CONTENTS

Chapter 1  Introduction
Terminology................................................................................................  12
  System and device................................................................................  12
  Modeled topology...............................................................................  12
  Object..............................................................................................  12
  Network Protocol Manager installation directory.................................  12
Architectural and functional overview.........................................................  13
  IP Availability Manager......................................................................  16
  Network Protocol Manager...................................................................  16
  Global Manager.................................................................................  17
  Adapter Platform..............................................................................  17
  Global Console.................................................................................  18
  EMC Smarts Broker..........................................................................  18
Configuration roadmap...............................................................................  18
  Network Protocol Manager configuration tasks....................................  18
  IP Availability Manager configuration tasks.......................................  19
  Global Manager configuration tasks....................................................  19
  Adapter Platform configuration tasks (optional)....................................  20
What to do after configuration.....................................................................  20

Chapter 2  Setting Configuration Parameters
  Domain Manager configuration directories............................................  22
User configuration parameters....................................................................  23
Methods to modify user configuration parameters ......................................  23
  Editing configuration files to modify configuration parameters ..............  23
  Issuing the dmctl command to modify configuration parameters ..........  25
Description of bgp.conf.............................................................................  27
Description of eigrp.conf..........................................................................  30
Description of isis.conf.............................................................................  31
Description of ospf.conf..........................................................................  33
Description of perl-cli.conf......................................................................  35
EMC Smarts secure communications.........................................................  36

Chapter 3  Opening the Global Console
Global Console overview.............................................................................  38
User accounts and passwords.....................................................................  38
Procedure for opening the Global Console..............................................  39
Procedure for opening the Global Manager Administration Console.......  41
Procedure for opening the Domain Manager Administration Console ......  41
Procedure for opening the Polling and Thresholds Console....................  42

Chapter 4  Configuring IP Availability Manager
Configuration overview...............................................................................  44
Toplogy and CLI device-access object import..........................................  44
  Import of topology.............................................................................  45
  Import of CLI device-access objects...................................................  45
  Types of imported objects...................................................................  46
## Contents

- Syslog message format ................................................................. 160
- Sample syslog message ............................................................... 160
- Syslog messages processed and actions taken .............................. 160
- Enabling BGP Max Route (Prefix) threshold monitoring ............... 161
- Syslog messages processed for OSPF monitoring ....................... 162
- Syslog message format ............................................................... 162
- Sample syslog messages ............................................................. 162
- Syslog messages processed and actions taken .............................. 163

### Appendix D  
**CLI Commands for Monitoring**

- CLI commands for EIGRP monitoring........................................ 166
- CLI commands for IS-IS monitoring ........................................... 166
- CLI commands for BGP IPv6 discovery and monitoring of Cisco devices.... 167
- CLI commands for BGP IPv6 discovery and monitoring of Juniper devices .. 168

### Appendix E  
**SNMP Poller**

- SNMP polling overview ............................................................... 170
- SNMP poller operation ............................................................... 170
- Just-in-time polling ................................................................. 170
- Request-consolidation polling .................................................. 171

### Appendix F  
**NPM dump instrumentation utility**

- Network Protocol Manager dump instrumentation utility ............. 174
- Invoking the NPM dump instrumentation utility .......................... 174
- BGP instrumentation utility command ........................................ 174
- EIGRP instrumentation utility command ...................................... 174
- IS-IS instrumentation utility command ....................................... 175
- OSPF instrumentation utility command ....................................... 175

Index
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Protocol Manager architecture for BGP or OSPF</td>
<td>14</td>
</tr>
<tr>
<td>Network Protocol Manager architecture for EIGRP or IS-IS</td>
<td>15</td>
</tr>
<tr>
<td>Domain Manager configuration directories for Network Protocol Manager</td>
<td>22</td>
</tr>
<tr>
<td>Preview of how the sm_edit utility works</td>
<td>24</td>
</tr>
<tr>
<td>Attach Manager dialog box</td>
<td>39</td>
</tr>
<tr>
<td>Topology Browser Console</td>
<td>40</td>
</tr>
<tr>
<td>Notification Log Console</td>
<td>41</td>
</tr>
<tr>
<td>Domain Manager Administration Console</td>
<td>42</td>
</tr>
<tr>
<td>Importing topology and CLI device-access objects from IP Availability Manager</td>
<td>45</td>
</tr>
<tr>
<td>Topology and CLI device-access objects imported from IP Availability Manager</td>
<td>46</td>
</tr>
<tr>
<td>CLI discovery, CLI polling, and CLI device-access object creation and transfer</td>
<td>50</td>
</tr>
<tr>
<td>Global Manager Administration Console interaction with the Global Manager</td>
<td>59</td>
</tr>
<tr>
<td>IC Domain Configuration objects and their relationships</td>
<td>60</td>
</tr>
<tr>
<td>Default domain configurations for a Network Protocol Manager deployment</td>
<td>61</td>
</tr>
<tr>
<td>Global Manager and Administration Console</td>
<td>62</td>
</tr>
<tr>
<td>How reconfiguring the Global Manager works</td>
<td>63</td>
</tr>
<tr>
<td>Access to server tools for loading XML configuration files</td>
<td>64</td>
</tr>
<tr>
<td>Before and after completing configuration scenario 1</td>
<td>66</td>
</tr>
<tr>
<td>Before and after completing configuration scenario 2</td>
<td>70</td>
</tr>
<tr>
<td>Using the Domain Creation Wizard to create the EAST-INCHARGE-BGP domain</td>
<td>72</td>
</tr>
<tr>
<td>Using the Domain Creation Wizard to create the EAST-INCHARGE-AM domain</td>
<td>73</td>
</tr>
<tr>
<td>Global Manager Administration Console with admin-profile selected</td>
<td>75</td>
</tr>
<tr>
<td>Console Operations dialog box</td>
<td>76</td>
</tr>
<tr>
<td>Recommended trap-integration design</td>
<td>78</td>
</tr>
<tr>
<td>Configuration directory for a trap exploder</td>
<td>81</td>
</tr>
<tr>
<td>Mapping of trap exploder configuration steps to configured forwarded-trap paths</td>
<td>86</td>
</tr>
<tr>
<td>Recommended syslog message processing and forwarding design</td>
<td>96</td>
</tr>
<tr>
<td>SSH connection between a Network Protocol Manager host and a Cisco router</td>
<td>100</td>
</tr>
<tr>
<td>Polling and Thresholds Console</td>
<td>112</td>
</tr>
<tr>
<td>Relating managed objects to groups and settings</td>
<td>114</td>
</tr>
<tr>
<td>Polling tab for Network Protocol Manager for BGP</td>
<td>122</td>
</tr>
<tr>
<td>Thresholds tab for Network Protocol Manager for BGP</td>
<td>123</td>
</tr>
<tr>
<td>SNMP-polling and CLI-polling configuration and operation</td>
<td>124</td>
</tr>
<tr>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>User configuration files for Network Protocol Manager</td>
<td>23</td>
</tr>
<tr>
<td>Parameters in the bgp.conf file</td>
<td>27</td>
</tr>
<tr>
<td>Parameters in the eigrp.conf file</td>
<td>30</td>
</tr>
<tr>
<td>Parameters in the isis.conf file</td>
<td>31</td>
</tr>
<tr>
<td>Parameters in the ospf.conf file</td>
<td>33</td>
</tr>
<tr>
<td>Parameters in the perl-cli.conf file</td>
<td>35</td>
</tr>
<tr>
<td>Partial list of DXA configuration commands</td>
<td>47</td>
</tr>
<tr>
<td>Default values for the CLI Access Setting</td>
<td>54</td>
</tr>
<tr>
<td>Trap exploder translation of incoming traps to forwarded traps</td>
<td>80</td>
</tr>
<tr>
<td>Configuration parameters in the trapd.conf file</td>
<td>83</td>
</tr>
<tr>
<td>Polling and Thresholds Console toolbar buttons</td>
<td>113</td>
</tr>
<tr>
<td>Default Network Protocol Manager for BGP polling groups</td>
<td>126</td>
</tr>
<tr>
<td>Default Network Protocol Manager for EIGRP polling groups</td>
<td>126</td>
</tr>
<tr>
<td>Default Network Protocol Manager for IS-IS polling groups</td>
<td>126</td>
</tr>
<tr>
<td>Default Network Protocol Manager for OSPF polling groups</td>
<td>126</td>
</tr>
<tr>
<td>BGP SNMP Setting parameters and their values</td>
<td>128</td>
</tr>
<tr>
<td>BGP External Setting parameters and their values</td>
<td>129</td>
</tr>
<tr>
<td>EIGRP CLI Setting parameters and their values</td>
<td>130</td>
</tr>
<tr>
<td>EIGRP EXTERNAL Setting parameters and their values</td>
<td>131</td>
</tr>
<tr>
<td>ISIS CISCO CLI Setting parameters and their values</td>
<td>132</td>
</tr>
<tr>
<td>ISIS EXTERNAL Setting parameters and their values</td>
<td>133</td>
</tr>
<tr>
<td>OSPF SNMP Setting parameters and their values</td>
<td>134</td>
</tr>
<tr>
<td>OSPF External Setting parameters and their values</td>
<td>135</td>
</tr>
<tr>
<td>Default Network Protocol Manager for BGP threshold groups</td>
<td>137</td>
</tr>
<tr>
<td>BGP Session Flapping setting parameters and their values</td>
<td>138</td>
</tr>
<tr>
<td>Basic wildcard patterns</td>
<td>140</td>
</tr>
<tr>
<td>Compound wildcard patterns</td>
<td>141</td>
</tr>
<tr>
<td>Instrumentation MIB objects polled by NPM for BGP (IPv4)</td>
<td>144</td>
</tr>
<tr>
<td>SNMP traps processed by Network Protocol Manager for BGP</td>
<td>146</td>
</tr>
<tr>
<td>Instrumentation MIB objects polled by Network Protocol Manager for OSPF</td>
<td>148</td>
</tr>
<tr>
<td>SNMP traps processed by Network Protocol Manager for OSPF</td>
<td>153</td>
</tr>
<tr>
<td>MIB object polled for instrumentation by Network Protocol Manager for IS-IS</td>
<td>156</td>
</tr>
<tr>
<td>Syslog messages processed and actions taken</td>
<td>161</td>
</tr>
<tr>
<td>Syslog messages processed and actions taken</td>
<td>163</td>
</tr>
<tr>
<td>Authentication and privacy protocol support for SNMPv3</td>
<td>170</td>
</tr>
<tr>
<td>NPM dump instrumentation utility scripts</td>
<td>174</td>
</tr>
</tbody>
</table>
CHAPTER 1
Introduction

This chapter presents an overview of EMC Smarts Network Protocol Manager and highlights the configuration tasks that are needed to set up a Network Protocol Manager deployment. It consists of the following sections:

- Terminology............................................................................................................ 12
- Architectural and functional overview ................................................................. 13
- Configuration roadmap ......................................................................................... 18
- What to do after configuration............................................................................... 20
Introduction

Terminology

The EMC® Smarts® Network Protocol Manager includes the following components:

◆ Network Protocol Manager for BGP
◆ Network Protocol Manager for EIGRP
◆ Network Protocol Manager for IS-IS
◆ Network Protocol Manager for OSPF

EMC Smarts Network Protocol Manager represents four EMC Smarts Domain Managers. A Domain Manager is a service-assurance application that is associated with a particular type of information-technology domain, such as networks, systems, applications, or application services. For Network Protocol Manager, the domain is a routing-protocol network, that is, a Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System to Intermediate System (IS-IS), or Open Shortest Path First (OSPF) distributed application that is running in an IP network. Each Domain Manager is autonomous in the sense that it:

◆ Maintains its own data models, repository, and problem signatures.
◆ Monitors and analyzes the discovered objects in its own domain.

