - Change the frequency of the DHCP operations from the default of 60 seconds to 5 minutes.
   - Do not configure a large number of DHCP operations on the same subnet (using the same DHCP server).

Q. When I attempt to generate reports, I get an error message, No data available for the selected time period. What should I do?
Frequently Asked Questions

A. It may be caused by any of the following:
   • You have tried to generate report for a collector that has no data in the database for the selected time period (From and To time specified while creating the report) and granularity (such as minute, hourly, daily, weekly, and monthly).
   • The selected collectors and the report type are different. For example, you cannot select UDP Jitter as the report type for generating report on a collector with ICMP Jitter as the operation type. However, report types, namely Latency and Availability support all collectors.
   • You have tried to generate minute reports and graphs for collectors with polling interval 60 minutes. You can generate minute reports and graphs only if you have set the polling interval as 1, 5, 15, or 30 minutes while creating the collector.
   • You have tried to generate reports for real-time collectors that do not store data in the database.

Q. When does the system consolidation happen?
A. The system consolidation happens everyday based on the granularity:
   • Hourly to Daily
   • Daily to Weekly
   • Daily to Monthly

Hourly to Daily
During the hourly to daily consolidation, the system consolidates the Daily statistical data everyday at 12:30 AM. At the end of every day, the statistical data collected every hour is consolidated and averaged for the day and stored in the Daily table.

Daily to Weekly
During the daily to weekly consolidation, the system consolidates the Weekly statistical data every Sunday at 1:00 AM. At the end of every week, the statistical data collected every day is consolidated and averaged for the week, and stored in the Weekly table.

Daily to Monthly
During the daily to monthly consolidation, the system consolidates the Monthly statistical data on the first day of every month at 2:00 AM. At the end of every month, the statistical data collected every day is consolidated and averaged for the month and stored in the Monthly table.

Device Management

Q. Some of the devices in DCR are not managed in LMS, but the group to which it belongs to, is included in the Auto mode settings. What could be the reason?
A. Check whether these devices are manually excluded from LMS in the Manually Excluded Devices report. If the device you are looking for is available here, then it will not be managed in LMS unless it is manually included.

Q. When I exclude a device, will it get deleted immediately or during next Data Collection?
A. If you are manually excluding a device, it will be immediately deleted from Campus Manager and it will not be managed in further Data Collections.
**Q.** What is the difference between manually excluding a device and deleting a device from Topology Services screen?

**A.** Manually Excluding a Device: If you manually exclude a device, it gets deleted from Campus. Even if you do Data Collection from the neighboring device, it does not get managed in LMS.

Deleting a device from Topology Services screen: If you delete a device from Topology services, and run Data Collection on its neighbor device, the device becomes managed in LMS.

**Q.** I have manually included a device. How do I exclude it?

**A.** Select and exclude that device from the device selector in the Exclude Devices page. Alternatively, you can exclude that device from the Manually Included Devices report.

**Q.** I have manually excluded a device. How do I include it?

**A.** Select and include that device from the device selector in the Include Devices page. Alternatively, you can include that device from Manually Excluded Devices report.

**Q.** When I manually include a device, will it be managed immediately in LMS?

**A.** No. Unless you run Data collection, this will not get managed in LMS.

**Q.** I have both Auto mode and Manual mode enabled. Which one will take higher priority?

**A.** Manual mode always gets higher priority.
Q. I have manually added some devices and started Data collection for all devices. For which devices will Data collection run?
A. Data collection will run for manually added devices and the devices that are already managed in LMS.

Q. I have added n devices in DCR and in that I want to manage only subset of devices in LMS. Is there any way to do this?
A. Either:
   - Manually include those devices and run Data collection.
   Or
   - Create a group in LMS that includes these IP addresses, include the group in Auto mode settings in LMS and run Data Collection.

Q. How to make LMS identify the HSRP devices and perform data collection?
A. To make LMS identify the HSRP devices and perform data collection, do the following:

   **Step 1**
   Add the virtual IP address of the HSRP router as the value for the property “HsrpVirtualIPAddress” in the ANIServer.properties file
   Since there is no UI to specify the virtual IP address, you need to enter it in the ANIServer.properties file.
   When you need to specify multiple virtual IP addresses, separate them with a colon.
   For example:
   ```bash
   HsrpVirtualIPAddress=10.77.210.20:10.77.211.21
   ```

   **Step 2**
   Restart the ANIServer for the changes to take effect.

Q. I have an office with 300 remote branches each with a Cisco router. The routers are connected to the head office over an SP infrastructure and IPSec is used to encrypt the traffic between the remote branches and the head office. How do I manage the devices in the remote network using LMS?
A. If you want to discover and manage the devices in the remote network, add these devices to DCR.

**VRF-Lite**

Q. What is VRF-Lite?
A. VRF-Lite is an application that allows you to pre-provision, provision and monitor Virtual Routing and Forwarding-Lite (VRF-Lite) technology on an enterprise network.

Q. What is Network Virtualization?
A. Virtualization deals with extending a traditional IP routing to a technology that helps companies utilize network resources more effectively and efficiently. Using virtualization, a single physical network can be logically segmented into many logical networks. The virtualization technology supports multiple virtual routing instances of a routing table to exist within a single routing device and work simultaneously.
**Q.** What is VRF-Lite?

**A.** Virtual Routing and Forwarding - Lite (VRF - Lite) is one of the simplest forms of implementing virtualization technology in an Enterprise network. A Virtual Routing and Forwarding is defined as VPN routing/forwarding instance. A VRF consists of an IP Routing table, a derived forwarding table, a set of interfaces that use the forwarding table and set of routing protocols that determine what goes into the forwarding table.

**Q.** What are the pre-requisites to manage a device using VRF-Lite?

**A.** The pre-requisites to manage a device in VRF-Lite are:

1. The device must be managed by Campus Manager.
2. The device must either be L2/L3 or L3 device
3. The devices failing to satisfy pre-requisite # 1 or #2, are not displayed in VRF-Lite.
   
   The device must have the necessary hardware support. For more information on hardware support, see [http://www.cisco.com/en/US/products/sw/cscowork/ps2425/products_device_support_tables_list.html](http://www.cisco.com/en/US/products/sw/cscowork/ps2425/products_device_support_tables_list.html).

   If the device hardware is not supported then the device will be classified as Other devices
4. If a device does not support MPLS VPN MIB, it is classified as a capable device.
5. VTP Server must be support MPLS VPN MIB. If the VTP Server does not support MPLS VPN MIB, VRF-Lite will not manage VTP Clients.

**Q.** The device must be managed by Configuration functionality to exercise all the functionality of VRF-Lite. The desired device is not listed in the device selector for the VRF-Lite configuration workflows. What is the reason for a device not listed in the device selector? Configuration functionality

**A.** A device is not listed in the device selector due to the following reasons:

All VRF-Lite Configuration workflows like Create, Edit, Extend, Delete VRF and Edge VLAN Configuration.

If VRF-Lite Configuration workflow is either Edit VRF, or Delete VRF or Edge VLAN Configuration then a device will not be listed in the Device Selector, if a device is not participating in the selected VRF.

In the Readiness Report, a device listed as a supported device may be because it is not managed by Configuration functionality. You can check if a device is managed by Configuration functionality using the Device Management State Summary.

In Extend VRF workflow, the devices listed in the Device Selector are the devices that are not participating in the selected VRF.

In Edge VLAN Configuration workflow, the devices listed in the Device Selector are only L2/L3 devices that are not participating in the selected VRF.
Q. What are the different categories in which the devices are managed VRF-Lite? Or what criteria are used by VRF-Lite to categorize the devices in the network?

A. VRF-Lite identifies the devices based on the minimum hardware and software support required to configure VRF on the devices.

Based on the available hardware and software support in the devices, VRF-Lite classifies the devices into following categories:

- **VRF Supported Devices** – Represents the devices with required hardware and software support available to configure VRF on the devices.

- **VRF Capable Devices** – Represents the devices with required hardware support available. But the device software must be upgraded to support MPLS VPN MIB. For information on the IOS version that supports MPLS VPN MIB, refer [http://tools.cisco.com/ITDIT/MIBS/MainServlet](http://tools.cisco.com/ITDIT/MIBS/MainServlet).

  VRF-Lite classifies all the devices from Cat 3k and Cat 4k family of devices as VRF Capable devices as these devices do not have the required MPLS VPN MIB support.

- **Other** – Represents the devices without required hardware support to configure VRF. SysOID of the device needs to be checked.
Q. While performing the VRF-Lite Configuration, VRF-Lite application prompts the following messages:

“The device(s) with display name(s) are already locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time or ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

Or

Selected Device(s) are locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time or ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

The above messages appear even if no VRF-Lite configuration is performed parallelly. Why do I get these messages?

A. The VRF-Lite application prompts with these messages when some other configurations are performed simultaneously.

You can check the status of the configuration workflow using Resource Browser. The JOB Id/Owner column will give the details of the workflows currently running in the application.

These messages also appear if any VRF-Lite configuration workflow is abruptly ended or an error has occurred while unlocking the device. You can release the locked devices only after ensuring that no other configuration workflows are running simultaneously. You can release the locked device using the Resource Browser option.

Note

If you unlock a device which is participating in a configuration workflow, the configurations details will be overwritten or corrupted. By default, a lock will be released after two hours.

Q. Sometimes, while performing VRF-Lite configuration, I get the following message:

“The device(s) with display name(s) are already locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time Or Ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

Or

Selected Device(s) are locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time OR Ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

Can I get the details of the user who has locked the devices to perform VRF-Lite configuration?

A. You cannot get the details of user who has locked the devices to perform VRF-Lite configurations.

Q. In the Create, Edit, or Extend workflow, the application do not list the Routing Protocols used while configuring VRF. The Routing Protocol information displayed is NA. What do I need to do to get the routing protocol configurations details?

A. When the Routing Protocol information displayed is NA, it means that the configuration details are not fetched successfully in LMS.
Q. What are the details of the VRF-Lite log files? In which location are the VRF-Lite log files located?

A. The following are the details of the VRF-Lite log files:

1. Vnmserver.log – This log file logs the messages pertaining to the VNMServer process.
2. Vnmcollector.log – This log file logs the messages pertaining to the VRF-Lite collection.
3. Vnmclient.log – This log file logs the messages related to the User Interface.
4. Vnmutils.log – This log file logs the messages pertaining to the utility classes used by VRF-Lite client and server.

The above-mentioned VRF-Lite log files are located in the following location:

In Solaris or Soft Appliance: /var/adm/CSCOpx/log/

In Windows: NMSROOT/logs
Q. What is the reason for VLANs not getting populated in the VLAN to VRF Mapping page in the Create VRF and Extend VRF workflows?

A. The VLAN to VRF Mapping page lists the links connecting the source and the destination device. The VLANs are not listed in fields displaying the links in the VLAN to VRF Mapping page because VRF-Lite tries to find a free VLAN in the devices connected using a link based on the following procedure:

1. An SVI, VRF-Lite searches for free VLANs in the range 1-1005
2. An SI, VRF-Lite searches for free VLANs in the range 1006-4005

Q. Why do I see the VRF description for all VRF(s) in home page as “Discovered by VRF-Lite”?

A. While creating or extending VRF, the description that you have provided is deployed to the selected devices on which VRF is configured. But, the description provided while configuring or extending, is not read by the VRF-Lite application. Instead, the VRF-Lite application provides the default description for all VRFs as “Discovered by VNMServer”. Therefore, the description that you had provided is not displayed in the VRF-Lite home page.

Q. Why are some port-channels not discovered in VRF-Lite?

A. VRF-Lite does not support port-channel and GRE Tunnel. Also, Currently VRF-Lite supports only 802.1Q

Q. What are the processes newly introduced for VRF-Lite?

A. To run VRF-Lite, VNMServer process is newly introduced in the LMS. The VRF-Lite Collector process is executed as a Job.

Q. What is the tested number of devices support in VRF-Lite?

A. In an Enterprise network, VRF-Lite is tested to support the configuration of 32 VRFs with VRF configuration supported in 550 devices in your network. However, at a given time, you can select up to 20 devices and configure VRF using the Create, Edit and Extend VRF workflow.

Q. What are the property files associated with VRF-Lite?

A. The following property files are associated with VRF-Lite:

1. NMSROOT/vnm/conf/VNMClient.properties - This property file is used to provide the settings for Purge and Home page auto Refresh
2. NMSROOT/vnm/conf/VNMServer.properties – This property file is used to provide the SNMP and VNMServer settings.
3. NMSROOT/vnm/conf/VRFCollectorSnmp.conf – This property file stores the SNMP Timeout and Retries that you have configured.
Frequently Asked Questions

Q. In the Interface to VRF Mapping page for the Create, Edit and Extend VRF workflow, why are values for the IP Address and SubnetMask fields empty?
A. If the physical interface that links two devices is not configured with an IP Address, then the IP Address and the SubnetMask fields are empty.

Q. If you configure commands to be deployed to two different devices, will the commands be deployed parallelly or serially?
A. The commands will be deployed to multiple devices parallelly, whereas a series of commands within a single device, will be deployed in serial manner.

Q. Which VRF-Lite configuration jobs that are failed can be retried?
A. You can retry all the VRF-Lite Configuration jobs which are failed. VRF-Lite Configuration jobs are the jobs pertaining to Create, Edit, Extend, Delete VRF and Edge VLAN Configuration workflow.

Q. In the Troubleshooting VRF page, after selecting the source device, no VRFs are listed in the VRF List to troubleshoot. Why?
A. Initially, check if a VRF is configured on the selected source device. The VRF list in the Troubleshooting page enlists the VRF(s) configured in the selected source device as well as in the Global Table, which refers to the global routing table.