System and device

The term “system” is a generic term that represents a computer-based network entity, such as a host, router, or switch. The term “device” has essentially the same meaning as system except that, in some cases, “device” also conveys the sense of specific model, such as a specific model of host, router, or switch.

Modeled topology

Network Protocol Manager uses EMC Smarts object class models to create within its repository instances of logical routing topology objects, their relationships, and their logical connections. The “modeled topology” mirrors the real topology in the managed network.

Object

The term “object” is intended to have a dual meaning: To simultaneously represent both (1) an EMC Smarts object in the modeled topology and (2) a physical or logical entity in the real topology. An EMC Smarts object corresponds to a physical or logical entity in the real topology.

Network Protocol Manager installation directory

In this document, the term BASEDIR represents the location where the software is installed:

◆ For UNIX, this location is: /opt/InCharge/<product>.
◆ For Windows, this location is: C:\InCharge\<product>.
The <product> represents the EMC Smarts product. For example, on UNIX operating systems, EMC Smarts Network Protocol Manager is, by default, installed to: /opt/InCharge/NPM/smarts. On Windows operating systems, this product is, by default, installed to: C:\InCharge\NPM\smarts. This location is referred to as BASEDIR/smarts.

Optionally, you can specify the root of BASEDIR to be something different, but you cannot change the <product> location under the root directory.

The *EMC Smarts System Administration Guide* provides detailed information about the directory structure for EMC Smarts software.

**Architectural and functional overview**

Network Protocol Manager, working with EMC Smarts IP Availability Manager (IP Availability Manager) and the EMC Smarts Service Assurance Manager (Global Manager), manages routing-protocol networks. Figure 1 on page 14 and Figure 2 on page 15 show how Network Protocol Manager interoperates with these components.
Introduction

Figure 1 Network Protocol Manager architecture for BGP or OSPF
Figure 2 Network Protocol Manager architecture for EIGRP or IS-IS
IP Availability Manager

IP Availability Manager diagnoses connectivity failures in multivendor, switched, and routed networks by discovering and monitoring Layer 2 (data-link) and Layer 3 (network) systems. Switches are examples of Layer 2 systems, and routers are examples of Layer 3 systems.

When included in a Network Protocol Manager deployment, IP Availability Manager:

- Discovers and monitors through SNMP the underlying physical-transport domain in the managed network.
- Analyzes the network connectivity to identify the root-cause problems and impacts of connectivity failures.
- Exports network topology, problem, and impact information to the Global Manager.
- Exports routing-enabled (BGP-enabled, EIGRP-enabled, IS-IS-enabled, OSPF-enabled) device topology and status information to Network Protocol Manager.
- Exports command line interface (CLI) device-access objects to Network Protocol Manager.

Routing-enabled device topology includes routers and switches (that house router cards) that are running BGP, EIGRP, IS-IS, or OSPF services. Device status information consists of status changes that are associated with the routing-enabled device topology.

CLI device-access objects are required by Network Protocol Manager when performing CLI discovery or CLI polling. The CLI device-access objects carry the login credential information needed by Network Protocol Manager to access the devices in the managed network that cannot be discovered or monitored by using SNMP. Upon logging into a device, Network Protocol Manager invokes CLI commands to query the device for discovery or status information.

A Network Protocol Manager deployment may contain one or more IP Availability Managers. An IP Availability Manager instance may consist of just an IP Availability Manager process, or may consist of an IP Availability Manager and an IP Performance Manager or IP Server Performance Manager that are running together as a single process.

Network Protocol Manager

Network Protocol Manager relies on the topology, topology updates, and topology status updates received from IP Availability Manager to discover and monitor routing-enabled devices and BGP, EIGRP, IS-IS, or OSPF services.

Network Protocol Manager collectively represents each of the following Network Protocol Manager products:

- Network Protocol Manager for BGP

On BGP-enabled devices initially discovered by IP Availability Manager, Network Protocol Manager for BGP discovers and monitors BGP services, BGP endpoints, BGP sessions participating in the routing updates, and BGP configurations.
- **Network Protocol Manager for EIGRP**
  On EIGRP-enabled devices initially discovered by IP Availability Manager, Network Protocol Manager for EIGRP discovers and monitors EIGRP services, EIGRP endpoints, and EIGRP sessions participating in the routing updates.

- **Network Protocol Manager for IS-IS**
  On IS-IS-enabled devices initially discovered by IP Availability Manager, Network Protocol Manager for IS-IS discovers and monitors IS-IS services, IS-IS endpoints, IS-IS adjacencies participating in the routing updates, and IS-IS configurations.

- **Network Protocol Manager for OSPF**
  On OSPF-enabled devices initially discovered by IP Availability Manager, Network Protocol Manager for OSPF discovers and monitors OSPF services, OSPF endpoints, OSPF adjacencies participating in the routing updates, and OSPF configurations.

Separate instances of Network Protocol Manager are required to manage the availability of each routing protocol: one each for BGP, EIGRP, IS-IS, and OSPF.

Upon importing the initial, routing-enabled device topology from IP Availability Manager, Network Protocol Manager performs its own SNMP and CLI discovery to query the devices for routing topology information. Upon building its routing topology data model, Network Protocol Manager exports the topology to the Global Manager.

Network Protocol Manager monitors the status of the routing topology by periodically SNMP- and CLI-polling the routing-enabled devices. It also subscribes to certain network topology object statuses (attributes) from IP Availability Manager.

Network Protocol Manager analyzes the received statuses to identify device and routing-protocol availability problems and impacts, and exports the results of its analysis to the Global Manager. In addition, whenever Network Protocol Manager detects a configuration-related error in a managed routing-protocol network, it exports the event to the Global Manager.

### Global Manager

The Global Manager integrates the topology, problem, and impact information that is imported from IP Availability Manager and Network Protocol Manager, and relates the information to services and customers. It also provides cross-domain and end-to-end impact analysis.

The Global Manager displays the topology, problem, and impact information through the Global Console.

### Adapter Platform

The EMC Smarts Service Assurance Manager Adapter Platform (Adapter Platform) is an optional component in a Network Protocol Manager deployment. The Adapter Platform is included in the deployment only if the customer wants to forward informational traps to the Global Manager for display in the Global Console.
Introduction

The Adapter Platform imports and normalizes topology from IP Availability Manager, and imports and normalizes events of interest from EMC Smarts adapters such as the SNMP Trap Adapter. Normalize means to convert topology or event information into a common form that is understood by the Global Manager. The normalized event information is transferred as EMC Smarts notifications to the Global Manager.

An Adapter Platform feature, called the Topology Importer, collects hostnames and IP addresses from IP Availability Manager so that the Adapter Platform can accurately place events in their topological context. The Adapter Platform updates this list as the information changes in IP Availability Manager.

Global Console

The Global Console provides a graphical user interface for configuration and administration of Global Managers, Adapter Platforms, Domain Managers, and externally running EMC Smarts adapters such as the SNMP Trap Adapter.

When the Global Console is attached to the Global Manager, a user can browse the topology in various forms, including maps, and view notifications about problems that impact availability and performance.

EMC Smarts Broker

The EMC Smarts Broker facilitates Global Console connections to the component applications in an EMC Smarts system deployment.

When a user starts a Global Console process, the process connects to the Broker and launches a dialog box through which the user views and selects any component application that is registered with the Broker. After the user selects an application, the Global Console connects to the application and disconnects from the Broker.

Configuration roadmap

The following sections highlight the configuration tasks that are associated with the setup of the components in a Network Protocol Manager deployment. These tasks involve configuring the Network Protocol Manager, IP Availability Manager, Global Manager, and (optional) Adapter Platform applications that are part of the deployment.

Some configuration tasks are performed before the applications are started, such as the editing of configuration files, and some are performed through the Global Console when the applications are up and running.

Network Protocol Manager configuration tasks

Configuring Network Protocol Manager consists of the following tasks:

- Configure SNMP trap integration to distribute BGP- or OSPF-related trap messages to Network Protocol Manager for processing (optional).

  Chapter 2, “Setting Configuration Parameters,” and Chapter 6, “Configuring SNMP Trap Integration,” provide the procedures for completing this task.

- Configure syslog message forwarding to forward BGP- or OSPF-related syslog messages to Network Protocol Manager for processing (optional).
Chapter 2, “Setting Configuration Parameters,” and Chapter 7, “Configuring Syslog Message Processing and Forwarding,” provide the procedures for completing this task.

- Configure Secure Shell (SSH) clients and servers to enable Network Protocol Manager to perform CLI discovery and CLI polling over a secure connection (optional).

  Chapter 8, “Configuring SSH Security,” provides the procedures for completing this task.

- Configure SNMP polling and CLI polling (optional).

  Chapter 10, “Configuring Polling and Threshold Groups,” provides the procedures for completing this task.

- Add IP Availability Manager as a source from which Network Protocol Manager imports topology and status updates (mandatory).

  The EMC Smarts Network Protocol Manager Discovery Guide provides the instructions for completing this task.

### IP Availability Manager configuration tasks

In addition to performing the configuration and administration tasks that are common to all IP Availability Managers, you perform the following additional tasks to set up IP Availability Manager in a Network Protocol Manager deployment:

- Enable protocol light discovery (mandatory).
- Enable overlapping IP address discovery (optional).
- Create CLI device-access groups to enable Network Protocol Manager to perform CLI discovery and polling of devices that cannot be discovered or monitored by using SNMP (mandatory if EIGRP- or IS-IS-enabled Cisco devices are to be managed by Network Protocol Manager).
- Configure SNMP trap integration to distribute network traps to IP Availability Manager (mandatory).

  Chapter 4, “Configuring IP Availability Manager,” and Chapter 6, “Configuring SNMP Trap Integration,” provide the procedures for performing these tasks. Procedures for configuring all aspects of IP Availability Manager are given in the IP Manager documentation.

### Global Manager configuration tasks

In addition to performing the configuration and administration tasks that are common to all Global Managers, you perform the following additional tasks to set up the Global Manager in a Network Protocol Manager deployment:

- Set up a communication link between the Global Manager and the Network Protocol Manager (mandatory).
- Set up a communication link between the Global Manager and the IP Availability Managers (mandatory).
- Set up a communication link between the Global Manager and the Adapter Platform (mandatory if the Adapter Platform is included in the deployment).
Introduction

- Enable access to the BGP, EIGRP, IS-IS, and OSPF maps (optional).