Q. Which interfaces are displayed in the Troubleshooting VRF page?
A. When a VRF is selected then all the interfaces that are configured with the selected VRF in the corresponding device is listed.
   If you select VRF as “Global Table”, then the application displays all the interfaces that are not configured to any VRF.
Q. In some scenarios, the VRF configuration commands are pushed to unselected devices. What is the reason?

A. In the following scenarios, the VRF configuration commands are pushed to unselected devices:

The VLANs are created in the VTPServer by default. In any VRF-Lite Configuration workflow, if you create a VLAN in VTP Client devices, then VRF-Lite application finds the corresponding VTP Server and create VLANs in that device.

In Delete VRF workflow, the virtualized interface in the connecting device will also be deleted, even if the device is not selected.

Q. Why the FHRP and DHCP configurations are not shown in VRF-Lite?

A. VRF-Lite does not fetch the details for the FHRP or DHCP configuration from the device. Also, VRF-Lite won’t put the list of vlan(s) allowed on a trunk

The Protocols and DHCP Server details for existing or newly created SVIs are not fetched from the selected devices.

### Troubleshooting LMS

Table 19-2 lists the error messages for LMS workflows.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have not entered a Poller name.</td>
<td>Poller Name field is blank.</td>
<td>Enter a Poller name.</td>
</tr>
<tr>
<td>You have not selected any instances.</td>
<td>You have not selected device instances from the Available Instances tree.</td>
<td>Select one or more device instances.</td>
</tr>
<tr>
<td>The MIB Alias Name field should not be blank.</td>
<td>Alias Name field for the MIB variable is blank. By default, the MIB variable name is shown in the field.</td>
<td>Enter an Alias name. You can assign a descriptive name as the Alias name for the MIB variable. After you have named the MIB variable with an Alias name, the variable appears with this Alias name throughout the application.</td>
</tr>
<tr>
<td>The MIB Alias name contains invalid characters.</td>
<td>The Alias name for the MIB variable contains invalid characters.</td>
<td>Enter a valid Alias name. Enter a name that contain either alphabets or numerals.</td>
</tr>
<tr>
<td>You have not defined a rule.</td>
<td>You have not specified a search criteria in the Advanced Search option.</td>
<td>Use the Advanced Search icon to open the Define Advanced Search Rule window and define a rule for Advanced Search. Define a search rule by applying the criteria, operator, and search expression.</td>
</tr>
<tr>
<td>Threshold Name contains invalid characters.</td>
<td>You have entered invalid characters in the Template Name field.</td>
<td>Enter a valid Threshold name. The Threshold name can contain a combination of alphabets, numerals and special characters (such as -_,#@&amp;$).</td>
</tr>
</tbody>
</table>
## Table 19-2  Error Messages for LMS Workflows (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have entered an invalid E-mail ID.</td>
<td>The format of E-mail ID that you have entered is invalid.</td>
<td>Enter a valid E-mail ID in the format: <a href="mailto:user@domain.com">user@domain.com</a>.</td>
</tr>
<tr>
<td>You have selected a To date that is later than the current date.</td>
<td>The To date that you have selected is later than the current date.</td>
<td>Select a To date that is earlier than or the same as the current date.</td>
</tr>
<tr>
<td>You have not selected a report.</td>
<td>In the Reports page, you have clicked GO without selecting a report from the drop-down list.</td>
<td>1. Select Reports &gt; Report Management. The Report page appears.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select a report from the drop-down list in the report type panel and then click GO.</td>
</tr>
<tr>
<td>You have selected an invalid Start date.</td>
<td>In the Reports page, you have selected the Start Date that is later than the To and current date.</td>
<td>The Start date should be earlier than the To date and the current date.</td>
</tr>
<tr>
<td>You have not selected a template.</td>
<td>You have not selected a template for polling while creating a Poller.</td>
<td>Select a template to poll from the Available Templates list.</td>
</tr>
<tr>
<td>You have entered an invalid value.</td>
<td>You have entered a value in the Last field that is less than one day or in fractions of days.</td>
<td>Enter a valid numeric value greater than 0 and less than or equal to 999. You should not enter fractional values.</td>
</tr>
<tr>
<td>You have entered an invalid From date and time.</td>
<td>You have selected a From date that is later than the To date.</td>
<td>The From date must always be earlier than the To and the current date.</td>
</tr>
<tr>
<td>You have not selected a Poller.</td>
<td>You have not selected a Poller from the Poller Selector.</td>
<td>You must select one or more Pollers from the Poller Selector before clicking the Show MIB Variables button.</td>
</tr>
<tr>
<td>You have not selected any devices.</td>
<td>You have not selected a device from the device selector.</td>
<td>You must select one or more devices from the Device Selector before clicking the Show MIB Variables button.</td>
</tr>
<tr>
<td>Do not enter more than 100 characters for the Report name.</td>
<td>You have entered more than 100 characters for the Report name.</td>
<td>Enter a Report name with less than or equal to 100 characters.</td>
</tr>
<tr>
<td>Enter an OID.</td>
<td>You have not entered OID as the filter string for filtering MIB variables.</td>
<td>Enter an OID as the string to filter the MIB variables.</td>
</tr>
<tr>
<td>You have not selected any thresholds.</td>
<td>You have not selected a threshold from the Threshold Selector.</td>
<td>You must select one or more thresholds from the Threshold Selector before before creating a Threshold Violations Report.</td>
</tr>
<tr>
<td>Cannot delete these jobs.</td>
<td>You have tried to select and delete one or more jobs that are in Running state.</td>
<td>Select only jobs that are in Scheduled, Successful, Partially Successful, Failed, Missed Start or Suspended states. You cannot delete jobs that are in Running state.</td>
</tr>
<tr>
<td>Select Successful jobs to view output.</td>
<td>You have tried to view the output of Scheduled, Failed or Suspended jobs.</td>
<td>You can view the report output of only Successful or Partially Successful jobs.</td>
</tr>
<tr>
<td>You cannot suspend a job that is in a Running state.</td>
<td>You have tried to suspend a job that is in a Running state.</td>
<td>You should suspend only Scheduled jobs.</td>
</tr>
</tbody>
</table>
### Table 19-2  Error Messages for LMS Workflows (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Probable Cause</th>
<th>Possible Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot connect to the database.</td>
<td>Either the UPMDbEngine process is down or the connection pool is exhausted.</td>
<td>Restart the UPMDbEngine process and retry the same operation after sometime, say 5 minutes.</td>
</tr>
<tr>
<td>Job Status Failed</td>
<td>Either: The JRM process is down or the UPMDbEngine or UPMDbMonitor is down.</td>
<td>• If JRM process is down, restart the JRM process.</td>
</tr>
<tr>
<td></td>
<td>Or</td>
<td>• If UPMDbEngine or UPMDbMonitor process is down, restart the process.</td>
</tr>
<tr>
<td></td>
<td>Job details are not available for the job. Check for failure reason.</td>
<td>• Create a similar job and try again.</td>
</tr>
<tr>
<td>You can select files only from /opt/CSCOpx/hum/templateEx, not from any other location.</td>
<td>You have tried to access some other directory path in the Server Side File Browser during template export.</td>
<td>You are allowed to select files only from the following directory path:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In Windows, $SNMSROOT\hum\templateEx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In Solaris or Soft Appliance, $SNMSROOT/hum/templateEx</td>
</tr>
<tr>
<td>$SNMSROOT is the default LMS installation directory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pollers in Active state are not polling.</td>
<td>You are in ACS mode and the System Identity user is not having the required privileges for running LMS tasks.</td>
<td>For running LMS application tasks, the System Identity user needs to have Super Admin privileges in ACS. Update the System Identity user with Super Admin privileges and restart the UPMProcess.</td>
</tr>
<tr>
<td>You cannot schedule multiple jobs to start at the same time. Check the scheduled time for job. You can schedule a maximum of 2 jobs to start at the same time.</td>
<td>You have tried to schedule more than two quick report jobs to run at the same time.</td>
<td>Change the schedule time for the quick report jobs.</td>
</tr>
</tbody>
</table>
Notification MIB

The CISCO-EPM-NOTIFICATION-MIB specifies the trap message format that LMS uses to generate SNMP traps when an alert occurs. The trap includes the attributes of the alert and the events that caused the alert.

This topic includes the following information:

- MIB Definition
- ciscoEpmHealthNotificationAlarm—Definitions of critical variables


MIB Definition

CISCO-EPM-NOTIFICATION-MIB DEFINITIONS ::= BEGIN

IMPORTS
MODULE-IDENTITY,
    NOTIFICATION-TYPE,
    Integer32,
    Unsigned32,
    OBJECT-TYPE,
OBJECT-IDENTITY FROM SNMPv2-SMI
MODULE-COMPLIANCE,
NOTIFICATION-GROUP,
OBJECT-GROUP FROM SNMPv2-CONF
TimeStamp,
RowPointer FROM SNMPv2-TC
SnmpAdminString FROM SNMP-FRAMEWORK-MIB
InetAddressType,
InetAddress FROM INET-ADDRESS-MIB
MIB Definition

Unsigned64 FROM CISCO-TC
ciscoMgmt FROM CISCO-SMI;

ciscoEpmNotificationMIB MODULE-IDENTITY
LAST-UPDATED "200901300000Z"
ORGANIZATION "Cisco Systems, Inc."

DESCRIPTION
"Notifications directly from hardware and software and processed
notifications from various management applications can be further
processed and forwarded by still other management applications to
indicate the status of devices and software (managed objects).
The status of these managed objects can be reported by traps.

The CISCO-EPM-NOTIFICATION-MIB contains the trap structure which
carries the identity and status info of the managed object as
analyzed by such an event processor. It is not possible for
receivers of these traps to query the mib objects.

A unique but optional feature of the application generating the
trap defined in this mib is the ability to contain multiple
partitions in the same system running the application. A
'Partition' is a logical grouping of a set of managed devices.
These devices can belong to only one partition at any given
time. The trap structure will contain information on the exact
partition number and the partition name of the device where it
resides.

The need for trap generation is to enable multiple management
applications in the network to have a consolidated view of the
whole network of Cisco and non-Cisco devices."

REVISION "200901300000Z"

DESCRIPTION
"Added a new Notification ciscoEpmHealthNotificationAlarm to reflect
the status of health and utilization related details of Managed Objects.

Added more attributes which are useful for the new Notification.
Added new oid subtree ciscoEpmNotificationComputedVar under ciscoEpmNotificationMIBObjects to support the computed/derived variables described with cenAlarmMibVariable.

REVISION "200406070000Z"

DESCRIPTION

"Updated the cenAlarmEntry to include new attributes. The new attributes carries information that adds more value to the already existing trap structure.

The Management application computes events for a device via polling snmp mib objects on the device and/or by listening to SNMP Traps. Multiple events on a single device roll up into what is called an Alert - there can be only one alert for a given device at any given time. The objects contained in the cenAlarmEntry are the same for both Alert and Event based notification. The attribute cenAlarmMode added in this revision of the mib can be used to distinguish between the Alert based and event based notification.

In case of event based notification, the cenAlertID would contain the alert id, as computed by the management system, to which the generated event has been rolled up.

Traps generated from systems that support multiple Partition, the cenPartitionNumber and cenPartitionName attributes will carry the exact partition details of the device for which the trap is generated.

Through the management application user interface, the user can customize few attributes of the trap structure. Two attributes included in this mib revision that allows the user to customize each trap sent out are cenCustomerIdentification and cenCustomerRevision.

ciscoEpmNotificationObjectsGroup, ciscoEpmNotificationAlarm, and ciscoEpmNotificationMIBCompliance have been deprecated in this revision.
ciscoEpmNotificationAlarmRev1,
ciscoEpmNotificationAlarmGroupRev1,
ciscoEpmNotificationMIBComplianceRev1,
and ciscoEpmNotificationObjectsGroupRev1 have been newly created in this revision.

REVISION        "200308210000Z"
DESCRIPTION
"Included imports for Integer32, Unsigned32, and NOTIFICATION-GROUP."

REVISION        "200207281420Z"
DESCRIPTION
"Initial version of this MIB."
::= { ciscoMgmt 311 }

-- MIB Object Definitions

ciscoEpmNotificationMIBNotifs OBJECT IDENTIFIER
 ::= { ciscoEpmNotificationMIB 0 }

ciscoEpmNotificationMIBObjects OBJECT IDENTIFIER
 ::= { ciscoEpmNotificationMIB 1 }

ciscoEpmNotificationMIBConform OBJECT IDENTIFIER
 ::= { ciscoEpmNotificationMIB 2 }

cenAlarmData OBJECT IDENTIFIER
 ::= { ciscoEpmNotificationMIBObjects 1 }

ciscoEpmNotificationComputedVar OBJECT IDENTIFIER
 ::= { ciscoEpmNotificationMIBObjects 2 }

cenAlarmTableMaxLength OBJECT-TYPE
  SYNTAX          Unsigned32 (1..4294967295)
  MAX-ACCESS      read-write
  STATUS          current
  DESCRIPTION
"Maximum number of entries permissible in the cenAlarmTable."

DEFVAL { 1 }
::= { cenAlarmData 1 }

cenAlarmTable OBJECT-TYPE
SYNTAX SEQUENCE OF CenAlarmEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "A table containing the device identification and alarm value. The maximum number of entries permissible in this table is defined by cenAlarmTableMaxLength. When the number of entries in the table reaches the maximum limit, the next entry would replace the oldest existing entry in the table."
::= { cenAlarmData 2 }

cenAlarmEntry OBJECT-TYPE
SYNTAX CenAlarmEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "The information regarding a single device status alarm. An entry is created when an alarm is processed."
INDEX { cenAlarmIndex }
::= { cenAlarmTable 1 }

CenAlarmEntry ::= SEQUENCE {
  cenAlarmIndex                    Unsigned32,
  cenAlarmVersion                  SnmpAdminString,
  cenAlarmTimestamp                TimeStamp,
  cenAlarmUpdatedTimestamp         TimeStamp,
  cenAlarmInstanceID               SnmpAdminString,
  cenAlarmStatus                   Integer32,
  cenAlarmStatusDefinition         SnmpAdminString,
  cenAlarmType                     INTEGER,
  cenAlarmCategory                 Integer32,
  cenAlarmCategoryDefinition       SnmpAdminString,
MIB Definition

-- Alarm attributes

cenAlarmIndex OBJECT-TYPE
SYNTAX Unsigned32 (1..4294967295)
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"A monotonically increasing integer for the sole purpose of indexing the attributes in ciscoEpmNotificationMIBObjects. When the maximum value is reached, this value wraps back to 1."
::= { cenAlarmEntry 1 }
Appendix A      Notification MIB

MIB Definition

cenAlarmVersion OBJECT-TYPE
SYNTAX            SnmpAdminString (SIZE  (1..16))
MAX-ACCESS        read-only
STATUS            current
DESCRIPTION
"The release version of this MIB. The version string will
be of the form <major version>.<minorversion>." ::= { cenAlarmEntry 2 }

cenAlarmTimestamp OBJECT-TYPE
SYNTAX            TimeStamp
MAX-ACCESS        read-only
STATUS            current
DESCRIPTION
"The time when the alarm was raised." ::= { cenAlarmEntry 3 }

cenAlarmUpdatedTimestamp OBJECT-TYPE
SYNTAX            TimeStamp
MAX-ACCESS        read-only
STATUS            current
DESCRIPTION
"Alarms persist over time and can have their field(s)
change values. The last time a field(s) changed, this
alarm is updated. The updated time denotes this time.
Each alarm is identified by the unique alarm instance id, cenAlarmInstanceID." ::= { cenAlarmEntry 4 }

cenAlarmInstanceID OBJECT-TYPE
SYNTAX            SnmpAdminString (SIZE  (1..20))
MAX-ACCESS        read-only
STATUS            current
DESCRIPTION
"The Unique Alarm Instance ID." ::= { cenAlarmEntry 5 }

cenAlarmStatus OBJECT-TYPE
SYNTAX          Integer32 (1..250)
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
"The alarm status indicates the status of the alarm
in integer value."
::= { cenAlarmEntry 6 }

cenAlarmStatusDefinition OBJECT-TYPE
SYNTAX          SnmpAdminString (SIZE (1..255))
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
"The short description of the status of the alarm.
The string is formatted in
'\langle integer\rangle,<alarmStatus description>' tuples. The \langle integer\rangle
value is the same value that the 'cenAlarmStatus'
attribute holds. \langle alarmStatus description \rangle contains one line
description of the alarm status generated."
::= { cenAlarmEntry 7 }

cenAlarmType OBJECT-TYPE
SYNTAX          INTEGER  {
    unknown(1),
    direct(2),
    indirect(3),
    mixed(4)
}
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
"unknown: When the value for this attribute could not be
determined.
direct: Denotes an alarm generated by a set of events where
all events are reported by an observation(s) of a
managed object.
indirect: Denotes an alarm generated by a set of events where
all events were deduced or inferred by the status of
managed objects as determined by the network management system.
mixed: Denotes an alarm generated by a set of events which were either direct or indirect.*
::= { cenAlarmEntry 8 }

cenAlarmCategory OBJECT-TYPE
SYNTAX          Integer32 (1..250)
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
"The category of the alarm generated represented in integer value."
::= { cenAlarmEntry 9 }

cenAlarmCategoryDefinition OBJECT-TYPE
SYNTAX          SnmpAdminString (SIZE (1..255))
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
"The short description of the category of the alarm generated. The String is formatted in "<integer>,<alarmCategory description>" tuples. The <integer> value is the same value that the 'cenAlarmCategory' attribute holds. <alarmCategory description> contains one line description of the alarm category generated."
::= { cenAlarmEntry 10 }

cenAlarmServerAddressType OBJECT-TYPE
SYNTAX          InetAddressType
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
"The type of Internet address by which the server is reachable. The Server is the server that is generating this trap."
::= { cenAlarmEntry 11 }
cenAlarmServerAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The IP Address or the DNS name of the Management Server that raised this alarm to be notified."
 ::= { cenAlarmEntry 12 }

cenAlarmManagedObjectClass OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE (1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The class of the managed object for which this alarm was generated. For example, Router, Switch, GateKeeper and VoicePort."
 ::= { cenAlarmEntry 13 }

cenAlarmManagedObjectAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The type of Internet address by which the managed object is reachable."
 ::= { cenAlarmEntry 14 }

cenAlarmManagedObjectAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The IP Address or the DNS name of the Managed Object."
 ::= { cenAlarmEntry 15 }

cenAlarmDescription OBJECT-TYPE
SYNTAX OCTET STRING (SIZE (1..1024))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "A detailed description of the alarm."
 ::= { cenAlarmEntry 16 }

cenAlarmSeverity OBJECT-TYPE
SYNTAX Integer32 (0..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The alarm severity indicates the severity of the alarm
in integer value."
 ::= { cenAlarmEntry 17 }

cenAlarmSeverityDefinition OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE (1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The short description of the severity of the alarm
generated. The String is formatted in
'<integer>,<alarmSeverity description>' tuples. The <integer>
value is the same value that the 'cenAlarmSeverity '
attribute holds. <alarmSeverity description> contains one line
description of the alarm severity generated."
 ::= { cenAlarmEntry 18 }

cenAlarmTriageValue OBJECT-TYPE
SYNTAX Integer32 (0..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The triage value of an alarm is a hierarchical weighting value
(applied by the application, and more importantly customizable
by the end user) to allow an artificial form of evaluating
impact, interest, or other user-determined functions between
alarms. The value is a positive number or zero where zero
denotes an undetermined or uncomputable value."

 ::= { cenAlarmEntry 19 }


cenEventIDList OBJECT-TYPE
SYNTAX OCTET STRING (SIZE (1..1024))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Comma separated list of the Unique Event identifiers that led to the generation of this Alarm."
 ::= { cenAlarmEntry 20 }


cenUserMessage1 OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE (1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"User input message. This value can be configured."
 ::= { cenAlarmEntry 21 }


cenUserMessage2 OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE (1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"User input message. This value can be configured."
 ::= { cenAlarmEntry 22 }


cenUserMessage3 OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE (1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"User input message. This value can be configured."
 ::= { cenAlarmEntry 23 }


cenAlarmMode OBJECT-TYPE
SYNTAX INTEGER {
unknown(1),
alert(2),
event(3)
}
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"unknown: When the value for this attribute could not be
determined.
alert: Denotes an alarm generated by a set of events where
all events are reported by polling of managed
objects and/or listening to SNMP notifications.
event: Denotes an event generated by polling of managed
objects and/or listening to SNMP notifications."
 ::= { cenAlarmEntry 24 }
cenPartitionNumber OBJECT-TYPE
SYNTAX Unsigned32 (0..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"In traps generated by the management application that support
multiple partitions, the attribute will carry the integer
value assigned to identify the logical group where the managed
device resides."
 ::= { cenAlarmEntry 25 }
cenPartitionName OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE (1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"In traps generated by the management application that support
multiple partitions, the attribute will carry the name
assigned to identify the logical group where the managed
device resides."
 ::= { cenAlarmEntry 26 }
cenCustomerIdentification OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE (1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"User input message. The attribute takes in a free format text. This attribute can be used by advanced management applications to sort responses from the fault management server."
::= { cenAlarmEntry 27 }

cenCustomerRevision OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE (1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"User input message. The attribute takes in a free format text. This attribute can be used by advanced management applications to sort responses from the fault management server."
::= { cenAlarmEntry 28 }

cenAlertID OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE (1..20))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"In event based notification, this attribute will contain the alert id to which the generated event has been rolled up to. In alert based notification, the cenAlarmInstanceId and cenAlertID would be identical."
::= { cenAlarmEntry 29 }

cenAlarmObjectId OBJECT-TYPE
SYNTAX OBJECT IDENTIFIER
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"This object represents the identifier of the Object that has exceeded the configured value.

The OIDs populated through this object would represent one of the following kind of Objects.

1) Existing MIB objects that represent a particular statistic like ifInOctets (RFC1213-MIB). The OID of the respective object will be populated.

2) New Objects that are derived out of already-existing objects.

Eg: 'TxUtilization' which is computation of 'ifOutOctets' and 'ifSpeed'. For this kind of variables the OID values are mentioned in this MIB under the subtree ciscoEpmNotificationMIBObjects.ciscoEpmNotificationComputedVar.

::= { cenAlarmEntry 30 }

cenAlarmObjectInstance OBJECT-TYPE
SYNTAX RowPointer
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"This object identifies the instance of the OID populated through cenAlarmObjectId."

::= { cenAlarmEntry 31 }

cenAlarmViolatedValue OBJECT-TYPE
SYNTAX Unsigned32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"This object represents the value of the objectId represented in cenAlarmObjectId when it exceeded the rule represented with cenAlarmDescription."

::= { cenAlarmEntry 32 }
cenAlarmViolatedValueMantissa OBJECT-TYPE
  SYNTAX            Integer32 (0..99)
  MAX-ACCESS       read-only
  STATUS           current
  DESCRIPTION
  "This represents the mantissa part of the violated value. As
  cenAlarmViolatedValue cannot accommodate floating point
  value, this part required to be mentioned separately. This will
  represent the values up to 1/100th of the decimal part."
 ::= { cenAlarmEntry 33 }

cencIfRxUtilization OBJECT-IDENTITY
  STATUS           current
  DESCRIPTION
  "This object represents the incoming data utilization of a low
  speed interface (which is < 20mbps).

  This is calculated as below

  RxUtilization of an interface

  \[ RxUtilization = \frac{\text{ifInOctets} \times 8 \times 100}{\text{ifSpeed}} \]
 ::= { ciscoEpmNotificationComputedVar 1 }

cencIfTxUtilization OBJECT-IDENTITY
  STATUS           current
  DESCRIPTION
  "This object represents the outgoing data utilization of a low
  speed interface (which is < 20mbps).

  This is calculated as below

  TxUtilization of an interface
\[ \text{TxUtilization} = \frac{(\text{ifOutOctets} \times 8 \times 100)}{\text{ifSpeed}} \]

\[ ::= \{ \text{ciscoEpmNotificationComputedVar 2} \} \]

cencMemoryUtilization OBJECT-IDENTITY

STATUS current

DESCRIPTION
"This object represents the memory utilization of different instances (modules) on a managed object as represented in CISCO-MEMORY-POOL-MIB.

Memory utilization of the managed object

\[ \text{Memory Utilization} = \frac{\text{ciscoMemoryPoolUsed}}{\text{ciscoMemoryPoolUsed} + \text{ciscoMemoryPoolFree}} \times 100 \]

\[ ::= \{ \text{ciscoEpmNotificationComputedVar 3} \} \]

cencHrStorageUtilization OBJECT-IDENTITY

STATUS current

DESCRIPTION
"This object represents the memory utilization of different instances (modules) on a managed object as represented in HOST-RESOURCES-MIB.

\[ \text{hrStorageUtilization} = \frac{\text{hrStorageUsed}}{\text{hrStorageSize}} \times 100 \]

\[ ::= \{ \text{ciscoEpmNotificationComputedVar 4} \} \]

cenc64bitIfRxUtilization OBJECT-IDENTITY

STATUS current

DESCRIPTION
"This object represents the incoming data utilization of a high capacity interface (which is > 20mbps).

This is calculated as below

\[ \text{This is calculated as below} \]
64bitRxUtilization = (ifHcInOctets*8*100)/(ifHighSpeed*1000000)

 ::= { ciscoEpmNotificationComputedVar 5 }

cenc64bitIfTxUtilization OBJECT-IDENTITY

 STATUS current

 DESCRIPTION

 "This object represents the outgoing data utilization of a high capacity interface (which is > 20 mbps).

 This is calculated as below

 64bitTxUtilization =
 (ifHcOutOctets*8*100)/(ifHighSpeed*1000000)

 ::= { ciscoEpmNotificationComputedVar 6 }

cencPowerUtilization OBJECT-IDENTITY

 STATUS current

 DESCRIPTION

 "This object represents the power utilization of Power over Ethernet enabled interfaces.

 Power Utilization =
 (pethMainPseConsumptionPower/pethMainPsePower)*100"

 ::= { ciscoEpmNotificationComputedVar 7 }

ciscoEpmNotificationAlarm NOTIFICATION-TYPE

 OBJECTS { cencAlarmVersion,
 cencAlarmTimestamp,
 cencAlarmUpdatedTimestamp,
 cencAlarmInstanceID,
 cencAlarmStatus,
 cencAlarmStatusDefinition,
 cencAlarmType,}
MIB Definition


cenAlarmCategory,
cenAlarmCategoryDefinition,
cenAlarmServerAddressType,
cenAlarmServerAddress,
cenAlarmManagedObjectClass,
cenAlarmManagedObjectAddressType,
cenAlarmManagedObjectAddress,
cenAlarmDescription,
cenAlarmSeverity,
cenAlarmSeverityDefinition,
cenAlarmTriageValue,
cenEventIDList,
cenUserMessage1,
cenUserMessage2,
cenUserMessage3

}  

STATUS  deprecated

DESCRIPTION

"Notification of the status of the managed object as
generated by the management server.