Chapter 5, “Configuring the Global Manager,” provides the procedures for performing these tasks. Procedures for configuring all aspects of the Global Manager are given in the *EMC Smarts Service Assurance Manager Configuration Guide*.

Adapter Platform configuration tasks (optional)

Only if you want to forward informational traps to the Global Manager for display as EMC Smarts notifications in the Global Console do you include the Adapter Platform in your Network Protocol Manager deployment.

If you decide to include the Adapter Platform, Chapter 6, “Configuring SNMP Trap Integration,” provides the procedure for configuring the Adapter Platform to receive, convert, and forward traps to the Global Manager. Procedures for configuring all aspects of the Adapter Platform and the SNMP Trap Adapter are given in the *EMC Smarts Service Assurance Manager Adapter Platform User Guide*.

What to do after configuration

Upon configuring your Network Protocol Manager deployment, you are ready to begin the discovery. To understand, prepare for, and initiate Network Protocol Manager discovery, consult the *EMC Smarts Network Protocol Manager Discovery Guide*.

After the discovery, consult the individual user guides (BGP, EIGRP, IS-IS, OSPF) for Network Protocol Manager to understand Network Protocol Manager monitoring and analysis.
CHAPTER 2
Setting Configuration Parameters

This chapter identifies Network Protocol Manager configuration parameters that are relevant to discovery, describes their settings, and provides instructions for changing their settings. It consists of the following sections:

- Domain Manager configuration directories .......................................................... 22
- User configuration parameters ................................................................................ 23
- Methods to modify user configuration parameters .................................................. 23
- Description of bgp.conf ........................................................................................... 27
- Description of eigrp.conf ......................................................................................... 30
- Description of isis.conf ........................................................................................... 31
- Description of ospf.conf .......................................................................................... 33
- Description of perl-cli.conf ...................................................................................... 35
- EMC Smarts secure communications ....................................................................... 36
- Description of perl-cli.conf ...................................................................................... 35
- EMC Smarts secure communications ....................................................................... 36
Domain Manager configuration directories

The Network Protocol Manager installation directory contains the four Domain Manager configuration directories that are shown in Figure 3 on page 22.

BASEDIR

```
<table>
<thead>
<tr>
<th>BASEDIR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>smarts</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>conf</td>
</tr>
</tbody>
</table>
```

- Network Protocol Manager for BGP configuration directory
- Network Protocol Manager for EIGRP configuration directory
- Network Protocol Manager for IS-IS configuration directory
- Network Protocol Manager for OSPF configuration directory

**Figure 3** Domain Manager configuration directories for Network Protocol Manager

BASEDIR, which is not an environment variable, is used in documentation to represent the top-level directory structure of an EMC Smarts product installation. For the Network Protocol Manager, BASEDIR represents `<root_dir>/NPM`.

Each configuration directory in Figure 3 on page 22 contains the bootstrap and configuration files for its associated Domain Manager. The `--config` option in a Domain Manager startup command points to the appropriate configuration directory:

- The `--config=bgp` option in a Network Protocol Manager for BGP startup command points to the bootstrap and configuration files in the bgp directory. The default name of Network Protocol Manager for BGP is INCHARGE-BGP.
- The `--config=eigrp` option in a Network Protocol Manager for EIGRP startup command points to the bootstrap and configuration files in the eigrp directory. The default name of Network Protocol Manager for EIGRP is INCHARGE-EIGRP.
- The `--config=isis` option in a Network Protocol Manager for IS-IS startup command points to the bootstrap and configuration files in the isis directory. The default name of Network Protocol Manager for IS-IS is INCHARGE-ISIS.
- The `--config=ospf` option in a Network Protocol Manager for OSPF startup command points to the bootstrap and configuration files in the ospf directory. The default name of Network Protocol Manager for OSPF is INCHARGE-OSPF.

The bootstrap and configuration files for a Domain Manager set up the environment for the Domain Manager.
User configuration parameters

A major part of configuring Network Protocol Manager involves the setting of user configuration parameters in the files that are identified in Table 1 on page 23.

Table 1 User configuration files for Network Protocol Manager

<table>
<thead>
<tr>
<th>Directory under BASEDIR</th>
<th>Filename</th>
<th>Description</th>
<th>Object configured by this file</th>
</tr>
</thead>
<tbody>
<tr>
<td>smarts/conf/bgp</td>
<td>bgp.conf</td>
<td>File in which you customize Network Protocol Manager for BGP discovery.</td>
<td>MSI_AdapterManager::BGP-Adapter-Manager for BGP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This object is the topology manager for Network Protocol Manager for BGP.</td>
</tr>
<tr>
<td>smarts/conf/eigrp</td>
<td>eigrp.conf</td>
<td>File in which you customize Network Protocol Manager for EIGRP discovery.</td>
<td>MSI_AdapterManager::EIGRP-Adapter-Manager for EIGRP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This object is the topology manager for Network Protocol Manager for EIGRP.</td>
</tr>
<tr>
<td>smarts/conf/isis</td>
<td>isis.conf</td>
<td>File in which you customize Network Protocol Manager for IS-IS discovery.</td>
<td>MSI_AdapterManager::ISIS-Adapter-Manager for IS-IS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This object is the topology manager for Network Protocol Manager for IS-IS.</td>
</tr>
<tr>
<td>smarts/conf/ospf</td>
<td>ospf.conf</td>
<td>File in which you customize Network Protocol Manager for OSPF discovery.</td>
<td>MSI_AdapterManager::OSPF-Adapter-Manager for OSPF.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This object is the topology manager for Network Protocol Manager for OSPF.</td>
</tr>
</tbody>
</table>

As with most EMC Smarts configuration files, the bgp.conf, eigrp.conf, isis.conf, and ospf.conf files are used to set attributes for certain objects within a Domain Manager’s environment when the Domain Manager starts up. The parameters and their values in a configuration file become the attributes and their values for the created objects.

Methods to modify user configuration parameters

There are two methods to modify user configuration parameters:

1. Edit the user configuration files and modify configuration parameters.
2. Issue the dmctl command to modify configuration parameters when Network Protocol Manager is running.

Command-modified parameters are not persistent, which means that the modifications will be forgotten when Network Protocol Manager is shut down and restarted. Every time that Network Protocol Manager starts up, it sets its configurations in accordance to the parameter values in the user (and other) configuration files.

Editing configuration files to modify configuration parameters

EMC Smarts provides the sm_edit utility to ensure that modified files are always saved to the appropriate local area and that original copies of the files remain unchanged. Figure 4 on page 24 previews the operation of the sm_edit utility.
BASEDIR

<root_dir>

BASEDIR/smarts/conf

BASEDIR/smarts/local/conf

* The dasl directory appears only in a Network Protocol Manager installation on a Windows system.

**Figure 4** Preview of how the sm_edit utility works

All EMC Smarts products use the same basic installation directory structure that is shown in **Figure 4 on page 24**.

To invoke the sm_edit utility, go to the BASEDIR/smarts/bin directory and specify the path and the name of the file, relative to the BASEDIR/smarts directory, that you want to edit. For example,

```
sm_edit conf/bgp/bgp.conf
```

opens in a text editor either a local copy of the bgp.conf file in BASEDIR/smarts/local/conf/bgp or an original copy of the bgp.conf file in BASEDIR/smarts/conf/bgp if no local copy exists.

After you modify and save the bgp.conf file, the sm_edit utility saves the modified version of the file to the BASEDIR/smarts/local/conf/bgp directory.
You can use the sm_edit utility to edit any text file, not just a configuration file, in the BASEDIR/smarts or BASEDIR/smarts/local directory. Because sm_edit assumes a starting point of BASEDIR/smarts, the text-file path that you specify begins with the directory name (conf, rules, script, and so on) under the BASEDIR/smarts directory.

**NOTICE**

Original versions of files may be changed or updated as part of an EMC Smarts software upgrade. However, files in the BASEDIR/smarts/local directory are retained during an upgrade.

The *EMC Smarts System Administration Guide* provides additional information about the sm_edit utility.

**Issuing the dmctl command to modify configuration parameters**

In general, you can use the following dmctl command to change the value of any basic-type attribute (string, boolean, integer, float, and so on) of any EMC Smarts object:

```
dmctl -s <Domain Manager instance name> put
<class::instance::attribute> <value>
```

**NOTICE**

The dmctl utility is described in the HTML pages that are located in the BASEDIR/smarts/doc/html/usage directory of any Domain Manager installation area.

Upon issuing a dmctl command, you might be prompted for a username and password. Respond with your user account. For example, to specify the default administrative account, enter username *admin* and password *changeme*.

For Network Protocol Manager, you use the dmctl put command to override parameter settings in the bgp.conf file, the eigrp.conf file, the isis.conf file, and the ospf.conf file.

**Temporary versus permanent change**

The use of the dmctl command to override a parameter value in a configuration file is temporary in the following sense: When the Domain Manager is restarted, it reads the original parameter value in the configuration file. To make the change permanent, use the sm_edit utility to change the parameter value in the configuration file.

**Example**

As an example of using the dmctl command, you can issue the following dmctl command from the BASEDIR/smarts/bin directory to override the AdminDownFlag parameter value in the bgp.conf file:

```
dmctl -s INCHARGE-BGP put
MSI_AdapterManager::BGP-Adapter-Manager::AdminDownFlag TRUE
```

The parameters in the bgp.conf file are defined as attributes of the BGP-Adapter-Manager object, which is an instance of the MSI_AdapterManager class. The BGP-Adapter-Manager object is not saved to disk, that is, is not saved to a Network Protocol Manager for BGP repository file in the BASEDIR/smarts/local/repos/icf directory.
Setting Configuration Parameters

More examples

As further examples, you can issue the following dmctl commands from the BASEDIR/smarts/bin directory to override the AdminDownFlag parameter value in the eigrp.conf, isis.conf, and ospf.conf files:

```bash
dmctl -s INCHARGE-EIGRP put
    MSI_AdapterManager::EIGRP-Adapter-Manager::AdminDownFlag TRUE

dmctl -s INCHARGE-ISIS put
    MSI_AdapterManager::ISIS-Adapter-Manager::AdminDownFlag TRUE

dmctl -s INCHARGE-OSPF put
    MSI_AdapterManager::OSPF-Adapter-Manager::AdminDownFlag TRUE
```

As with the BGP-Adapter-Manager object, the EIGRP-Adapter-Manager, ISIS-Adapter-Manager, and OSPF-Adapter-Manager objects are not saved to disk, that is, are not saved to individual Network Protocol Manager repository files in the BASEDIR/smarts/local/repos/icf directory.

Limitations

Although you can use the dmctl command to override parameter values in the bgp.conf, eigrp.conf, isis.conf, or ospf.conf file, your changes might not take effect because Network Protocol Manager reads some parameters only at startup.

For example, even if you issue the dmctl command to override the TrapPort or SyslogName setting in the bgp.conf file, your change will not be known to the target Network Protocol Manager for BGP until you:

1. Use the sm_edit utility to make the change to the TrapPort or SyslogName parameter in the bgp.conf file.
2. Restart the target Network Protocol Manager for BGP.
Description of bgp.conf

The bgp.conf file contains configuration parameters that you edit to customize Network Protocol Manager for BGP discovery. The parameters are a subset of attributes that are defined for the topology manager (BGP-Adapter-Manager) that will run in the Network Protocol Manager for BGP environment.