New attributes are added to the ciscoEpmNotificationAlarmRev1.
Hence this notification is deprecated."

::= { ciscoEpmNotificationMIBNotifs 1 }

ciscoEpmNotificationAlarmRev1 NOTIFICATION-TYPE

OBJECTS

{  
cenAlarmVersion,
cenAlarmTimestamp,
cenAlarmUpdatedTimestamp,
cenAlarmInstanceID,
cenAlarmStatus,
cenAlarmStatusDefinition,
cenAlarmType,
cenAlarmCategory,
cenAlarmCategoryDefinition,
cenAlarmServerAddressType,
cenAlarmServerAddress,
ciscoEpmHealthNotificationAlarm NOTIFICATION-TYPE
OBJECTS ( 

  cenAlarmObjectId,
  cenAlarmObjectInstance,
  cenAlarmViolatedValue,
  cenAlarmViolatedValueMantissa,
  cenAlarmTimestamp,
  cenAlarmCategory,
  cenAlarmCategoryDefinition,
  cenAlarmManagedObjectAddressType,
  cenAlarmManagedObjectAddress,
  cenAlarmDescription,
  cenAlarmSeverity,
  cenUserMessage1,
cenAlarmSeverityDefinition

} STATUS current
DESCRIPTION "Notification of details of the violation configured for mib
variables that are monitored by management server."
::= { ciscoEpmNotificationMIBNotifs 3 }

-- Conformance information

ciscoEpmNotificationMIBCompliances OBJECT IDENTIFIER
::= { ciscoEpmNotificationMIBConform 1 }

ciscoEpmNotificationMIBGroups OBJECT IDENTIFIER
::= { ciscoEpmNotificationMIBConform 2 }

-- Compliance

ciscoEpmNotificationMIBCompliance MODULE-COMPLIANCE
STATUS deprecated
DESCRIPTION "The compliance statement for entities which
implement the CISCO-EPM-NOTIFICATION-MIB.

New attributes are included in
 ciscoEpmNotificationMIBComplianceRev1. Hence this object is
deprecated."
MODULE -- this module
MANDATORY-GROUPS {
ciscoEpmNotificationObjectsGroup,
ciscoEpmNotificationAlarmGroup
}

GROUP ciscoEpmAlarmConfigGroup
DESCRIPTION "This group is optional."
OBJECT  cenAlarmTableMaxLength
MIN-ACCESS  read-only
DESCRIPTION
  "Write access is not required."

OBJECT  cenAlarmVersion
MIN-ACCESS  accessible-for-notify
DESCRIPTION
  "Read access is not required."

OBJECT  cenAlarmTimestamp
MIN-ACCESS  accessible-for-notify
DESCRIPTION
  "Read access is not required."

OBJECT  cenAlarmUpdatedTimestamp
MIN-ACCESS  accessible-for-notify
DESCRIPTION
  "Read access is not required."

OBJECT  cenAlarmInstanceID
MIN-ACCESS  accessible-for-notify
DESCRIPTION
  "Read access is not required."

OBJECT  cenAlarmStatus
MIN-ACCESS  accessible-for-notify
DESCRIPTION
  "Read access is not required."

OBJECT  cenAlarmStatusDefinition
MIN-ACCESS  accessible-for-notify
DESCRIPTION
  "Read access is not required."

OBJECT  cenAlarmType
MIN-ACCESS  accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT          cenAlarmCategory
MIN-ACCESS      accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT          cenAlarmCategoryDefinition
MIN-ACCESS      accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT          cenAlarmServerAddressType
MIN-ACCESS      accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT          cenAlarmServerAddress
MIN-ACCESS      accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT          cenAlarmManagedObjectClass
MIN-ACCESS      accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT          cenAlarmManagedObjectAddressType
MIN-ACCESS      accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT          cenAlarmManagedObjectAddress
MIN-ACCESS      accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT          cenAlarmDescription
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmSeverity
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmSeverityDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmTriageValue
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenEventIDList
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenUserMessage1
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenUserMessage2
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenUserMessage3
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."
::= { ciscoEpmNotificationMIBCompliances 1 }

ciscoEpmNotificationMIBComplianceRev1 MODULE-COMPLIANCE

STATUS          current

DESCRIPTION
   "The compliance statement for entities which
   implement the CISCO-EPM-NOTIFICATION-MIB."

MODULE          -- this module

MANDATORY-GROUPS {
   ciscoEpmNotificationObjectsGroupRev1,
   ciscoEpmNotificationAlarmGroupRev1
}

GROUP           ciscoEpmAlarmConfigGroup

DESCRIPTION
   "This group is optional."

OBJECT          cenAlarmTableMaxLength

MIN-ACCESS      read-only

DESCRIPTION
   "Write access is not required."

OBJECT          cenAlarmVersion

MIN-ACCESS      accessible-for-notify

DESCRIPTION
   "Read access is not required."

OBJECT          cenAlarmTimestamp

MIN-ACCESS      accessible-for-notify

DESCRIPTION
   "Read access is not required."

OBJECT          cenAlarmUpdatedTimestamp

MIN-ACCESS      accessible-for-notify

DESCRIPTION
   "Read access is not required."

OBJECT          cenAlarmInstanceID
MIN-ACCESS  accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT  cenAlarmStatus
MIN-ACCESS  accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT  cenAlarmStatusDefinition
MIN-ACCESS  accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT  cenAlarmType
MIN-ACCESS  accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT  cenAlarmCategory
MIN-ACCESS  accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT  cenAlarmCategoryDefinition
MIN-ACCESS  accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT  cenAlarmServerAddressType
MIN-ACCESS  accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT  cenAlarmServerAddress
MIN-ACCESS  accessible-for-notify
DESCRIPTION
"Read access is not required."
OBJECT cenAlarmManagedObjectClass
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmManagedObjectAddressType
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmManagedObjectAddress
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmDescription
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmSeverity
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmSeverityDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenAlarmTriageValue
MIN-ACCESS accessible-for-notify
DESCRIPTION
"Read access is not required."

OBJECT cenEventIDList
MIN-ACCESS accessible-for-notify
DESCRIPTION

"Read access is not required."

OBJECT cenUserMessage1
MIN-ACCESS accessible-for-notify
DESCRIPTION

"Read access is not required."

OBJECT cenUserMessage2
MIN-ACCESS accessible-for-notify
DESCRIPTION

"Read access is not required."

OBJECT cenUserMessage3
MIN-ACCESS accessible-for-notify
DESCRIPTION

"Read access is not required."

OBJECT cenAlarmMode
MIN-ACCESS accessible-for-notify
DESCRIPTION

"Read access is not required."

OBJECT cenPartitionNumber
MIN-ACCESS accessible-for-notify
DESCRIPTION

"Read access is not required."

OBJECT cenPartitionName
MIN-ACCESS accessible-for-notify
DESCRIPTION

"Read access is not required."

OBJECT cenCustomerIdentification
MIN-ACCESS accessible-for-notify
DESCRIPTION

"Read access is not required."
OBJECT                  cenCustomerRevision
MIN-ACCESS              accessible-for-notify
DESCRIPTION             "Read access is not required."

OBJECT                  cenAlertID
MIN-ACCESS              accessible-for-notify
DESCRIPTION             "Read access is not required."
 ::= { ciscoEpmNotificationMIBCompliance 2 }

-- Units of Conformance

ciscoEpmNotificationAlarmGroup NOTIFICATION-GROUP
NOTIFICATIONS           { ciscoEpmNotificationAlarm }
STATUS                  deprecated
DESCRIPTION             "The collection of notifications used to indicate managed object status.

                ciscoEpmNotificationAlarmGroupRev1 is defined. Hence this object is deprecated."
 ::= { ciscoEpmNotificationMIBGroups 1 }

ciscoEpmNotificationObjectsGroup OBJECT-GROUP
OBJECTS                  {
              cenAlarmVersion,  
              cenAlarmTimestamp,  
              cenAlarmUpdatedTimestamp,  
              cenAlarmInstanceID,  
              cenAlarmStatus,  
              cenAlarmStatusDefinition,  
              cenAlarmType,  
              cenAlarmCategory,  
              cenAlarmCategoryDefinition,  
              cenAlarmServerAddressType,  
              cenAlarmServerAddress,  
              cenAlarmManagedObjectClass,
MIB Definition

```
cenAlarmManagedObjectAddressType,
cenAlarmManagedObjectAddress,
cenAlarmDescription,
cenAlarmSeverity,
cenAlarmSeverityDefinition,
cenAlarmTriageValue,
cenEventIDList,
cenUserMessage1,
cenUserMessage2,
cenUserMessage3
}

STATUS          deprecated

DESCRIPTION

"Trap reflecting the alarm. New attributes are added to the new notification
ciscoEpmNotificationObjectsGroupRev1. Hence this object is deprecated."
::= { ciscoEpmNotificationMIBGroups 2 }

ciscoEpmAlarmConfigGroup OBJECT-GROUP

OBJECTS         { cenAlarmTableMaxLength }

STATUS          current

DESCRIPTION

"A collection of objects providing information about the total number of cenAlarmTable entries maintained."
::= { ciscoEpmNotificationMIBGroups 3 }

ciscoEpmNotificationAlarmGroupRev1 NOTIFICATION-GROUP

NOTIFICATIONS    {
    ciscoEpmNotificationAlarmRev1,
    ciscoEpmHealthNotificationAlarm
}

STATUS          current

DESCRIPTION

"The collection of notifications used to indicate managed object status."
Appendix A  Notification MIB

MIB Definition

::= \{ ciscoEpmNotificationMIBGroups 4 \}

ciscoEpmNotificationObjectsGroupRev1 OBJECT-GROUP

OBJECTS {\n   cenAlarmVersion,
   cenAlarmTimestamp,
   cenAlarmUpdatedTimestamp,
   cenAlarmInstanceID,
   cenAlarmStatus,
   cenAlarmStatusDefinition,
   cenAlarmType,
   cenAlarmCategory,
   cenAlarmCategoryDefinition,
   cenAlarmServerAddressType,
   cenAlarmServerAddress,
   cenAlarmManagedObjectClass,
   cenAlarmManagedObjectAddressType,
   cenAlarmManagedObjectAddress,
   cenAlarmDescription,
   cenAlarmSeverity,
   cenAlarmSeverityDefinition,
   cenAlarmTriageValue,
   cenEventIDLlist,
   cenUserMessage1,
   cenUserMessage2,
   cenUserMessage3,
   cenAlarmMode,
   cenPartitionNumber,
   cenPartitionName,
   cenCustomerIdentification,
   cenCustomerRevision,
   cenAlertID,
   cenAlarmObjectId,
   cenAlarmObjectInstance,
   cenAlarmViolatedValue,
   cenAlarmViolatedValueMantissa
\}

STATUS current
ciscoEpmHealthNotificationAlarm—Definitions of critical variables

Table A-1 explains the critical variables that are used by the MIB variable ciscoEpmHealthNotificationAlarm.

<table>
<thead>
<tr>
<th>MIB Variable</th>
<th>Description</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>cenAlarmObjectId</td>
<td>OID of the mib variable that violated the threshold.</td>
<td>For computed variables, the OIDs are defined in the same MIB.</td>
</tr>
<tr>
<td>cenAlarmObjectInstance</td>
<td>Instance of the mib variable that violated the threshold.</td>
<td></td>
</tr>
<tr>
<td>cenAlarmSeverityDefinition</td>
<td>Severity of threshold or Trendwatch.</td>
<td></td>
</tr>
<tr>
<td>cenAlarmCategoryDefinition</td>
<td>Name of the threshold or Trendwatch.</td>
<td></td>
</tr>
<tr>
<td>cenAlarmManagedObjectAddress</td>
<td>Device that violated the threshold.</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B

Processing SNMP Traps

For some SNMP traps, LMS either processes them or treats them as pass-through traps. These traps, and how LMS treats them, are described in these topics:

- Processed SNMP Traps
- Pass-Through SNMP Unidentified Traps
- Unidentified Traps

Processed SNMP Traps

When LMS receives certain SNMP traps, it analyzes the data found in the following fields of each SNMP trap message, and changes the property value of the object property if required:

- Enterprise (the sysObjectID of the agent or object)
- Generic Trap Identifier
- Specific Trap Identifier
- Variable-Bindings
- IP address of the SNMP agent

Note

Use Notification Services to forward specific traps to e-mail recipients or host machines.

All processed traps are forwarded in V1 format. For more information on Processed Traps, see:

- Processed Standard SNMP Traps (RFC 1215)
- Processed CISCO-STACK-MIB Traps
- Processed CISCO-ISDN-MIB Traps
- Processed CISCO-ENTITY-FRU-CONTROL-MIB Trap

Processed Standard SNMP Traps (RFC 1215)

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cold Start</td>
<td>RepeatedRestarts</td>
</tr>
<tr>
<td>Warm Start</td>
<td></td>
</tr>
</tbody>
</table>
Pass-Through SNMP Unidentified Traps

Pass-through traps are the traps that are generated from devices and are not processed by LMS. The traps appear in the alerts and activities page, if they are generated from the devices that are managed by LMS. LMS cannot process these traps and map them to a topology element such as cards and interfaces. However, LMS can forward the traps irrespective of the device state is either managed or unmanaged. Forwarding these traps is controlled using Monitor > Fault Settings > SNMP Traps > Forwarding.

Pass-through traps are displayed as follows:

- As one of the following events:
  - InformAlarm
  - MinorAlarm
  - MajorAlarm
- With the device type and the device name from which it was generated

Pass-through traps will be cleared after a default interval of 10 minutes to one hour. If LMS does not know which device generated the trap, it ignores the trap.

For more information on Pass-Through Traps, see:

- Pass-Through Standard SNMP Traps (RFC 1215)
- Pass-Through CISCO-STACK-MIB Traps
Pass-Through STP Traps
Pass-Through Repeater MIB Traps
Pass-Through CISCO-RHINO-MIB Traps
Pass-Through CISCO-VTP-MIB Traps
Pass-Through CISCO-ENVMON-MIB Traps
Pass-Through CISCO-VLAN-MEMBERSHIP-MIB Traps
Pass-Through CISCO-ACCESS-ENVMON-MIB Traps
Pass-Through CISCO-CONFIG-MAN-MIB Traps
Pass-Through CISCO-ENTITY-FRU-CONTROL-MIB Traps
Pass-Through CISCO-CONTENT-ENGINE-MIB Traps
Pass-Through CISCO-DEVICE-EXCEPTION-REPORTING-MIB Traps
Pass-Through CISCO-RTTMON-MIB Traps
Pass-Through CISCO-VPDN-MGMT-MIB Traps
Pass-Through POWER-ETHERNET-MIB Traps

Pass-Through Standard SNMP Traps (RFC 1215)

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Failure</td>
<td>MinorAlarm</td>
</tr>
</tbody>
</table>

Pass-Through CISCO-STACK-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>lerAlarmOn</td>
<td>MinorAlarm</td>
</tr>
<tr>
<td>lerAlarmOff</td>
<td>MinorAlarm</td>
</tr>
<tr>
<td>ipPermitDeniedTrap</td>
<td>InformAlarm</td>
</tr>
<tr>
<td>sysConfigChangeTrap</td>
<td>InformAlarm</td>
</tr>
</tbody>
</table>

Pass-Through STP Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>STPnewRoot</td>
<td>MajorAlarm</td>
</tr>
<tr>
<td>STPtopologyChange</td>
<td>MinorAlarm</td>
</tr>
</tbody>
</table>

Pass-Through Repeater MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>rptrHealth</td>
<td>MinorAlarm</td>
</tr>
</tbody>
</table>
## Pass-Through SNMP Unidentified Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>rptrGroupChange</td>
<td>InformAlarm</td>
</tr>
<tr>
<td>rptrResetEvent</td>
<td>InformAlarm</td>
</tr>
</tbody>
</table>

### Pass-Through CISCO-RHINO-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>ciscoLS1010ChassisFailureNotification</td>
<td>MajorAlarm</td>
</tr>
<tr>
<td>ciscoLS1010ChassisChangeNotification</td>
<td>InformAlarm</td>
</tr>
</tbody>
</table>

### Pass-Through CISCO-VTP-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>vtpConfigRevNumberError</td>
<td>InformAlarm</td>
</tr>
<tr>
<td>vrtpConfigDigestError</td>
<td>InformAlarm</td>
</tr>
<tr>
<td>vtpServerDisabled</td>
<td>MinorAlarm</td>
</tr>
<tr>
<td>vtpMtuTooBig</td>
<td>MinorAlarm</td>
</tr>
<tr>
<td>vtpVlanRingNumberConfigConflict</td>
<td>MinorAlarm</td>
</tr>
<tr>
<td>vtpVersionOneDeviceDetected</td>
<td>InformAlarm</td>
</tr>
<tr>
<td>vlanTrunkPortDynamicStatusChange</td>
<td>InformAlarm</td>
</tr>
</tbody>
</table>

### Pass-Through CISCO-ENVMON-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>ciscoEnvMonShutdownNotification</td>
<td>InformAlarm</td>
</tr>
</tbody>
</table>

### Pass-Through CISCO-VLAN-MEMBERSHIP-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmVmpsChange</td>
<td>MajorAlarm</td>
</tr>
</tbody>
</table>

### Pass-Through CISCO-ACCESS-ENVMON-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>caemTemperatureNotification</td>
<td>InformAlarm</td>
</tr>
<tr>
<td>caemVoltageNotification</td>
<td>MinorAlarm</td>
</tr>
</tbody>
</table>
Pass-Through CISCO-CONFIG-MAN-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>ciscoConfigManEvent</td>
<td>InformAlarm</td>
</tr>
</tbody>
</table>

Pass-Through CISCO-ENTITY-FRU-CONTROL-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>cevFanONS15540FanTray8</td>
<td>MajorAlarm</td>
</tr>
<tr>
<td>cevPortTransparent</td>
<td>MajorAlarm</td>
</tr>
<tr>
<td>cevPortWave</td>
<td>MajorAlarm</td>
</tr>
</tbody>
</table>

Pass-Through CISCO-CONTENT-ENGINE-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>ciscoContentEngineWriteTransFailed</td>
<td>MajorAlarm</td>
</tr>
<tr>
<td>ciscoContentEngineOverloadBypass</td>
<td>MajorAlarm</td>
</tr>
</tbody>
</table>

Pass-Through CISCO-DEVICE-EXCEPTION-REPORTING-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdrMonitoredExceptionEvent</td>
<td>InformAlarm</td>
</tr>
</tbody>
</table>

Pass-Through CISCO-RTTMON-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonConnectionChangeNotification</td>
<td>InformAlarm</td>
</tr>
<tr>
<td>rttMonTimeoutNotification</td>
<td>InformAlarm</td>
</tr>
<tr>
<td>rttMonThresholdNotification</td>
<td>MajorAlarm</td>
</tr>
<tr>
<td>rttMonVerifyErrorNotification</td>
<td>InformAlarm</td>
</tr>
<tr>
<td>rttMonNotification</td>
<td>MajorAlarm</td>
</tr>
</tbody>
</table>

Pass-Through CISCO-VPDN-MGMT-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>cvpdnNotifSession</td>
<td>MajorAlarm</td>
</tr>
</tbody>
</table>


### Unidentified Traps

LMS may display an event as an Unidentified Trap. Normally an Unidentified Trap is reported when an event occurs on a device that is being discovered by LMS. To get more information on an Unidentified Trap see the corresponding Events page.

For details on clearing unidentified traps see Clearing an Unidentified Trap.

### Clearing an Unidentified Trap

You can manually clear Unidentified Traps from LMS. To do this:

**Step 1**  
Select the Unidentified Trap and click **Clear**.

A message appears prompting you to confirm the clearing.

**Step 2**  
Enter your user ID.

This will be used as a reference to identify who cleared the Unidentified Trap.

**Step 3**  
Click **OK** to confirm.

The Unidentified trap is cleared.

To retain the trap click **Cancel**.

---

### Pass-Through POWER-ETHERNET-MIB Traps

<table>
<thead>
<tr>
<th>SNMP Trap</th>
<th>Corresponding Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>pethMainPowerUsageOnNotification</td>
<td>InformAlarm</td>
</tr>
<tr>
<td>pethMainPowerUsageOffNotification</td>
<td>MajorAlarm</td>
</tr>
</tbody>
</table>
| pethPsePortDetectionStatus                    | • InformAlarm if deliveringPower  
                                              | • MajorAlarm if Others                                  |
Polling—SNMP and ICMP

The topics in this appendix describe the SNMP versions that LMS Fault Manager supports. They also describe how the ICMP and SNMP polling processes that LMS uses work.

The following topics are covered:

- SNMP and ICMP Polling
- How LMS Calculates ICMP Polling Intervals

SNMP and ICMP Polling

These topics describe the polling LMS uses to obtain reachability and network health information:

- ICMP Polling
- SNMP Polling

ICMP Polling

LMS uses a high-performance, asynchronous ICMP poller. The poller uses two threads: one sends polls, and the other receives polls. These separate operations allow polling to continue at a stable rate.

An ICMP poll will determine an element to be in one of three possible states, as shown in Figure C-1: Up, Notification Pending, and Down.

![Figure C-1: Three Possible States of an Element During a Polling Cycle](image)

Up

Notification Pending

Down

[Image of a man sitting on a chair]
When an element in the Up state fails to respond to an ICMP poll, LMS moves it to the Notification Pending state until LMS can determine whether it is up or down.

- The element returns to the Up state when the poll exceeds the maximum success retry count.
- The element is returned to the Up state when it responds to an ICMP poll before the maximum failure entry retry count is exceeded.

If it does not respond in time, it is placed in the Down state. LMS does not poll the element again until the next scheduled polling cycle. An element stays in the Down state until it responds to an ICMP poll.

- When the element responds, LMS changes the status of the element to the Up state.

LMS performs this polling for each managed IP endpoint.

### SNMP Polling

By default, the SNMP poller uses ten synchronous polling threads. The SNMP poller supports the following SNMP versions:

- SNMP V1
- SNMP V2C
- SNMP V3

**Note**

SNMP V3 authentication and encryption pass phrases should not contain any special characters, such as !, @, #, $, %, ^, &, *, due to the limitations in the tool used by fault management to poll devices.

LMS uses a 32-bit counter in its correlation analysis for SNMP V1. For SNMP V2C or V3, LMS uses high-capacity, 64-bit counters. This is critical to avoid *wrapping* which is the overflow of counters between polls—for high-speed data links).

LMS supports polling devices with multiple IP addresses because the SNMP poller supports multiple IP addresses for each SNMP agent. The poller automatically switches to an alternate IP address during failures.

These topics describe SNMP polling in more detail:

- Just-in-Time Polling
- Consolidating Requests to Optimize Polling
- Coordinating ICMP and SNMP Polling

### Just-in-Time Polling

The MIB variable poll list of the SNMP Poller is driven by a Just-In-Time polling algorithm. This algorithm ensures that only those MIB variables needed for correlation are polled. When an element is re-enabled, or comes back up, the variables are automatically polled again.

### Consolidating Requests to Optimize Polling

The SNMP poller consolidates as many attributes as possible into a single SNMP GET request. This consolidation is not restricted to variables from the same SNMP table. The poller continually adapts to changes in the MIB variable poll list.