Table 2 on page 27 describes the parameters in the bgp.conf file. The parameters and their values are case-sensitive.

Table 2 Parameters in the bgp.conf file (page 1 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config</td>
<td>Regular expression: bgp</td>
<td>Identifies this Domain Manager configuration as Network Protocol Manager for BGP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Do not change this parameter.</td>
</tr>
<tr>
<td>TrapPort</td>
<td>0, 162, 2049 to 65534</td>
<td>Enables the Network Protocol Manager for BGP built-in trap receiver, and specifies the port used by the trap receiver to receive traps.</td>
</tr>
<tr>
<td></td>
<td>Default: 0</td>
<td>• TrapPort = 0 disables the built-in trap receiver.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TrapPort = 162 or a value in the range 2049 to 65534 (inclusive) enables the built-in trap receiver and sets the trap port to the value specified for the parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“Procedure to configure the Network Protocol Manager built-in trap receiver” on page 89 clarifies the use of this parameter.</td>
</tr>
<tr>
<td>TraceTraps</td>
<td>TRUE, FALSE</td>
<td>Determines whether trap receiver tracing for Network Protocol Manager for BGP is enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td>Default: FALSE</td>
<td>• A value of TRUE indicates that trap receiver tracing is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of FALSE indicates that trap receiver tracing is disabled.</td>
</tr>
<tr>
<td>SyslogName</td>
<td>Regular expression</td>
<td>Enables the Network Protocol Manager for BGP built-in syslog adapter, and specifies the name of the local syslog file to be tailed by the syslog adapter.</td>
</tr>
<tr>
<td></td>
<td>Default: empty string</td>
<td>• SyslogName = &quot;&quot; (empty string) disables the built-in syslog adapter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SyslogName = &lt;full path and name of syslog file&gt; (for example, /var/adm/messages) enables the built-in syslog adapter and sets the name of the local syslog file to be tailed to the value specified for the parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chapter 7, “Configuring Syslog Message Processing and Forwarding,” clarifies the use of this parameter.</td>
</tr>
<tr>
<td>TraceSyslog</td>
<td>TRUE, FALSE</td>
<td>Determines whether syslog adapter tracing for Network Protocol Manager for BGP is enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td>Default: FALSE</td>
<td>• A value of TRUE indicates that syslog adapter tracing is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of FALSE indicates that syslog adapter tracing is disabled.</td>
</tr>
</tbody>
</table>
### Setting Configuration Parameters

#### Table 2 Parameters in the bgp.conf file (page 2 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| AdminDownFlag                 | TRUE, FALSE                  | Controls whether Network Protocol Manager for BGP generates alarms on the BGP sessions of BGP protocol endpoints that are administratively down (manually disabled).  
   - A value of TRUE indicates that alarms are not generated on the BGP sessions.  
   - A value of FALSE indicates that alarms are generated on the BGP sessions. |
| IsDisplayNameCustom           | TRUE, FALSE                  | Controls whether Network Protocol Manager for BGP accepts topology objects from EMC Smarts Adapter for Alcatel-Lucent 5620 SAM EMS (the Adapter).  
   - A value of TRUE indicates that topology objects from the Adapter are accepted.  
   - A value of FALSE indicates that topology objects from the Adapter are not accepted.  
   When the Adapter is present, set the IsDisplayNameCustom parameter to TRUE. The Adapter is described in the EMC Smarts Adapter for Alcatel-Lucent 5620 SAM EMS User Guide. |
| EnableRRDiscovery             | TRUE, FALSE                  | Controls whether Network Protocol Manager for BGP discovers Route Reflectors.  
   - A value of TRUE indicates that Route Reflectors are discovered.  
   - A value of FALSE indicates that Route Reflectors are not discovered.  
   To discover Route Reflectors, set the EnableRRDiscovery parameter to TRUE. |
| EnableIPv6Discovery           | TRUE, FALSE                  | Controls the discovery of IPv6 topology by Network Protocol Manager for BGP.  
   - TRUE — Enables IPv6 topology discovery.  
   - FALSE — Disables IPv6 topology discovery. |
| DisableBGPAccSNMPError        | TRUE, FALSE                  | Controls whether Network Protocol Manager for BGP should ignore  
   - TRUE — A value of TRUE SNMP error get's ignored  
   - FALSE                                             |
| DisableAlertsOnCLIError       | TRUE, FALSE                  | Controls whether Network Protocol Manager for BGP should ignore the CLI errors.  
   - TRUE — Disables the alerts on CLI errors.  
   - FALSE— Enables the alerts on CLI errors.       |

**Note:** Applicable only for BGP, OSPF and IS-IS.
### Parameter Values in the bgp.conf File (Page 3 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| **ProbeAllSystemsForIPv6** | TRUE, FALSE Default: TRUE | Controls the discovery probe for all systems in an IPv6 network by Network Protocol Manager for BGP.  
- TRUE — The BGP server will probe each and every device for IPv6 BGP regardless of the IPv6 IP objects are discovered on that device by IP Domain Managers.  
- FALSE — The BGP server will probe only those devices whose IPv6 objects are discovered by IP Domain Manager. |
| **RemoveOneMemberBGPSessionGroups** | TRUE, FALSE Default: TRUE | Controls whether Network Protocol Manager for BGP if this flag is set to TRUE then NPM BGP domain manager will remove one member BGPSessionGroups. |
| **Type** | AM | Indicates the type of the Domain Manager that is added as a topology source. |
| **DomainName** | INCHARGE-AM | This is the name of the IP Domain Manager that is added as a topology source.  
**Note:** This is the default domain name.  
You can use the right click option to delete it from the Domain Manager Administration Console, and then update the configuration file by commenting out the DomainName parameter. |
| **DisplayName** | INCHARGE-AM | This is the display name of the IP Domain Manager that is added as a topology source. |
| **EnableReconfigureLaunchedLiteSynchronization** | TRUE, FALSE Default: FALSE | Introduced with Network Protocol Manager 9.2.x patches, enables light discovery.  
To enable light discovery, set the EnableReconfigureLaunchedLiteSynchronization and EnablePeriodicLiteSynchronization parameters to TRUE and restart the Network Protocol Manager for BGP. Only newly-added devices are detected and imported into Network Protocol Manager for BGP.  
By default, light discovery between Network Protocol Manager for BGP and IP Availability Manager is disabled. |
| **EnablePeriodicLiteSynchronization** | TRUE, FALSE Default: FALSE | Introduced with Network Protocol Manager 9.2.x patches, enables periodic light discovery. |
| **LiteSynchronizationInterval** | 3600 | Introduced with Network Protocol Manager 9.2.x patches, is the interval in seconds for light discovery.  
Used with EnableReconfigureLaunchedLiteSynchronization and EnablePeriodicLiteSynchronization parameters. |
Description of eigrp.conf

The eigrp.conf file contains configuration parameters that you edit to customize Network Protocol Manager for EIGRP discovery. The parameters are a subset of attributes that are defined for the topology manager (EIGRP-Adapter-Manager) that will run in the Network Protocol Manager for EIGRP environment.

Table 3 on page 30 describes the parameters in the eigrp.conf file. The parameters and their values are case-sensitive.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config</td>
<td>Regular expression: eigrp</td>
<td>Identifies this Domain Manager configuration as Network Protocol Manager for EIGRP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Do not change this parameter.</td>
</tr>
<tr>
<td>AdminDownFlag</td>
<td>TRUE, FALSE, Default: FALSE</td>
<td>Controls whether Network Protocol Manager for EIGRP generates alarms on the EIGRP sessions of EIGRP protocol endpoints that are administratively down (manually disabled).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of TRUE indicates that alarms are not generated on the EIGRP sessions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of FALSE indicates that alarms are generated on the EIGRP sessions.</td>
</tr>
<tr>
<td>ProhibitPrivLevelCLILogon</td>
<td>TRUE, FALSE, Default: FALSE</td>
<td>Controls whether the CLI login credentials for Network Protocol Manager for EIGRP are configured for Privileged mode or User mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of TRUE indicates that the credentials are configured for User mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of FALSE indicates that the credentials are configured for Privileged mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For User mode, a Privileged-mode enable password is not required when logging in to a managed device.</td>
</tr>
<tr>
<td>PrivLevel</td>
<td>enable_level_8, enable_level_1, Default: enable_level_8</td>
<td>Specified the access level of Privileged mode. PrivLevel is valid only when ProhibitPrivLevelCLILogon = FALSE.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PrivLevel = enable_level_8 configures the CLI login credentials for Privileged mode 8.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PrivLevel = enable_level_1 configures the CLI login credentials for Privileged mode 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Level 1 access is more restrictive than level 8 access. Both allow access to some information about a managed device, such as interfaces and the routes in routing tables, but neither allows configuration changes or the viewing of the running configuration file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> If you encounter discovery issues with Network Protocol Manager for EIGRP on Windows, shut down Network Protocol Manager for EIGRP, remove its repository file, set the PrivLevel parameter to enable_level_1, restart the manager, and perform a full discovery. The procedures for removing a repository file and performing a full discovery are presented in the EMC Smarts Network Protocol Manager Discovery Guide.</td>
</tr>
</tbody>
</table>
### Description of isis.conf

The isis.conf file contains configuration parameters that you edit to customize Network Protocol Manager for IS-IS discovery. The parameters are a subset of attributes that are defined for the topology manager (ISIS-Adapter-Manager) that will run in the Network Protocol Manager for IS-IS environment.

Table 4 on page 31 describes the parameters in the isis.conf file. The parameters and their values are case-sensitive.

#### Table 3 Parameters in the eigrp.conf file (page 2 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>AM</td>
<td>Indicates the type of the Domain Manager that is added as a topology source.</td>
</tr>
<tr>
<td>DomainName</td>
<td>INCHARGE-AM</td>
<td>This is the name of the IP Domain Manager that is added as a topology source.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This is the default domain name. You can use the right click option to delete it from the Domain Manager Administration Console, and then update the configuration file by commenting out the DomainName parameter.</td>
</tr>
<tr>
<td>DisplayName</td>
<td>INCHARGE-AM</td>
<td>This is the display name of the IP Domain Manager that is added as a topology source.</td>
</tr>
</tbody>
</table>

#### Table 4 Parameters in the isis.conf file (page 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config</td>
<td>Regular expression: isis</td>
<td>Identifies this Domain Manager configuration as Network Protocol Manager for IS-IS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Do not change this parameter.</td>
</tr>
<tr>
<td>AdminDownFlag</td>
<td>TRUE, FALSE</td>
<td>Controls whether Network Protocol Manager for IS-IS generates alarms on the IS-IS adjacency relationships of IS-IS interfaces that are administratively down (manually disabled).</td>
</tr>
<tr>
<td></td>
<td>Default: FALSE</td>
<td>• A value of TRUE indicates that alarms are not generated on the IS-IS adjacency relationships.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of FALSE indicates that alarms are generated on the IS-IS adjacency relationships.</td>
</tr>
<tr>
<td>ProhibitPrivLevelCLILogon</td>
<td>TRUE, FALSE</td>
<td>Controls whether the CLI login credentials for Network Protocol Manager for IS-IS are configured for Privileged mode or User mode.</td>
</tr>
<tr>
<td></td>
<td>Default: FALSE</td>
<td>• A value of TRUE indicates that the credentials are configured for User mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of FALSE indicates that the credentials are configured for Privileged mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For User mode, a Privileged-mode enable password is not required when logging in to a managed device.</td>
</tr>
</tbody>
</table>
Setting Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| PrivLevel       | enable_level_8, enable_level_1             | Specified the access level of Privileged mode. PrivLevel is valid only when ProhibitPrivLevelCLILogon = FALSE.  
• PrivLevel = enable_level_8 configures the CLI login credentials for Privileged mode 8.  
• PrivLevel = enable_level_1 configures the CLI login credentials for Privileged mode 1.  
Level 1 access is more restrictive than level 8 access. Both allow access to some information about a managed device, such as interfaces and the routes in routing tables, but neither allows configuration changes or the viewing of the running configuration file.   
**Note:** If you encounter discovery issues with Network Protocol Manager for IS-IS on Windows, shut down Network Protocol Manager for IS-IS, remove its repository file, set the PrivLevel parameter to enable_level_1, restart the manager, and perform a full discovery. The procedures for removing a repository file and performing a full discovery are presented in the EMC Smarts Network Protocol Manager Discovery Guide. |
| EnableIPv6Discovery | TRUE, FALSE                               | Determines the discovery of IPv6 topology by Network Protocol Manager for ISIS.  
• TRUE — Discovers IPv6 topology  
• FALSE — Does not discover the IPv6 topology.   
**Note:** Applicable only for BGP, OSPF and IS-IS. |
| Type            | AM                                         | Indicates the type of the Domain Manager that is added as a topology source.                                                                                                                                  |
| DomainName      | INCHARGE-AM                                 | This is the name of the IP Domain Manager that is added as a topology source.                                                                                                                                  |
| DisplayName     | INCHARGE-AM                                 | This is the display name of the IP Domain Manager that is added as a topology source.                                                                                                                              |
The ospf.conf file contains configuration parameters that you edit to customize Network Protocol Manager for OSPF discovery. The parameters are a subset of attributes that are defined for the topology manager (OSPF-Adapter-Manager) that will run in the Network Protocol Manager for OSPF environment.

Table 5 on page 33 describes the parameters in the ospf.conf file. The parameters and their values are case-sensitive.

**Table 5 Parameters in the ospf.conf file (page 1 of 2)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config</td>
<td>Regular expression: ospf</td>
<td>Identifies this Domain Manager configuration as Network Protocol Manager for OSPF.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Do not change this parameter.</td>
</tr>
<tr>
<td>TrapPort</td>
<td>0, 162, 2049 to 65534, Default: 0</td>
<td>Enables the Network Protocol Manager for OSPF built-in trap receiver, and specifies the port used by the trap receiver to receive traps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TrapPort = 0 disables the built-in trap receiver.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TrapPort = 162 or a value in the range 2049-to-65534 (inclusive) enables the built-in trap receiver and sets the trap port to the value specified for the parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“Procedure to configure the Network Protocol Manager built-in trap receiver” on page 89 clarifies the use of this parameter.</td>
</tr>
<tr>
<td>TraceTraps</td>
<td>TRUE, FALSE, Default: FALSE</td>
<td>Determines whether trap receiver tracing for Network Protocol Manager for OSPF is enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of TRUE indicates that trap receiver tracing is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of FALSE indicates that trap receiver tracing is disabled.</td>
</tr>
<tr>
<td>SyslogName</td>
<td>Regular expression</td>
<td>Enables the Network Protocol Manager for OSPF built-in syslog adapter, and specifies the name of the local syslog file to be tailed by the syslog adapter.</td>
</tr>
<tr>
<td></td>
<td>Default: empty string</td>
<td>• SyslogName = &quot;&quot; (empty string) disables the built-in syslog adapter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SyslogName = &lt;full path and name of syslog file&gt; (for example, /var/adm/messages) enables the built-in syslog adapter and sets the name of the local syslog file to be tailed to the value specified for the parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chapter 7, “Configuring Syslog Message Processing and Forwarding,” clarifies the use of this parameter.</td>
</tr>
<tr>
<td>TraceSyslog</td>
<td>TRUE, FALSE, Default: FALSE</td>
<td>Determines whether syslog adapter tracing for Network Protocol Manager for OSPF is enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of TRUE indicates that syslog adapter tracing is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of FALSE indicates that syslog adapter tracing is disabled.</td>
</tr>
</tbody>
</table>
### Setting Configuration Parameters

#### Table 5 Parameters in the ospf.conf file (page 2 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdminDownFlag</td>
<td>TRUE, FALSE</td>
<td>Controls whether Network Protocol Manager for OSPF generates alarms on the OSPF neighbor relationships of OSPF interfaces that are administratively down (manually disabled).</td>
</tr>
<tr>
<td></td>
<td>Default: FALSE</td>
<td>• A value of TRUE indicates that alarms are not generated on the OSPF neighbor relationships.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of FALSE indicates that alarms are generated on the OSPF neighbor relationships.</td>
</tr>
<tr>
<td>IsDisplayNameCustom</td>
<td>TRUE, FALSE</td>
<td>Controls whether Network Protocol Manager for OSPF accepts topology objects from the EMC Smarts Adapter for Alcatel-Lucent 5620 SAM EMS (the Adapter).</td>
</tr>
<tr>
<td></td>
<td>Default: FALSE</td>
<td>• A value of TRUE indicates that topology objects from the Adapter are accepted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A value of FALSE indicates that topology objects from the Adapter are not accepted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When the Adapter is present, set the IsDisplayNameCustom parameter to TRUE. The Adapter is described in the <em>EMC Smarts Adapter for Alcatel-Lucent 5620 SAM EMS User Guide</em>.</td>
</tr>
<tr>
<td>EnableAlertsOnDynamicOSPFLinks</td>
<td>TRUE, FALSE</td>
<td>Introduced as of Network Protocol Manager 9.2.2, for OSPFNeighborRelationship, controls whether Neighbor Down alarms are notified for both IPv4 and IPv6.</td>
</tr>
<tr>
<td></td>
<td>Default: TRUE</td>
<td>If an SNMP error occurs and the value is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TRUE — The Neighbor state is set as DOWN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FALSE — The Neighbor state is set as UNKNOWN.</td>
</tr>
<tr>
<td>EnableOSPFPassiveInterfaceDiscovery</td>
<td>TRUE, FALSE</td>
<td>Determines the discovery of OSPF passive interfaces by Network Protocol Manager for OSPF.</td>
</tr>
<tr>
<td></td>
<td>Default: TRUE</td>
<td>• TRUE — Discovers the OSPF Passive Interfaces using CLI mechanism.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FALSE — Does not discover the OSPF passive interfaces.</td>
</tr>
<tr>
<td>EnableIPv6Discovery</td>
<td>TRUE, FALSE</td>
<td>Determines the discovery of IPv6 topology by Network Protocol Manager for OSPF.</td>
</tr>
<tr>
<td></td>
<td>Default: TRUE</td>
<td>• TRUE — Enables discovery of IPv6 topology.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FALSE — Disables discovery of IPv6 topology.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Applicable only for BGP, OSPF and IS-IS.</td>
</tr>
<tr>
<td>Type</td>
<td>AM</td>
<td>Indicates the type of the Domain Manager that is added as a topology source.</td>
</tr>
<tr>
<td>DomainName</td>
<td>INCHARGE-AM</td>
<td>This is the name of the IP Domain Manager that is added as a topology source.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is the default domain name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can use the right click option to delete it from the Domain Manager Administration Console, and then update the configuration file by commenting out the DomainName parameter.</td>
</tr>
<tr>
<td>DisplayName</td>
<td>INCHARGE-AM</td>
<td>This is the display name of the IP Domain Manager that is added as a topology source.</td>
</tr>
</tbody>
</table>
Description of perl-cli.conf

The perl-cli.conf file contains the list of parameters for Perl, Telnet and SSH discovery. The perl-cli.conf file is located at BASEDIR/smarts/conf/tbgp/isis/ospf/eigrp. Table 6 on page 35 describes the parameters in the perl-cli.conf file.

**NOTICE**

For any entry in the perl-cli.conf file, do not enclose the name or value in quotes, and do not punctuate the entry with commas, semicolons, or periods.

Table 6 Parameters in the perl-cli.conf file

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_versions</td>
<td>The values can be:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• v4 — To use IPv4 addresses only.</td>
<td><strong>Note:</strong> The CLI connection is Perl-based, and not DASL based.</td>
</tr>
<tr>
<td></td>
<td>• v6—To use IPv6 addresses only.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• v4v6—To use IPv4 addresses first, and then IPv6 addresses. (Default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• v6v4—To use IPv6 addresses first, and then use IPv4 addresses.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• any—To use any type of IP address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you are running the NPM server in Windows, do not use the value:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip_versions=any</td>
<td></td>
</tr>
<tr>
<td>timeout</td>
<td>Default: 10 seconds</td>
<td>This is the timeout for establishing the connection from NPM server to the device.</td>
</tr>
<tr>
<td>get_timeout</td>
<td>Default: 0.1 seconds</td>
<td>Determines the time to fetch the information from the device through CLI.</td>
</tr>
<tr>
<td>read_timeout</td>
<td>Default: 0.1 seconds</td>
<td>Determines the time to read the information from the device through CLI.</td>
</tr>
<tr>
<td>debug</td>
<td>Default: 0</td>
<td>Determines the generation of CLI log files in the NPM server log directory.</td>
</tr>
<tr>
<td></td>
<td>• 1—Enables debugging</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0—Disables debugging</td>
<td></td>
</tr>
<tr>
<td>ssh_client</td>
<td>Default location: /usr/bin/ssh</td>
<td>Specifies the location of the SSH client in your system.</td>
</tr>
</tbody>
</table>
EMC Smarts secure communications

The security configuration files, clientConnect.conf and serverConnect.conf, located in the BASEDIR/smarts/conf directory of each EMC Smarts software installation, enable you to set up secure connections between the component applications in a Network Protocol Manager deployment. By default, the configuration option settings in the clientConnect.conf file and the serverConnect.conf files enable minimally secure connections between the components.

A Network Protocol Manager deployment that employs secure communications has the following environment variables set to the same value in each component application’s BASEDIR/smarts/local/conf/runcmd_env.sh file:

- SM_INCOMING_PROTOCOL=[1,0 or 2,0 or 3,0]
- SM_OUTGOING_PROTOCOL=[1,0 or 2,0 or 3,0]

For example:

- SM_INCOMING_PROTOCOL=2,0
- SM_OUTGOING_PROTOCOL=2,0

The *EMC Smarts System Administration Guide* presents detailed information about EMC Smarts secure communications.
CHAPTER 3
Opening the Global Console

This chapter includes procedures for opening the Global Console and describes console views. It consists of the following sections:

- Global Console overview ................................................................. 38
- User accounts and passwords ............................................................. 38
- Procedure for opening the Global Console ........................................... 39
- Procedure for opening the Global Manager Administration Console .......... 41
- Procedure for opening the Domain Manager Administration Console .......... 41
- Procedure for opening the Polling and Thresholds Console ......................... 42
Global Console overview

The Global Console is a collection of many consoles, or console views, that together enable administrators to manage EMC Smarts Domain Managers and Global Managers.