If the SNMP poller encounters a nonfatal error while consolidating, the SNMP poller responds differently to an SNMP V1 agent than to an SNMP V2C or V3 agent.

This is because an SNMP V1 agent will stop processing a request upon encountering an error, while an SNMP V2C or V3 agent continues processing a request upon encountering an error. (SNMP V2C or V3 agents handle errors on a per-OID basis.)

- If an SNMP V1 agent encounters a nonfatal error during a GET request seeking multiple variables, the SNMP poller suspends the polling of the affected variable. If it continued to poll that variable, the remainder of the request would have to be resent after receiving the error. This could impact SNMP V1 agent performance.

  The SNMP poller continues to poll the unaffected variables. An affected variable is one that, for example, has become unavailable because of a configuration change.

  This enables the SNMP poller to operate efficiently with an SNMP V1 agent during unexpected device configuration changes.

- In contrast, if an SNMP V2C or V3 agent encounters a nonfatal error during a GET request seeking multiple variables, the SNMP poller continues to poll both the affected and unaffected variables.

Coordinating ICMP and SNMP Polling

LMS links its ICMP and SNMP pollers; the SNMP poller will not send requests to any SNMP agent IP address that the ICMP poller has determined is unreachable.

These IP addresses are added to a Do Not Poll list, which the SNMP poller checks before sending SNMP requests. It does not send requests to addresses on this list.

If the SNMP agent has multiple IP addresses, the SNMP poller checks for each address in the Do Not Poll list:

- If an address does not appear on the list, the SNMP poller sends a request to it.
- If all addresses for an agent are on the list, the SNMP poller considers the agent unreachable and temporarily suspends sending SNMP requests to it. As soon as an agent’s IP address becomes responsive (per the ICMP poller), the address is removed from the list, and SNMP polling resumes.

How LMS Calculates ICMP Polling Intervals

LMS calculates ICMP polling intervals for a system (for example, a switch or router) as an offset of the reachability setting’s polling interval for a system.

System reachability is monitored using a combination of ICMP (Ping) requests for IP status and SNMP requests for interface, port, and card status. If a device does not respond to an ICMP poll, it is placed on a Do Not Poll list.

LMS calculates ICMP polling intervals as an offset of the reachability setting’s polling interval for a system. The following is an example of a calculation based on the default value of 240 seconds.

1. LMS calculates the offset using this formula:

   ```c
   offset = 60;
   if (offset > pollingInterval * 0.5) {
     offset = pollingInterval * 0.5;
   }
   ```
2. LMS calculates the ICIM polling interval using this formula:

\[
icimPollingInterval = pollingInterval - offset
\]

Thus, the default polling intervals are as follows:

- ICMP polling interval is 3 minutes.
- SNMP polling interval is 4 minutes.
How LMS Troubleshooting Calculates Repeated Restarts and Flapping

IPM (LMS) uses similar calculations to diagnose both repeated restarts and flapping. LMS considers a system to be restarting repeatedly when it performs too many cold or warm starts over a short period of time.

Table D-1 lists the elements, traps, and user-definable parameters that LMS uses to calculate repeated restarts.

<table>
<thead>
<tr>
<th>Elements</th>
<th>SNMP Traps</th>
<th>Threshold Category</th>
<th>Parameter</th>
<th>Parameter Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>All elements except ports and interfaces</td>
<td>Cold Start</td>
<td>Reachability Settings</td>
<td>Restart trap threshold</td>
<td>Minimum number of SNMP traps required in a user-defined period of time to trigger an event.</td>
</tr>
<tr>
<td></td>
<td>Warm Start</td>
<td></td>
<td>Restart trap window</td>
<td>User-defined period within which minimum number of traps must be received to trigger an event.</td>
</tr>
</tbody>
</table>

LMS considers a network adapter to be flapping when it fluctuates between the Up and Down states too often over a short period of time.

Table D-2 lists the elements, traps, and user-definable parameters LMS uses to diagnose flapping.

<table>
<thead>
<tr>
<th>Elements</th>
<th>SNMP Traps</th>
<th>Threshold Category</th>
<th>Parameter</th>
<th>Parameter Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports and Interfaces</td>
<td>Link Up</td>
<td>Interface/port flapping settings</td>
<td>Link trap threshold</td>
<td>Minimum number of SNMP traps required in a user-defined period of time to trigger an event.</td>
</tr>
<tr>
<td></td>
<td>Link Down</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Link trap window</td>
<td>User-defined period within which minimum number of traps must be received to trigger an event.</td>
</tr>
</tbody>
</table>

After LMS generates a Repeated Restarts event or a Flapping event, LMS computes the stable time. This is the amount of time that must elapse without further traps before LMS declares the element stable again.
The stable time is at least as long as the time the element was at fault, and at least as long as the trap window. However, it can be no longer than one hour.

Figure D-1 illustrates how a system is diagnosed as performing repeated restarts, or how a network adapter is diagnosed as flapping.

In Figure D-1, the trap window (Restart trap window or Link trap window parameter) has a value of 30 seconds. The trap threshold (Restart trap threshold or Link trap threshold parameter) has a value of 2.

LMS performs the following actions:

1. As soon as LMS receives a Link Down Trap from a physical port or interface (or a Warm Start/Cold Start Trap from a system), LMS begins counting the traps.

2. When LMS receives two or more traps within 30 seconds, it considers the network adapter or system to be at fault and LMS generates a Repeated Restarts event or a Flapping event. The minimum traps parameter is set by the Link trap threshold or Restart trap threshold and the minimum seconds parameter is set by the Link trap window or restart trap window. LMS must receive a minimum of two traps within the trap window in a minimum of 30 seconds before it considers an element at fault.

3. LMS continues to receive traps for 80 seconds after the initial trap, resulting in a stable time of 80 seconds. The stable time is the amount of time that LMS waits before it clears the Repeated Restarts event or Flapping event.
Events Processed

Table E-1 lists all possible events you might see in LMS with the following information:

- **Description** — A summary of the event, including typical causes (if known).
- **Trigger** — How Fault Management function learns of the event. This can be either from normal polling, a threshold that was exceeded, or a trap that was received.
- **Severity** — The severity that Fault Management assigns to the event. This can be critical or informational.
- **Device Type** — The devices, as classified in Fault Management, on which the event can occur.
- **Event Code** — The code used by Notification Services to track changes to default LMS event names using the Notification Customization feature. (For more information, see Administration of Cisco Prime LAN Management Solution 4.1.)

Event names correspond to what is displayed in the Description column of the Alerts and Activities Detail page.

The events a device can report are determined by the device function.

**Table E-1  Events that the Fault Management Functions Supports**

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>BackupActivated</td>
<td>Description: Backup port or interface has come online, indicating that the port or interface it backs up has gone down.</td>
</tr>
<tr>
<td></td>
<td>Trigger: Polling.</td>
</tr>
<tr>
<td></td>
<td>Severity: Critical.</td>
</tr>
<tr>
<td></td>
<td>Device Type: All.</td>
</tr>
<tr>
<td></td>
<td>Event Code: 1000.</td>
</tr>
<tr>
<td></td>
<td>Component Codes:</td>
</tr>
<tr>
<td></td>
<td>- Port: 1009.</td>
</tr>
<tr>
<td></td>
<td>- Interface: 1008.</td>
</tr>
<tr>
<td></td>
<td>- On any other Component: 1007.</td>
</tr>
</tbody>
</table>
### Table E-1  Events that the Fault Management Functions Supports (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
</table>
| Duplicate           | Description: Same IP address is configured on multiple managed systems.  
                      | Trigger: Polling (often during rediscovery).  
                      | Severity: Critical.  
                      | Device Type: All.  
                      | Event Code: 1001.  
                      | Component Codes:  
                      | • Duplicate IP: 1025.  
                      | • On any other Component: 1024. |
| ExceededMaximumUptime| Description: A backup or dial-on-demand port or interface has been in the Up state for a long time.  
                      | Trigger: Exceeded Maximum uptime threshold.  
                      | Severity: Critical.  
                      | Device Type: All (except Network Management).  
                      | Event Code: 1002.  
                      | Component Codes:  
                      | • Port: 1028.  
                      | • Interface: 1027.  
                      | • On any other Component: 1026. |
| ExcessiveFragmentation| Description: System memory is highly fragmented.  
                      | Trigger: Exceeded Memory fragmentation threshold.  
                      | Severity: Critical.  
                      | Device Type: All.  
                      | Event Code: 1003.  
                      | Component Codes:  
                      | • Memory: 1030.  
                      | • On any other Component: 1029. |
### Flapping

**Description:** Port or interface repeatedly alternates between Up and Down states over a short period of time.

It displays this event by monitoring the number of link downs received within the link window for a particular network adapter (using the Link threshold and Link Window parameters).

**Trigger:** Exceeded Link trap threshold for Link trap window; or processed trap (see Processed SNMP Traps, and How LMS Troubleshooting Calculates Repeated Restarts and Flapping).

**Severity:** Critical.

**Device Type:** All.

**Event Code:** 1004.

**Component Codes:**
- Port: 1033.
- Interface: 1032.
- On any other Component: 1031.

---

### HighBackplaneUtilization

**Description:** Utilization of the backplane bandwidth exceeds the Backplane utilization threshold.

**Trigger:** Exceeded Backplane utilization threshold.

**Severity:** Critical.

**Device Type:** All.

**Event Code:** 1005.

**Component Codes:**
- Chassis: 1035.
- On any other Component: 1034.

---

### HighBroadcastRate

**Description:** Input packet broadcast percentage exceeds the Broadcast threshold.

The input packet broadcast percentage calculates the percentage of total capacity that was used to receive broadcast packets.

**Trigger:** Exceeded Broadcast threshold.

**Severity:** Critical.

**Device Type:** All.

**Event Code:** 1006.

**Component Codes:**
- Port: 1038.
- Interface: 1037.
- On any other Component: 1036.

---
### Table E-1 Events that the Fault Management Functions Supports (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>HighBufferMissRate</td>
<td>Description: Rate of buffer misses exceeds the Memory buffer miss threshold.</td>
</tr>
<tr>
<td></td>
<td>Trigger: Exceeded Memory buffer miss threshold.</td>
</tr>
<tr>
<td></td>
<td>Severity: Critical.</td>
</tr>
<tr>
<td></td>
<td>Device Type: All.</td>
</tr>
<tr>
<td></td>
<td>Event Code: 1007.</td>
</tr>
<tr>
<td></td>
<td>Component Codes:</td>
</tr>
<tr>
<td></td>
<td>• Memory: 1040.</td>
</tr>
<tr>
<td></td>
<td>• On any other Component: 1039.</td>
</tr>
<tr>
<td>HighBufferUtilization</td>
<td>Description: Number of buffers used exceeds the Memory buffer utilization threshold.</td>
</tr>
<tr>
<td></td>
<td>Trigger: Exceeded Memory buffer utilization threshold.</td>
</tr>
<tr>
<td></td>
<td>Severity: Critical.</td>
</tr>
<tr>
<td></td>
<td>Device Type: All.</td>
</tr>
<tr>
<td></td>
<td>Event Code: 1008.</td>
</tr>
<tr>
<td></td>
<td>Component Codes:</td>
</tr>
<tr>
<td></td>
<td>• Memory: 1042.</td>
</tr>
<tr>
<td></td>
<td>• On any other Component: 1041.</td>
</tr>
</tbody>
</table>
### Table E-1 Events that the Fault Management Functions Supports (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
</table>
| HighCollisionRate | Description: Rate of collisions exceeds the Collision threshold. HighCollisionRate Event occurs if NetworkAdapterOperational && CollisionThreshold < 100 check (OutputPacketRate > 0) && (CollisionRate > MinimumCollisionRate) && (CollisionPct > CollisionThreshold); OutputPacketRate is calculated as: OutputPacketRate = rate(ifOutUcastPkts, PollingInterval) + rate(ifOutNUcastPkts, PollingInterval) CollisionRate is calculated as: CollisionRate = rate(dot3StatsSingleCollisionFrames, PollingInterval) + rate(dot3StatsMultipleCollisionFrames, PollingInterval) + rate(dot3StatsExcessiveCollisions, PollingInterval) or CollisionRate = rate(locIfCollisions, PollingInterval) Minimum collision rate is calculated as: MinimumCollisionRate = ((MaxSpeed > 0 && MaxTransferUnit > 0) * (my_MaxSpeed / (MaxTransferUnit+0.001) / 8) * 0.1) + ((MaxSpeed == 0 || MaxTransferUnit == 0) * 50) CollisionPct is calculated as: CollisionPct = CollisionRate / OutputPacketsSentRate OutputPacketsSentRate is calculated as: OutputPacketsSentRate = rate(ifOutUcastPkts, PollingInterval) + rate(ifOutNUcastPkts, PollingInterval) - rate(ifOutErrors, PollingInterval) - rate(ifOutDiscards, PollingInterval) CollisionThreshold = 10 Trigger: Exceeded Collision threshold. Severity: Critical. Device Type: All. Event Code: 1009. Component Codes:  
  - Port: 1045.  
  - Interface: 1044.  
  - On any other Component: 1043.
### Event Description, Cause, Severity, and Event Code

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HighDiscardRate</strong></td>
<td>Description: A HighDiscardRate event occurs when:</td>
</tr>
<tr>
<td></td>
<td>• The input packet queued rate is greater than the minimum</td>
</tr>
<tr>
<td></td>
<td>packet rate, and the input packet discard percentage is greater</td>
</tr>
<tr>
<td></td>
<td>than the Discard threshold.</td>
</tr>
<tr>
<td></td>
<td>The input packet queued rate is the rate of packets received without error.</td>