You will use the following three consoles to complete the configuration and administration tasks that are required to set up a Network Protocol Manager deployment:

- Domain Manager Administration Console

  Enables administrators to manage Domain Managers and to discover topology; for example, to add IP Availability Manager as a source to a Domain Manager.

**NOTICE**

  Using the Domain Manager Administration Console to add IP Availability Manager as a source to Network Protocol Manager is described in the *EMC Smarts Network Protocol Manager Discovery Guide*.

- Global Manager Administration Console

  Enables administrators to configure the Global Manager; for example, to set up connections to underlying Domain Managers, to enable map types that are disabled by default, or to enable server tools that are disabled by default.

- Polling and Thresholds Console

  Enables administrators to control periodic polling, to set thresholds for polled data, and to deploy and customize special groups such as CLI device-access groups.

User accounts and passwords

Attaching the Global Console to a Domain Manager (such as Network Protocol Manager for BGP) or to a Global Manager requires an EMC Smarts user account. The default user accounts are as follows:

- Administration account:
  
  - username: admin
  
  - password: changeme

- Operator account:
  
  - username: oper
  
  - password: oper

For users logged on with an administration account, the Global Console includes a Configure menu. This menu enables administrators to open the Domain Manager Administration Console and the Global Manager Administration Console.

The *EMC Smarts System Administration Guide* provides information about changing the password for the default administrative account (recommended) and configuring access privileges. The *EMC Smarts Service Assurance Manager Configuration Guide* provides information about configuring permissions to perform specific console operations.
Procedure for opening the Global Console

To open the Global Console:

1. Start the Global Console.
   - On a Windows system, select Start > Programs > InCharge > EMC Smarts Global Console.
   - On a UNIX system, go to the BASEDIR/smarts/bin directory in the Service Assurance Manager (Global Manager) installation area and type:

     `sm_gui
     Enter`

     The Attach Manager dialog box opens, as shown in Figure 5 on page 39.

     ![Attach Manager dialog box](image)

     **Figure 5** Attach Manager dialog box

2. In the dialog box:
   a. Ensure that the EMC Smarts Broker for your deployment appears in the Broker text box.
   b. Click the Manager list box or the Browse button to display a list of active (running) Managers, and from that list select a Domain Manager (for example, INCHARGE-BGP) or a Global Manager (for example, INCHARGE-SA) in your deployment as the Manager to which you want to connect.
   c. Type your login username and password.
   d. Click OK.

     A console view opens.

     What console view opens at this point depends on whether you selected a Domain Manager or a Global Manager application.

     If you selected a Domain Manager, a Topology Browser Console view of the Global Console will open by default, an example of which is shown in Figure 6 on page 40. In the example display, the Topology Browser Console is attached to a Domain Manager named INCHARGE-BGP.
Opening the Global Console

Figure 6  Topology Browser Console

If you selected a Global Manager, a Notification Log Console view of the Global Console will open by default, an example of which is shown in Figure 7 on page 41. In the example display, the Notification Log Console is attached to a Global Manager application named INCHARGE-SA.
The EMC Smarts Service Assurance Manager Operator Guide provides detailed instructions on using the Global Console.

Procedure for opening the Global Manager Administration Console

You can open a Global Manager Administration Console view from any Global Console that is attached to a Global Manager, such as the Notification Log Console in Figure 7 on page 41, by selecting the Configure > Global Manager Administration Console menu option. Figure 15 on page 62 is an example of a Global Manager Administration Console attached to a Global Manager named INCHARGE-SA.

Procedure for opening the Domain Manager Administration Console

You can open a Domain Manager Administration Console view from any Global Console that is attached to a Domain Manager, such as the Topology Browser Console in Figure 6 on page 40, by selecting the Configure > Domain Manager Administration Console menu option. Figure 8 on page 42 is an example of a Domain Manager Administration Console attached to a Domain Manager named INCHARGE-BGP.
Procedure for opening the Polling and Thresholds Console

You can open a Polling and Thresholds Console view from any Domain Manager Administration Console by selecting the Configure > Polling and Thresholds menu option. Figure 31 on page 122 is an example of a Polling and Thresholds Console attached to a Domain Manager named INCHARGE-BGP.
CHAPTER 4
Configuring IP Availability Manager

This chapter provides instructions for configuring an IP Availability Manager in a Network Protocol Manager deployment. It consists of the following sections:

- Configuration overview ................................................................. 44
- Topology and CLI device-access object import ................................. 44
- About the protocol topology collection sets ........................................ 48
- Tagged IP object import ................................................................. 48
- CLI discovery, CLI polling, and CLI device-access groups ................. 49
- Enabling protocol light discovery ..................................................... 51
- Enabling overlapping IP address discovery ....................................... 51
- Enabling interoperability with the VPN-Tagging Server ....................... 52
- Creating CLI device-access groups .................................................. 53
Configuration overview

For an IP Availability Manager in a Network Protocol Manager deployment, an administrator performs the standard configuration tasks that are presented in the EMC Smarts IP Manager documentation to prepare the IP Availability Manager application for SNMP discovery.

The administrator also performs the following additional configuration tasks to prepare IP Availability Manager for operation in a Network Protocol Manager deployment:

- Enables protocol light discovery (mandatory).
- Enables overlapping IP address discovery (optional).
- Creates CLI device-access groups to enable Network Protocol Manager to perform CLI discovery and polling of devices that cannot be discovered or monitored by using SNMP (mandatory if EIGRP- or IS-IS-enabled Cisco devices are to be managed by Network Protocol Manager).
- Configures SNMP trap integration to distribute network traps to IP Availability Manager (mandatory).

This chapter provides the background and the instructions for completing all but the last task. The instructions for completing the last task are presented in Chapter 6, “Configuring SNMP Trap Integration.”

Topology and CLI device-access object import

Upon adding IP Availability Manager as a source and every time thereafter when Network Protocol Manager starts up, Network Protocol Manager imports topology and CLI device-access objects from IP Availability Manager. The details of the Network Protocol Manager import are shown in Figure 9 on page 45.
Import of topology

As indicated in Figure 9 on page 45, Network Protocol Manager imports only the objects that it is designed to manage. To accomplish that end, IP Availability Manager, when it is configured to do so, not only performs its traditional discovery of network objects, but also creates protocol topology collection sets from the discovered network objects.

Import of CLI device-access objects

Figure 9 on page 45 also shows that Network Protocol Manager imports CLI device-access objects from IP Availability Manager.

IP Availability Manager maintains these user-created CLI device-access objects, which are required by Network Protocol Manager for CLI discovery and CLI polling of devices that cannot be discovered or monitored by using SNMP. Instructions for creating CLI device-access objects are given in “Creating CLI device-access groups” on page 53.
Configuring IP Availability Manager

Types of imported objects

Figure 10 on page 46 identifies the types of objects that are imported by Network Protocol Manager from IP Availability Manager. Network Protocol Manager imports the topology and CLI device-access objects in accordance to the dxa-am.conf file in the BASEDIR/smarts/conf/bgp|eigrp|isis|ospf directory.

**BGP-enabled devices**
- Contains SNMPv1, v2c, and v3 credentials

**EIGRP-enabled devices**
- Contains SNMPv1, v2c, and v3 credentials

**OSPF-enabled devices**
- Contains SNMPv1, v2c, and v3 credentials

**IS-IS-enabled devices**
- Contains SNMPv1, v2c, and v3 credentials

**CLI device-access groups**
- Contains SNMPv1, v2c, and v3 credentials
Through the `UnitaryComputerSystem` class in the `dxa-am.conf` file, Network Protocol Manager imports routing devices that are running BGP, EIGRP, IS-IS, or OSPF services. Those devices may be physical routers, virtual routers that are implemented within physical routers or switches, or the following types of router cards in switches:

- Route switch module (RSM)
- Route switch feature card (RSFC)
- Multilayer switch feature card (MSFC)

Through the `UnitaryComputerSystem` class in the `dxa-am.conf` file, Network Protocol Manager also imports switch devices that contain interface cards that are running BGP, EIGRP, IS-IS, or OSPF services.

`UnitaryComputerSystem` is the parent class of `Router` and `Switch`. `Router` is the parent class of MSFC, RSFC, and RSM.

IP Availability Manager discovers instances of the `Router` class and its subclasses, as well as instances of the `Switch` class. In turn, Network Protocol Manager imports the router and switch objects from IP Availability Manager, along with the network objects that are associated with the router and switch objects. Those network objects are identified in the `dxa-am.conf` file.

Also, for instances of the classes that are preceded with “proxy” in the `dxa-am.conf` file, Network Protocol Manager subscribes to routing-protocol-relevant status updates for those instances from IP Availability Manager. Table 7 on page 47 describes “proxy” and the other data exchange adapter (DXA) commands that are included in the `dxa-am.conf` file.

**Table 7 Partial list of DXA configuration commands (page 1 of 2)**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class</td>
<td><code>&lt;remote class name&gt; [local class name]</code>&lt;br&gt;Example: <code>class  IP</code></td>
<td>Identifies a class and the start of a class block that ends one line before another class block begins. A class block represents instances of a particular class and its subclasses, and contains all interested properties of those instances.</td>
</tr>
<tr>
<td>proxy</td>
<td><code>&lt;remote class name&gt; [local class name]</code>&lt;br&gt;Example: <code>proxy UnitaryComputerSystem</code></td>
<td>Same as “class” with the following additional behavior: For the specified class, all instances of the remote class will be instrumented locally. That is, the local server will continuously monitor the instrumented attributes or events of the class instances on the remote server, and reflect changes in the local objects as changes occur in the remote objects.</td>
</tr>
<tr>
<td>attr</td>
<td><code>&lt;remote attribute name&gt; [local attribute name]</code>&lt;br&gt;Example: <code>class  IP attr  DisplayName</code></td>
<td>Identifies the class attributes that are to be imported from the remote server.</td>
</tr>
<tr>
<td>rel</td>
<td><code>&lt;remote relationship name&gt; [local relationship name]</code>&lt;br&gt;Example: <code>class  IP rel  Underlying</code></td>
<td>Identifies the class relationships that are to be imported from the remote server.</td>
</tr>
</tbody>
</table>
Configuring IP Availability Manager

When the DisableProtocolDiscovery parameter in IP Availability Manager's tpmgr-param.conf file is set to FALSE, IP Availability Manager not only performs its traditional discovery of network objects, but it also creates BGP-, EIGRP-, IS-IS-, and OSPF-relevant topology collection sets from the discovered network objects. By default, it queries the SNMP agent of every device in the managed network for routing-protocol support.

The protocol light discovery feature is described in the EMC Smarts IP Manager documentation.

Tagged IP object import

Network Protocol Manager for BGP and Network Protocol Manager for OSPF are able to understand and store tagged IP objects that are imported from IP Availability Manager. Tagged IP objects enable a Domain Manager to include overlapping IP addresses in its modeled topology.

The inclusion of overlapping IP addresses in the modeled topology results in a more accurate and more complete model of the topology, which enables IP Availability Manager, Network Protocol Manager for BGP, and Network Protocol Manager for OSPF to perform more accurate correlation analysis.

Table 7  Partial list of DXA configuration commands (page 2 of 2)

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ignoreclass</td>
<td>&lt;subclass name&gt;</td>
<td>Stops the import of instances of the specified subclass from the remote server.</td>
</tr>
<tr>
<td></td>
<td>Example: class IP &lt;ignoreclass DuplicatedIP&gt;</td>
<td></td>
</tr>
<tr>
<td>in</td>
<td>&lt;container class name&gt; &lt;relation name&gt; [instance name]</td>
<td>Directs the local server to import instances that are related to a remote container-type class. The example directs the local server to import only those device instances that are members of the EIGRP-System ConsistsOf relationship.</td>
</tr>
<tr>
<td></td>
<td>Example: class UnitaryComputerSystem in TopologyCollection ConsistsOf EIGRP-System</td>
<td></td>
</tr>
<tr>
<td>probe</td>
<td>&lt;element type&gt;</td>
<td>Enables postprocessing scripts to be invoked from the local server whenever a new instance of the given class, with the specified element type, is created on the remote server.</td>
</tr>
<tr>
<td></td>
<td>Example: class SNMPAgent probe EIGRP</td>
<td></td>
</tr>
<tr>
<td>conditionalprobe</td>
<td>&lt;element type&gt; &lt;method&gt; &lt;remote attribute value&gt; &lt;same local attribute value&gt;</td>
<td>Behaves the same as “probe” when a new instance of the given class, with the specified element type, is created on the remote server. In addition, for an existing instance, “conditionalprobe” compares the value of the specified attribute in the remote instance to the same attribute in the local instance. If the value has changed in the remote instance, the probe takes place even though this instance is not new.</td>
</tr>
<tr>
<td></td>
<td>Example: class SNMPAgent conditionalprobe EIGRP getSystem DiscoveredLastAt DiscoveredLastAt</td>
<td></td>
</tr>
</tbody>
</table>
Overlapping IP addresses

In a networked environment, the same IP addresses can be reused and configured across multiple systems (devices) that are running in separate networks. These IP addresses, known as overlapping IP addresses, are prominent in (1) Multiprotocol Label Switching (MPLS) VPN environments and (2) networks that are centrally managed by Managed Service Providers, where private IP networks of customers often deploy identically numbered IP address spaces.

IP tagging feature

The IP tagging feature, which was introduced in IP Manager 7.0, enables IP Availability Manager to discover and create IP objects for both VPN Routing and Forwarding (VRF) and non-VRF overlapping IP addresses, where a non-VRF overlapping IP address is defined as an overlapping IP address that is not part of an MPLS VPN.

Network Protocol Manager for BGP and Network Protocol Manager for OSPF are able to understand VRF and non-VRF IP objects that have been tagged by IP Availability Manager.

IP Availability Manager also creates a corresponding IPNetwork object and tags it with the same value that is used to tag the IP object. And, for both tagged IP and IPNetwork objects, IP Availability Manager sets the object’s Tag attribute to the tag value that is used to tag the object.

The Route Distinguisher (RD) IP tagging policy is used in versions 8.1.x and 9.x of the IP Manager. These features are described in the EMC Smarts IP Manager documentation.

VPN-Tagging Server

The VPN-Tagging Server enables IP Availability Manager to correctly represent in its modeled topology certain VRF overlapping IP-address configurations. When the VPN-Tagging Server discovers these configurations, it sends the connection information to IP Availability Manager so that IP Availability Manager can distinguish the overlapping IP addresses in the configurations. Doing so enables IP Availability Manager to create the correct network connections for the configurations.

Creating the correct network connections means that Network Protocol Manager for BGP and Network Protocol Manager for OSPF will import more accurate topology information from IP Availability Manager.

CLI discovery, CLI polling, and CLI device-access groups

Network Protocol Manager performs CLI discovery and CLI polling to discover and monitor devices that cannot be discovered or monitored by using SNMP. As shown in Figure 11 on page 50, CLI discovery and CLI polling are controlled by CLI device-access objects that are created on the IP Availability Manager, through the Polling and Thresholds Console, and then imported by Network Protocol Manager.
Figure 11  CLI discovery, CLI polling, and CLI device-access object creation and transfer

The execution of CLI discovery and CLI polling requires login credentials, which are used by Network Protocol Manager to access the Network Protocol-enabled devices and to invoke CLI commands from the devices. The CLI device-access objects carry the login credential information.

Instructions for creating CLI device access objects for Network Protocol Manager are given in “Creating CLI device-access groups” on page 53.
Enabling protocol light discovery

By default, IP Availability Manager is not enabled to perform protocol light discovery. To enable this feature, set the DisableProtocolDiscovery parameter in IP Availability Manager’s tpmgr-param.conf file to FALSE.

To enable protocol light discovery:
1. Go to the BASEDIR/smarts/bin directory in the IP Manager installation area and type the following command to open the tpmgr-param.conf file:

   `sm_edit conf/discovery/tpmgr-param.conf`

   Press Enter.

2. Set the following parameter to FALSE:
   
   `DisableProtocolDiscovery FALSE`

3. Save and close the file.

   The modified version of the tpmgr-param.conf file is saved to the BASEDIR/smarts/local/conf/discovery directory.

4. If IP Availability Manager was running before you edited the tpmgr-param.conf file, type the following command from BASEDIR/smarts/bin to make your change take effect:

   `sm_tpmgr -s <IP Availability Manager instance name> --load-conf=tpmgr-param.conf`

   Press Enter.

---

Enabling overlapping IP address discovery

**NOTICE**

This procedure is not applicable for IP Availability Manager versions 8.1.x and higher. The VPNIP attribute has been deprecated in release 8.1.x and 9.x. Refer to the Route Distinguisher (RD) IP tagging policy configuration procedures in the *EMC Smarts IP Manager Concepts Guide*.

By default, IP Availability Manager releases prior to version 8.1.x are not enabled to perform overlapping IP address discovery. To enable this feature, set the following parameters in IP Availability Manager’s tpmgr-param.conf file to the shown values:

- `DisableOverlappingIP FALSE`
- `UseVPNIP FALSE`
- `EnableShadowIP TRUE` (default)

To enable overlapping IP discovery:
1. Go to the BASEDIR/smarts/bin directory in the IP Manager installation area and type the following command to open the tpmgr-param.conf file:

   `sm_edit conf/discovery/tpmgr-param.conf`

   Press Enter.
2. Set the following three parameters to the values shown:

EnableDisablingIP False
UseVPNIP FALSE
EnableShadowIP TRUE

3. Save and close the file.

The modified version of the tpmgr-param.conf file is saved to the BASEDIR/smarts/local/conf/discovery directory.

4. If IP Availability Manager was running before you edited the tpmgr-param.conf file, type the following command from BASEDIR/smarts/bin to make your change take effect:

```
sm_tpmgr -s <IP Availability Manager instance name> --load-conf=tpmgr-param.conf
```

Press Enter.

## Enabling interoperability with the VPN-Tagging Server

To enhance overlapping IP address discovery, you, as an administrator, enable IP Availability Manager to interoperate with the VPN-Tagging Server.

Assuming that the DisableDisablingIP, UseVPNIP, and EnableShadowIP parameters in the tpmgr-param.conf file are set as specified in the previous section, you do so by setting the following parameter in IP Availability Manager’s discovery.conf file to TRUE:

```
importExternalTagsConnections TRUE
```

In addition, you need to enable the VPN-Tagging Server to interoperate with IP Availability Manager. You do so by adding IP Availability Manager as a source to the VPN-Tagging Server.

To enable interoperability between IP Availability Manager and the VPN-Tagging Server:

1. Consult the EMC Smarts IP Manager documentation and follow the instructions to set the following parameter in the discovery.conf file to the value shown:

```
importExternalTagsConnections TRUE
```

2. Consult the *EMC Smarts IP Manager Concepts Guide* and follow the instructions to add IP Availability Manager as a source to the VPN-Tagging Server.

The VPN-Tagging Server performs overlapping-IP and corresponding network-connection discovery in two vendor-specific environments: Cisco and Alcatel-Lucent. To complete the configuration of the VPN-Tagging Server, open the BASEDIR/smarts/conf/vpn-tagging/vpn-tagging.conf file (in the Network Protocol Manager installation area) and perform the following additional tasks:

- **Mandatory and for Alcatel-Lucent only:** Add the Enable5620SAMDiscovery parameter with a value of TRUE to the vpn-tagging.conf file.
- **Optional and for Alcatel-Lucent only:** Modify the default values of the AlcatelDiscoveryInterval parameter.
- **Optional and for Cisco only:** Modify the default values of the DiscoveryFilter parameter.
Creating CLI device-access groups

Because IP Availability Manager is a component of many EMC Smarts deployments, IP Availability Manager has been selected as the central repository for specifying and storing device-access credentials, such as the login credentials that are required by Network Protocol Manager to perform CLI discovery and CLI polling.

When Network Protocol Manager adds IP Availability Manager as a source, Network Protocol Manager imports the device-access credentials from IP Availability Manager and makes the credentials available to the CLI discovery driver and the CLI poller.

You, as an administrator, use the Polling and Thresholds Console to specify sets of device-access credentials in the form of CLI device-access groups. Each CLI device-access group contains:

- An access-protocol method: Telnet, SSH1, or SSH2; Telnet, by default.
- A set of device-access credentials: a username, a user password, and a privileged-mode enable password.
- A set of member devices for which the access method and device-access credentials apply.

Attach the Polling and Thresholds Console

Upon attaching the Polling and Thresholds Console to IP Availability Manager, you use the Device Access tab, the CLI Access Group, and the CLI Access Setting on the Polling and Thresholds Console to specify the CLI device-access groups.

If your Network Protocol Manager deployment contains multiple IP Availability Managers, proceed as follows:

1. Choose one of those IP Availability Managers as the target IP Availability Manager.
2. Attach the Polling and Thresholds Console to the target IP Availability Manager and create all the CLI device-access groups for the deployment on that one server.

Creating CLI device-access groups on different IP Availability Managers can lead to matching-criteria priority conflicts between the groups.