</tr>
<tr>
<td></td>
<td>The input packet discard percentage is calculated by dividing the rate of</td>
</tr>
<tr>
<td></td>
<td>input packets discarded by the rate of packets received.</td>
</tr>
<tr>
<td></td>
<td>• The output packet queued rate is greater than the minimum</td>
</tr>
<tr>
<td></td>
<td>packet rate, and the output packet discard percentage is greater</td>
</tr>
<tr>
<td></td>
<td>than the Discard threshold.</td>
</tr>
<tr>
<td></td>
<td>The output packet queued rate is the rate of packets sent without error.</td>
</tr>
<tr>
<td></td>
<td>The output packet discard percentage is calculated by dividing the rate of</td>
</tr>
<tr>
<td></td>
<td>output packets discarded by the rate of packets sent.</td>
</tr>
<tr>
<td>Trigger</td>
<td>Exceeded Discard threshold.</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Device Type</td>
<td>All.</td>
</tr>
<tr>
<td>Event Code</td>
<td>1010.</td>
</tr>
<tr>
<td>Component Codes</td>
<td>• Port: 1048.</td>
</tr>
<tr>
<td></td>
<td>• Interface: 1047.</td>
</tr>
<tr>
<td></td>
<td>• On any other Component: 1046.</td>
</tr>
</tbody>
</table>

<p>| <strong>HighErrorRate</strong>    | Description: A HighErrorRate event occurs for input or output packets when  |
|                      |   both of the following thresholds are exceeded:                            |
|                      | • Error threshold—Percentage of packets in error                            |
|                      | • Error traffic threshold—Percentage of bandwidth in use                   |
| Trigger              | Exceeded Error threshold and equaled or exceeded Error traffic threshold.   |
| Severity             | Critical                                                                     |
| Device Type          | All.                                                                         |
| Event Code           | 1011.                                                                       |
| Component Codes      | • Port: 1051.                                                                |
|                      | • Interface: 1050.                                                          |
|                      | • On any other Component: 1049.                                             |</p>
<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
</table>
| HighQueueDropRate     | Description: Number of packets discarded due to input or output queue overflow exceeding the Queue drop threshold.  
The input (or output) queue overflow is derived by dividing the number of packets designated to be sent (or received) that were discarded due to queue overflow, by the total number of packets in the queue.  
Trigger: Exceeded Queue drop threshold.  
Severity: Critical.  
Device Type: All.  
Event Code: 1012.  
Component Codes:  
  • Port: 1054.  
  • Interface: 1053.  
  • On any other Component: 1052. |
| HighUtilization       | Description: Current utilization exceeds the utilization threshold configured for an element.  
Trigger: Exceeded one of these thresholds:  
  • Processor utilization (processor and memory settings)  
  • Utilization (interface settings)  
Severity: Critical.  
Device Type: All.  
Event Code: 1013.  
Component Codes:  
  • Processor: 1058.  
  • Port: 1057.  
  • Interface: 1056.  
  • On any other Component: 1055. |
### Table E-1: Events that the Fault Management Functions Supports (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>InformAlarm</td>
<td>Description: An information pass-through trap was generated. Trigger: Pass-through trap. See Pass-Through SNMP Unidentified Traps. Severity: Informational. Device Type: All. Event Code: 1014. Component Codes:</td>
</tr>
<tr>
<td></td>
<td>• Syslog Event: 1062.</td>
</tr>
<tr>
<td></td>
<td>• SNMP Trap: 1061.</td>
</tr>
<tr>
<td></td>
<td>• Event: 1060.</td>
</tr>
<tr>
<td></td>
<td>• On any other Component: 1059.</td>
</tr>
<tr>
<td>InsufficientFreeMemory</td>
<td>Description: System is running out of memory resources. Also reported if a buffer could not be allocated because of insufficient memory. Trigger: Exceeded Free memory threshold. Severity: Critical. Device Type: All. Event Code: 1015. Component Codes:</td>
</tr>
<tr>
<td></td>
<td>• Memory: 1064.</td>
</tr>
<tr>
<td></td>
<td>• On any other Component: 1063.</td>
</tr>
<tr>
<td>MajorAlarm</td>
<td>Description: Critical pass-through trap was generated. Trigger: Pass-through trap. See Pass-Through SNMP Unidentified Traps. Severity: Informational. Device Type: All. Event Code: 1016. Component Codes:</td>
</tr>
<tr>
<td></td>
<td>• Syslog Event: 1067.</td>
</tr>
<tr>
<td></td>
<td>• SNMP Trap: 1066.</td>
</tr>
<tr>
<td></td>
<td>• Event: 1065.</td>
</tr>
<tr>
<td></td>
<td>• On any other Component: 1064.</td>
</tr>
</tbody>
</table>
### Table E-1  Events that the Fault Management Functions Supports (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
</table>
| MinorAlarm    | Description: Significant pass-through trap was generated.  
                Trigger: Pass-through trap. See Pass-Through SNMP Unidentified Traps.  
                Severity: Informational.  
                Device Type: All.  
                Event Code: 1017.  
                Component Codes:  
                • Syslog Event: 1071.  
                • SNMP Trap: 1070.  
                • Event: 1069.  
                • On any other Component: 1068. |
| OperationallyDown | Description:  
                         Interface— Operational state of a card or network adapter is not normal.  
                         System Hardware—Disk’s operational state is not normal.  
                         Trigger: Polling, or processed trap (see Processed SNMP Traps).  
                         For interfaces, LMS will only generate an OperationallyDown clear event if the card is reinserted into the same slot, and if the module index is the same before and after the card is reinserted.  
                         Severity: Critical.  
                         Device Type: All.  
                         Event Code: 1018.  
                         Component Codes:  
                         • Disk: 1077.  
                         • Port: 1076.  
                         • Interface: 1075.  
                         • Chassis: 1074.  
                         • Card: 1073.  
                         • On any other Component: 1072. |
<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
</table>
| OutofRange    | Description: Device temperature or voltage is outside the normal operating range. When an OutofRange event is generated, you will normally also see fan, power supply, or temperature events. Trigger: Exceeded one of these thresholds:  
  • Relative temperature threshold  
  • Relative voltage threshold  
 Severity: Critical.  
 Device Type: All.  
 Event Code: 1019.  
 Component Codes:  
  • Voltage Sensor: 1080.  
  • Temperature Sensor: 1079.  
  • On any other Component: 1078. |
| RepeatedRestarts | Description: System repeatedly restarts over a short period of time. LMS issues this event. It does this by monitoring the number of system cold and warm starts received within the restart window (using the Restart threshold and the RestartWindow parameters). Trigger: Exceeded Restart trap threshold for Restart trap window; or processed trap (see Processed SNMP Traps, and How LMS Troubleshooting Calculates Repeated Restarts and Flapping).  
 Severity: Critical.  
 Device Type: All.  
 Event Code: 1020.  
 Component Codes:  
  • SNMP Agent: 1082.  
  • On any other Component: 1081. |
Table E-1  Events that the Fault Management Functions Supports (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
</table>
| StateNotNormal   | Description: A fan, power supply, temperature sensor, or voltage sensor is not acting normally. When an OutofRange event is generated, you will also see a fan, power supply, or temperature event. Trigger: Polling. Severity: Critical. Device Type: All. Event Code: 1021. Component Codes:  
|                  | • Fan: 1088.                                                                                                   |
|                  | • Temperature Sensor: 1087.                                                                                    |
|                  | • Voltage Sensor: 1086.                                                                                        |
|                  | • Power Supply: 1085.                                                                                          |
|                  | • PowerSupply_Fault_CiscoStack: 1084.                                                                           |
|                  | • On any other Component: 1083.                                                                                 |
### Events that the Fault Management Functions Supports (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description, Cause, Severity, and Event Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unresponsive</td>
<td>Description: Device does not respond to ICMP or SNMP requests. Probable causes are:&lt;br&gt;• On a system: ICMP Ping requests and SNMP queries to the device timeout received no response.&lt;br&gt;• On an SNMP Agent: Device ICMP ping requests are successful, but SNMP requests time out with no response.&lt;br&gt;A system might also be reported as Unresponsive if the only link (for example, an interface) to the system goes down.&lt;br&gt;Trigger: Polling.&lt;br&gt;Severity: Critical.&lt;br&gt;Device Type: All.&lt;br&gt;Event Code: 1022.&lt;br&gt;Component Codes:&lt;br&gt;• Router: 1101.&lt;br&gt;• SNMP Agent: 1100.&lt;br&gt;• Incharge Broker: 1099.&lt;br&gt;• IP: 1098.&lt;br&gt;• Hub: 1097.&lt;br&gt;• Host: 1096.&lt;br&gt;• HTTP Service: 1095.&lt;br&gt;• FTP Service: 1094.&lt;br&gt;• Duplicate IP: 1093.&lt;br&gt;• DLCI: 1092.&lt;br&gt;• Bridge: 1091.&lt;br&gt;• Application: 1090.&lt;br&gt;• On any other Component: 1089.</td>
</tr>
<tr>
<td>Suspended</td>
<td>Description: Device moved to Suspend state.&lt;br&gt;Trigger: When user moves the device to Suspend state.&lt;br&gt;Severity: Informational.&lt;br&gt;Device Type: All.&lt;br&gt;Event Code: 1023.&lt;br&gt;Component Codes: Not Applicable.</td>
</tr>
<tr>
<td>Event</td>
<td>Description, Cause, Severity, and Event Code</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Resumed</td>
<td>Description: Device moved to Resumed state from the Suspended state.</td>
</tr>
<tr>
<td></td>
<td>Trigger: When the user moves the device to Resumed state.</td>
</tr>
<tr>
<td></td>
<td>Severity: Informational.</td>
</tr>
<tr>
<td></td>
<td>Device Type: All.</td>
</tr>
<tr>
<td></td>
<td>Event Code: 1024.</td>
</tr>
<tr>
<td></td>
<td>Component Codes: Not Applicable.</td>
</tr>
<tr>
<td>SwitchOver</td>
<td>Description: When a supervisor failover occurs on Cat4500 platforms, a trap is sent by the standby supervisor when it becomes active.</td>
</tr>
<tr>
<td></td>
<td>LMS respond to this by creating a Supervisor SwitchOver event.</td>
</tr>
<tr>
<td></td>
<td>Trigger: On Polling.</td>
</tr>
<tr>
<td></td>
<td>Severity: Critical.</td>
</tr>
<tr>
<td></td>
<td>Device Type: All.</td>
</tr>
<tr>
<td></td>
<td>Event Code: 1025.</td>
</tr>
<tr>
<td></td>
<td>Component Codes: Not Applicable.</td>
</tr>
<tr>
<td>ManualClear</td>
<td>Description: Clearing the events manually by the user.</td>
</tr>
<tr>
<td></td>
<td>Trigger: When user clears the event from Fault Monitor UI.</td>
</tr>
<tr>
<td></td>
<td>Severity: Informational.</td>
</tr>
<tr>
<td></td>
<td>Device Type: All.</td>
</tr>
<tr>
<td></td>
<td>Event Code: 1026.</td>
</tr>
<tr>
<td></td>
<td>Component Codes: Not Applicable.</td>
</tr>
</tbody>
</table>
LMS Monitoring and Troubleshooting polls certain MIBs for information that is relevant to fault management. Polling is done based on the polling interval, as described in the Administration of Cisco Prime LAN Management Solution 4.1 User Guide.

Obtaining MIB information depends on several contingencies, such as whether a device supports a MIB, has the proper SNMP implementation, is accessible, and so forth.

LMS polls the following MIBs:

- POWER-ETHERNET-MIB
- ALTIGA-GENERAL-STATS-MIB
- AIRESPACE-SWITCHING-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- OLD-CISCO-CHASSIS-MIB-V1SMI
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-SENSOR-MIB
- ONS15501-MIB
- CHASSISMGREXT-MIB
- AIRESPACE-WIRELESS-MIB
- CISCO-VPDN-MGMT-MIB
- CISCO-RTTMON-MIB
- ALTIGA-HARDWARE-STATS-MIB
- CISCO-CONENT-ENGINE-MIB
- CISCO-ENVMON-MIB
- CISCO-FC-FE-MIB
- CISCO-FLASH-MIB
- CISCO-FRAME-RELAY-MIB
- CISCO-ISDN-MIB
- CISCO-LS1010-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-METRO-PHY-MIB
- CISCO-PAGP-MIB
- CISCO-PROCESS-MIB
- CISCO-RHINO-MIB
- CISCO-STACK-MIB
- CISCO-SYSTEM-EXT-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VOICE-APPS-MIB
- CISCO-VTP-MIB
- CPQHLTH-MIB
- CPQHOST-MIB
- CPQNIC-MIB
- CPQSIINFO-MIB
- CPQSM2-MIB
- ENTITY-FRU-CONTROL-MIB
- ENTITY-MIB
- ETHERLIKE-MIB
- HOST-RESOURCES-MIB (RFC 1514)
- IF-MIB (RFC 1493)
- IF-MIB (RFC 1573)
- MIB-II (RFC 1213)
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-CPU-MIB
- OLD-CISCO-ENV-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-MEMORY-MIB
- OLD-CISCO-MEMORY-POOL-MIB
- OLD-CISCO-SYSTEM-MIB
- SYS-APPL-MIB
- TOPSPIN_MIB
- UMSASSETID-MIB
- UMSEVENT-MIB
- UMSEVENT-MIB
- UMSLMSSENSOR-MIB
INDEX

A

access ports
  managing and unmanaging  3-28
  overriding groups  3-11
polling and thresholds  3-2, 3-14
polling categories  3-15
previewing thresholds  2-3
threshold categories  2-8
viewing thresholds  2-2
acknowledging
  events, from events display  9-9
Alerts and Events display
  layout  9-3
  tool buttons on  9-16
alerts and events display
  number of records viewable  9-3
ANI discover metrics, displaying  7-76
applications
  NetShow  10-1
application servers, working with  7-71
Apply Changes page  3-22
Archiving netshow job output
  argument
    function-dependent  18-4
    function-specific  18-4
arguments  18-3
  function-independent  18-4
  mandatory  18-3

B

BackupActivated  £-1

Bandwidth Utilization  7-40
Bandwidth Utilization
  enabling RMON  7-43

C

cautions regarding Cisco Visio stencil file names, changing  7-55
CiscoView, starting
  from VLAN Port Assignment  7-67
Cisco Visio stencil file, downloading  7-55
clearing
  alerts, timing of  9-5
  events, from events display  9-7, 9-9
cli commands  18-1
  ipm addadhoctarget  18-17
  ipm baseline  18-18
  ipm controlcollector  18-8
  ipm deletedevice  18-17
  ipm deletereports  18-16
  ipm export  18-12
  ipm exportstats  18-15
  ipm generatereports  18-16
  ipm -help  18-6, 18-7, 18-18
  ipm importcollector  18-9
  ipm listcollectors  18-9
collector
  configuring  15-9
  deleting  15-23
  editing  15-23
  export  15-27
  filtering  15-18
  import  15-30
license information 15-6
monitor 15-33
overlay 15-24
real-time graph 15-33
sorting 15-21
specifying operations 15-8
specifying source device 15-7
specifying target device 15-8
start 15-35
stopping 15-34
viewing details 15-21
collector management 15-1
understanding 15-1
collector status 15-3
command reference 18-1
configuring collector 15-9
creating collector 15-9
creating
user-defined operation 16-9
Creating netshow jobs 10-7
customizable groups 3-3

D

defining
call setup 16-39
DHCP 16-44
DLSW 16-50
DNS 16-43
echo 16-26
Ethernet Jitter 16-55
Ethernet Jitter Auto IP SLA 16-58
Ethernet Ping 16-53
Ethernet Ping Auto IP SLA 16-56
FTP 16-48
gatekeeper registration delay 16-41, 16-42
HTTP 16-46
ICMP jitter 16-32
path echo 16-27
RTP 16-37, 16-60
TCP connect 16-51
UDP echo 16-30
UDP jitter 16-34
deleting
collector 15-23
operation 16-22
Device Center
devices
overriding groups 3-11
polling and thresholds 3-14
syslog messages for, not getting 19-9
devices, working with 7-62
(see also MLS devices) 7-69
device attributes, working with | 7-64
device labels
  clearing | 7-63
  displaying | 7-63
device tooltips, interpreting | 7-63, 7-64
device service modules, displaying | 7-72
duplexity, interface | 2-12
DuplexMode | 2-12
DuplexSource | 2-12
Duplicate (event) | E-2

**E**

Edge VLAN Configuration
  At Access Layer with Trunk | 7-30
editing
  collector | 15-23
  device attributes | 14-4
  operation | 16-21
eem
  about EEM | 12-1
  configure
    embedded event manager | 12-9
    environmental variables | 12-6
  EEM action types | 12-2
  EEM components | 12-2
  EEM NetConfig tasks | 12-3
    EEM environmental variable task | 12-3
    embedded event manager task | 12-4
  Configuration NetShow commands | 12-14
  Configuration reports | 12-12
  Configuration support for EEM | 12-3
  configure EEM | 12-5
  events
    changing names | E-1
    thresholds and | 2-15
  ExceededMaximumUptime | 2-15, E-2
  ExcessiveFragmentation | 2-15, E-2
  export collector | 15-27

**F**

FAQ
  CLI commands | 19-38
  collectors | 19-35
  devices | 19-31
  general | 19-26
  operations | 19-33
Fault Summary tab, description | 9-3, 9-14
Flapping | 2-15, E-3

**G**

gold
  about GOLD | 13-1
  configure
    GOLD tests
diagnostics
    boot up | 13-2
    runtime monitoring | 13-2
  GOLD test in Configuration | 13-3
  NetConfig tasks for GOLD | 13-3
    GOLD boot level task | 13-3
    GOLD monitoring test task | 13-4
types of diagnostics | 13-2
graph
  overlay | 15-24
  real time | 15-33
groups
  customizable | 3-3
  overriding (polling and thresholds) | 3-13

**H**

HighBackplaneUtilization | 2-15, E-3
HighBroadcastRate | 2-15, E-3
HighBufferMissRate | 2-15, E-4
HighBufferUtilization | 2-15, E-4
HighCollisionRate | 2-15, E-5
HighDiscardRate  2-15, E-6
HighErrorRate  2-15, E-6
HighQueueDropRate  2-15, E-7
HighUtilization  2-15, E-7
HP OpenView  3-24

ICMP polling
  intervals  C-3
  overview  C-1
SNMP polling and  C-3
IEEE 802.1Q, VLAN trunking protocol  7-87
import collector  15-30
import DCR devices
  automatic  14-3
InformAlarm  E-8
input file format  18-5
Instance Selector  4-10
  Advanced Search  4-10
  Simple Search  4-10, 4-26
InsufficientFreeMemory  2-15, E-8
interfaces
  managing and unmanaging  3-28
  overriding groups  3-11
  polling and thresholds  3-14
  polling categories  3-15
  previewing thresholds  2-3
  threshold categories  2-8
  viewing thresholds  2-2
IP addresses, managing and unmanaging  3-28
IPSLA cli commands  18-6
IPSLA portlets
  Availability Dashboard  6-14
  Collector Information  6-37
  Device Categorization  6-38
  Highest Jitter  6-12
  Highest Latency  6-11
  IPSLA Lowest Availability  6-13
Violation Summary  6-9
ISL (Inter-Switch Link), VLAN trunking protocol  7-86

License
  collector  15-6
  devices  14-4
listing collectors
  system-defined groups  15-17, 15-20
  user-defined groups  15-17, 15-21

Managing Pollers  4-2
  Activating a Poller  4-14
  Clearing Failures  4-16
  Clearing Missed Cycles  4-15
  Creating a Poller  4-4
  Deactivating a Poller  4-13
  Deleting a Poller  4-13
  Editing a Poller  4-11
  Filtering Pollers  4-17
  Selecting Instances  4-17
  Viewing Failures  4-14
    Permanent  4-15
    Transient  4-15
  Viewing Poller Configuration  4-16
Managing Templates  4-19
  Copying a Template  4-28
  Creating a Template  4-24
  Deleting a Template  4-27
  Editing a Template  4-26
  Exporting a Template  4-28
Filtering Templates 4-30
Importing a Template 4-29
System-defined Templates 4-19
User-defined Templates 4-23
Viewing a Template 4-31

Masking credentials of show commands 10-7
measuring network performance
call setup 16-39
DHCP 16-44
DLSW 16-49
DNS 16-42
echo 16-25
Ethernet Jitter 16-54
Ethernet Jitter Auto IP SLA 16-57
Ethernet Ping 16-53
Ethernet Ping Auto IP SLA 16-56
FTP 16-47
gatekeeper registration delay 16-41
HTTP 16-45
ICMP jitter 16-31
IP 16-24
path echo 16-27
RTP 16-37
TCP connect 16-51
UDP echo 16-28
UDP jitter 16-33
memory, managing and unmanaging 3-28
MIBs
pass-through SNMP traps B-2
processed SNMP traps B-1
MIBs polled F-1
MinorAlarm E-9
Missed Cycles 4-3
MLS devices, working with 7-69
MLS reports, displaying 7-70
MLS reports, interpreting 7-70
Route Processors report 7-70
Switching Engines report 7-71

NetShow
adding and deleting adhoc commands 10-22
archiving job output 10-15
Commands
adding and deleting adhoc commands 10-22
custom command execution privilege, assigning 10-25
cwcli netshow command 10-27
launching show commands from device center 10-25
using show commands 10-1
Command Sets 10-18
assigned Command Sets, showing 10-24
assigning 10-23
assigning to users 10-24
command set details, viewing 10-20
creating 10-20
deleting 10-22
editing 10-21
managing 10-19
system-defined command sets 10-18
credentials, masking 10-7
Deleting output archive 10-17
Job Work Order 10-10
NetShow job browser 10-3
copying jobs 10-13
creating jobs 10-7
deleting jobs 10-15
editing jobs 10-11
stopping jobs 10-13
NetShow jobs, working with 10-2
viewing job output 10-16
viewing permission report 10-2
Netshow
Working with NetShow Jobs 10-2
NetView 3-24
network topology views
connecting to a device from a client 7-20

customizing 7-25
  background images, setting 7-34
devices, deleting 7-26
saving layouts 7-26
topology filters, using 7-37
view features, modifying 7-32
view properties, changing 7-33
displaying 7-21
exporting to Visio 7-55
Find, using in 7-48
navigating in 7-18
summary view, understanding 7-49
  interpreting 7-50
summary views, understanding
  unconnected device information, interpreting 7-50
understanding 7-17
using 7-23
view layouts
  changing 7-27
  upgrading 7-51
N-Hop view portlet 7-51
NMS, integrating with Fault Management 3-24

P

packet capture, using 11-40
pass-through SNMP traps B-2
Performance Management Portlets
  Histo-Graph It 6-19
  Threshold Information 6-31
  Top-N CPU Utilization 6-30
  Top-N Interface Discards 6-22
  Top-N Interface Errors 6-23
  Top-N Interface Utilization 6-25
  Top-N Memory Utilization 6-27
PoE devices 7-39
polling
  applying changes 3-20
  changing settings 3-7
  device groups 3-21
  editing settings 3-15
  how settings are applied 3-2
  ICMP
    intervals C-3
    overview C-1
    SNMP and C-3
    previewing settings 3-17
    restoring default settings 3-20
    setting priorities 3-13
  SNMP
    ICMP and C-3
    overview C-2
    versions supported by Fault Management C-2
    viewing settings 3-15
polling and thresholds
  applying changes 3-20
  changing settings 3-7
  customizable groups and 3-3
  priorities 3-13
  setting priorities 3-13
  port attributes, displaying 7-65
    aggregate link attributes, displaying 7-57

O

OperationallyDown E-9
OutOfRange 2-15, E-10
overlay 15-24
overriding groups 3-13
  default 3-8
  devices 3-11
  interfaces 3-11
  port 3-11
overview
  IP SLA operations 16-1
aggregate link attributes, interpreting 7-58
interpreting 7-65
ports
managing and unmanaging 3-28
occupied by CiscoWorks 3-23
overriding groups 3-11
polling and thresholds 3-2
predefined IP SLA operations 16-2
priorities (polling and thresholds) 3-13
processed SNMP traps B-1
processors, managing and unmanaging 3-28
protocol filtering, monitoring by port 7-75
filter information, displaying 7-76
understanding filtering 7-75
protocols, used by CiscoWorks 3-23

SNMP Set, using 11-37
SNMP traps
cold start D-1
integrating SNMP trap receiving with other NMS 3-24
pass-through B-2
processed B-1
trap forwarding port 3-26
trap receiving port 3-25
warm start D-1
SNMP Walk, using 11-35
specifying operations 15-8
specifying source device 15-7
specifying target device 15-8
starting
CiscoView from VLAN Port Assignment 7-67
Telnet 7-68
Topology Services 7-2
starting collector 15-35
StateNotNormal E-11
stopping collector 15-34
STP (Spanning Tree Protocol) 8-1
configuring on a network 8-13
MISTP devices 8-32
MISTP instances 8-37
MISTP ports 8-21
MISTP trunks 8-42
MST devices 8-28
MST instances 8-36
MST ports 8-17
MST trunks 8-40
PVST devices 8-25
PVST ports 8-13
PVST trunks 8-38
filters in Switch Cloud View, displaying 8-45
Cisco MISTP instances 8-46
IEEE 802.1s instances 8-46
STP loop inconsistencies 8-44
STP PVID inconsistencies 8-45
STP root inconsistencies 8-45
STP type inconsistencies 8-45
VLANs in switch clouds 8-47

Instance Reduction Recommendation report
interpreting 8-8
preparing 8-7

MISTP (multiple instance STP), about 8-3
MST (multiple STP), about 8-2

Number of Instances Recommendation report
interpreting 8-6
preparing 8-6

Optimal Root Recommendation report
interpreting 8-5
preparing 8-4

PVST (per VLAN STP), about 8-2
reports 8-3
Instance Reduction Recommendation 8-7
Number of Instances Recommendation 8-6
Optimal Root Recommendation 8-4

STP Visualizer
interpreting 8-12
notes 8-12
preparing 8-10
topology filters 8-44
understanding 8-1
MST (multiple STP) 8-2
PVST (per VLAN STP) 8-2

VLAN to Instance Mapping Recommendation report
interpreting 8-9
preparing 8-8

Switch Cloud View, and spanning tree filters 8-45
Cisco MISTP instances 8-46
IEEE 802.1s instances, displaying 8-46
STP loop inconsistencies, displaying 8-44
STP PVID inconsistencies, displaying 8-45
STP root inconsistencies, displaying 8-45
STP type inconsistencies, displaying 8-45
VLANs in switch clouds, displaying 8-47

Syslog Analysis application
FAQs on
location of syslog messages 19-9
not getting syslog messages for devices 19-9

system administration
devices from traps to Fault Management 3-23
SNMP trap forwarding port 3-26
SNMP trap receiving port 3-25

System-defined command sets 10-18

T

TDR (Time Domain Reflectometer) reports 7-58
understanding 7-58
using 7-59

Telnet, starting 7-68

Threshold 2-16
Threshold Violation 2-16
Threshold Management 2-16
Creating a Threshold 2-18
Deleting a Threshold 2-25
Editing a Threshold 2-25
Filtering Thresholds 2-26
Viewing Threshold Configuration 2-27
thresholds
applying changes 3-20
categories
Backup Interface Support 2-11, 2-15
Dial-on-Demand Interface Support 2-11, 2-15
Environment 2-11, 2-15
Generic Interface/Port Performance 2-11, 2-15
Interface/Port Flapping 2-13, 2-15
Processor and Memory 2-13, 2-15
Reachability 2-14, 2-15
changing settings 2-1, 3-7
default values 2-15
events triggered by 2-15
how settings are applied 3-2
previewing 2-3
restoring defaults  2-7
setting priorities  3-13
values  2-15
viewing  2-2
tool buttons, on
   Alerts and Events display  9-16
topology groups
   hierarchical maps  7-78
displaying  7-79
understanding  7-78
Topology Services  7-1
   ANI discovery metrics, displaying  7-76
   application servers, working with  7-71
   command reference  7-80
      main window commands  7-80
      network topology view commands  7-82
   connecting to a device from a client  7-20
devices, working with  7-62
      device attributes, interpreting  7-64
      device labels, clearing  7-63
      device labels, displaying  7-63
      device tooltips, working with  7-63, 7-64
device service modules, displaying  7-72
link attributes
   displaying  7-56
   interpreting  7-57
links, working with  7-56
link tooltips, interpreting  7-56
main window
   colors in  7-5
   Find, using in  7-17
   icons in  7-5
   legend  7-5
   navigating in  7-14
   understanding  7-12
management addresses, setting preferred  7-66
MLS devices, working with  7-69
   MLS reports, displaying  7-70
   MLS reports, interpreting  7-70
network topology views
   customizing  7-25
displaying  7-21
exporting to Visio  7-55
Find, using in  7-48
layouts, changing  7-27
navigating in  7-18
summary views, understanding  7-49
understanding  7-17
using  7-23
port attributes, displaying  7-65
   aggregate link attributes
   aggregate link attributes, displaying  7-57
   interpreting  7-65
protocol filtering, monitoring by port  7-75
   filter information, displaying  7-76
   understanding filtering  7-75
protocols supported in spanning tree  8-1
starting  7-2
Time Domain Reflectometer (TDR) reports  7-58
   understanding  7-58
   using  7-59
topology groups  7-77
   hierarchical maps  7-78
   understanding  7-77
   understanding  7-2
traps
   forwarding from devices to Fault Management  3-23
   pass-through SNMP  B-2
   processed SNMP  B-1
   SNMP (see SNMP traps)
   unidentified traps  B-6
TrendWatch  2-28
   TrendWatch Violation  2-28
TrendWatch Management  2-27
   Activating a TrendWatch  2-43
   Copying a TrendWatch  2-43
   Creating a TrendWatch  2-30
Creating a TrendWatch based on Templates 2-30
Creating TrendWatch based on Thresholds 2-39
Deactivating a TrendWatch 2-42
Deleting a TrendWatch 2-42
Editing a TrendWatch 2-41
Filtering TrendWatch 2-45
Troubleshooting 11-42
  Ping or Traceroute 11-42
  Show Commands 11-45
Troubleshooting and FAQs 19-1
troubleshooting tips 19-38
  trunk ports
    managing and unmanaging 3-28
    overriding groups 3-11
    polling and thresholds 3-2, 3-14
    polling categories 3-15
    previewing thresholds 2-3
    threshold categories 2-8
    viewing thresholds 2-2

U
unidentified traps and events
  clearing 8-6
  other 8-6
Unresponsive E-12
user-defined operation
  deleting 16-22
  editing 16-21
    general settings 16-9
    specific settings 16-19
    view summary 16-20
using
  cli commands 18-1

V
viewing

W
working with collectors 15-6