Create CLI device-access groups

You create a CLI device-access group for each group of managed devices that is configured with a different access protocol and/or different set of CLI login credentials. The assumption is that all devices that use a particular access protocol are configured with the same set of credentials (and timeout value). If there are two groups of devices that use a particular access protocol, each configured with its own set of credentials, you would create two CLI device-access groups for that particular access protocol. For example, you would create two CLI device-access groups named SSH2_S1 and SSH2_S2. The matching criteria for each of the groups would limit the group's members to the appropriate devices.
### Table 8 Default values for the CLI Access Setting

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessProtocol</td>
<td>TELNET, SSH1, SSH2 Default: TELNET</td>
<td>Determines the remote-access application to use to establish connections to the managed devices that belong to this group. Secure Shell 2 (SSH2) is recommended. The Network Protocol Manager includes Telnet client software, and for installations on Windows systems, also includes SSH client software. Instructions for configuring an SSH client are given in Chapter 8, “Configuring SSH Security.”</td>
</tr>
<tr>
<td>LoginID</td>
<td>String of unspecified length Default: null string (empty)</td>
<td>Specifies the username (user ID) for the managed devices that belong to this group. You must enter a value for this parameter.</td>
</tr>
<tr>
<td>Password</td>
<td>A structure that has the following default value: (NULL String, ENCRYPTED)</td>
<td>Specifies the user password for the managed devices that belong to this group. If the managed devices that belong to this group are configured for passwordless authentication, or if the access protocol for this group is SSH1 or SSH2 and passwordless authentication is in effect, leave this parameter blank. Otherwise, enter the password twice to confirm the password value. <strong>Note:</strong> IP Availability Manager uses the site key to encrypt the entered password value. As explained in <em>EMC Smarts System Administration Guide</em>, the site key is created during the installation of EMC Smarts applications.</td>
</tr>
<tr>
<td>PrivilegedModePassword</td>
<td>A structure that has the following default value: (NULL String, ENCRYPTED)</td>
<td>Specifies the Privileged-mode enable password for the managed devices that belong to this group. For Privileged-mode access (not User-mode access), and assuming that the ProhibitPrivLevelCLILogon parameter in the eigrp.conf file (Table 3 on page 30) or the isis.conf file (Table 4 on page 31) is FALSE (default), you must enter a value for this parameter. Enter the password twice to confirm the password value. <strong>Note:</strong> IP Availability Manager uses the site key to encrypt the entered password value. As explained in <em>EMC Smarts System Administration Guide</em>, the site key is created during the installation of EMC Smarts applications.</td>
</tr>
<tr>
<td>Timeout</td>
<td>1 to 496 seconds Default: 10 seconds</td>
<td>Sets the amount of time to wait for a Telnet/SSH response before the Telnet/SSH session request times out.</td>
</tr>
</tbody>
</table>
Synchronize CLI credentials between IP and NPM

When you finish editing the properties of CLI device-access groups, follow these procedures in IP Availability Manager to ensure changes in CLI credentials are synchronized with your Network Protocol Manager servers.

1. Click the **Apply** button to save the configuration changes to an existing group object or to a newly created group object in the repository of IP Availability Manager.

2. Click the **Reconfigure** toolbar button (described in Table 11 on page 113) to make the configuration changes take effect.

3. **Rediscover** those devices affected by the change in credentials.

When the IP discovery process completes, the Network Protocol Manager discovery process automatically starts. Network Protocol Manager imports the group object and saves the group object to its repository.

Network Protocol Manager synchronizes its CLI-device-access group and group-related objects with the CLI-device-access group and group-related objects on IP Availability Manager.

**NOTICE**

There may be an 8-minute delay before the credentials are synchronized between the IP and NPM servers.
CHAPTER 5
Configuring the Global Manager

This chapter provides instructions for configuring the Global Manager in a Network Protocol Manager deployment. It consists of the following sections:

◆ Configuration overview ................................................................. 58
◆ About the Global Manager ............................................................... 58
◆ IC Domain Configuration objects .................................................. 61
◆ Loading the XML configuration file for Network Protocol Manager .......... 64
◆ Specifying the underlying domains .................................................. 65
◆ Enabling the display of BGP, EIGRP, IS-IS, and OSPF topology maps .......... 75
Configuration overview

For the Global Manager to import topology and events from the underlying components in a Network Protocol Manager deployment, you must configure the Global Manager with the proper data exchange adapter (DXA) files. The Global Manager integrates and correlates the imported topology and events, and relates the data to services and customers.

You use the Global Console to configure the DXA files. The *EMC Smarts Service Assurance Manager Configuration Guide* provides detailed instructions on using the Global Console to complete Global Manager configurations.

**NOTICE**

The Global Manager and Global Console are part of the EMC Smarts Service Assurance Manager.

About the Global Manager

Most of the configuration tasks for configuring the Global Manager in a Network Protocol Manager deployment are accomplished by using the Global Manager Administration Console view of the Global Console. *Figure 12 on page 59* summarizes the Global Manager Administration Console interaction with the Global Manager.
Figure 12  Global Manager Administration Console interaction with the Global Manager

As shown in Figure 12, the initial configurations for the Global Manager are stored in the ics-default.xml file and imported into the Global Manager’s repository when the Global Manager starts up. The configurations displayed in a newly started Global Manager Administration Console are exported from the Global Manager’s repository.

Figure 13 on page 60 shows the relationships between Domain Group, Domain, Domain Type, and Domain Tag configuration objects. The intent of the Domain Group is to represent the server components of a split-server Domain Manager as a single entity. Doing so makes a split-server Domain Manager look just like a standalone Domain Manager to administrators and users.
Figure 13 IC Domain Configuration objects and their relationships

Figure 14 on page 61 identifies the default Network Protocol Manager, IP Availability Manager, and Adapter Platform domain configurations held by the Global Manager. The default names for the respective domains are:

- INCHARGE-BGP
- INCHARGE-EIGRP
- INCHARGE-ISIS
- INCHARGE-OSPF
Each of these domain names represents a standalone Domain Manager.

Directed lines (→) represent Relationships

Figure 14  Default domain configurations for a Network Protocol Manager deployment

IC Domain Configuration objects

Figure 15 on page 62 presents an example display of a Global Manager Administration Console attached to a Global Manager named INCHARGE-SA.
Configuring the Global Manager

Listed at the bottom of the configuration tree of the Global Manager Administration Console are the four categories of IC Domain Configuration objects: Domains, Domain Groups, Domain Tags, and Domain Types. Listed under each category are instances of these objects; for example, the default domain “INCHARGE-AM” is listed under Domains. Selecting an object in the left panel displays its attributes and their values in the right panel.

IC Domain Configuration creation wizards

Each IC Domain Configuration category has an associated creation wizard to simplify how to specify its configuration objects. You launch an IC Domain Configuration wizard in one of three ways:

- By clicking one of the four wizard toolbar buttons that are identified in Figure 15 on page 62
- By right-clicking an IC Domain Configuration category name (for example, right-clicking Domains) and then clicking the pop-up menu
- By selecting New Domain, New Domain Group, New Domain Type, or New Domain Tag from the Edit menu

When you create a domain, the created domain is enabled automatically.
IC Domain Configuration server reconfiguration

Clicking the Apply button, which is available to all configuration categories, writes configuration changes to the Global Manager’s repository. Clicking the Reconfigure button, which is available only to the IC Domain Configuration categories, calls a “reconfigure” method that determines which underlying domains need to be synchronized or resynchronized (that is, determines from which underlying domains topology or events need to be imported or reimported) and then initiates the needed data transfers. Calling the reconfigure method is referred to as “reconfiguring the Global Manager.”

In addition to clicking the Reconfigure button, the reconfigure method can be initiated in two other ways: by clicking the Reconfigure toolbar button that is identified in Figure 15 on page 62, or by selecting Reconfigure Server from the Configure menu.

Figure 16 on page 63 demonstrates how reconfiguring the Global Manager works.
Loading the XML configuration file for Network Protocol Manager

By default, the XML domain configuration file for Network Protocol Manager is not loaded into the Global Manager, which means that by default Network Protocol Manager is not available to a Global Console attached to the Global Manager. You use the Import XML Domain Configuration server tool that is shown in Figure 17 on page 64 to load it.

1. Attach the Global Manager Administration Console to the target Global Manager.

   Instructions for opening the Global Manager Administration Console are presented in Chapter 3, “Opening the Global Console.”

2. Select File > New > Topology Browser Console to launch a Topology Browser Console.

3. In the Topology Browser Console, expand the topology tree to display the InChargeDomain objects.

4. Right-click the local InChargeDomain object that represents the Global Manager (for example, INCHARGE-SA (Local)) and select Server Tools > Import XML Domain Configuration from the pop-up menu.

   The Import XML Domain Configuration dialog box appears.

5. To load the XML domain configuration file for Network Protocol Manager, type npm in the Domain Type Descriptor field and click OK.

6. Switch back to the Global Manager Administration Console.
7. In the left panel of the Global Manager Administration Console, expand the configuration tree to display the Domains.

The Network Protocol Manager domains appear in the Domains list as INCHARGE-BGP, INCHARGE-EIGRP, INCHARGE-ISIS, and INCHARGE-OSPF. Because the names appear as gray text, the domains are disabled.

8. Continue with the procedures in "Specifying the underlying domains" on page 65.

Specifying the underlying domains

An administrator uses the IC Domain Configuration objects to specify the underlying Network Protocol Manager, IP Availability Manager, and Adapter Platform domains in a Network Protocol Manager deployment. Doing so provides the sources of topology and events for the Global Manager and associates each underlying domain with the proper DXA file.

The expectation is that a user will either accept the default Network Protocol Manager domains named INCHARGE-BGP, INCHARGE-EIGRP, INCHARGE-ISIS, and INCHARGE-OSPF, or make copies of the default domains to create new domains that have a different name. For example, you can make a copy of INCHARGE-BGP and name it ASIA-INCHARGE-BGP.

This section provides procedures for the following two configuration scenarios:

- **Configuration scenario 1:** A Network Protocol Manager deployment that contains:
  - A Network Protocol Manager for BGP named INCHARGE-BGP
  - A Network Protocol Manager for EIGRP named INCHARGE-EIGRP
  - A Network Protocol Manager for IS-IS named INCHARGE-ISIS
  - A Network Protocol Manager for OSPF named INCHARGE-OSPF
  - An IP Availability Manager named INCHARGE-AM
  - An Adapter Platform named INCHARGE-OI
Configuration scenario 2: A Network Protocol Manager deployment that contains:

- A Network Protocol Manager for BGP named EAST-INCHARGE-BGP
- An IP Availability Manager named EAST-INCHARGE-AM
- An Adapter Platform named EAST-INCHARGE-OI

To specify the underlying domains in a more complex Network Protocol Manager deployment, consult the *EMC Smarts Service Assurance Manager Configuration Guide*.

Specify the underlying domains for configuration scenario 1

By default, after loading Network Protocol Manager, as described in “Loading the XML configuration file for Network Protocol Manager,” INCHARGE-BGP, INCHARGE-EIGRP, INCHARGE-ISIS, and INCHARGE-OSPF are disabled. Also, by default, INCHARGE-AM is enabled, and INCHARGE-OI is disabled. The names of disabled domains appear as gray text in the Global Manager Administration Console, and the names of enabled domains appear as black text.

*Figure 18 on page 66* previews the configuration changes for configuration scenario 1.

---

**Figure 18** Before and after completing configuration scenario 1

During its initial startup the Global Manager performs the following tasks:

- Creates an InChargeDomain object named INCHARGE-AM and starts the appropriate topology and event drivers.
- Consults the EMC Smarts Broker for the deployment and establishes a connection to the INCHARGE-AM application.
- Subscribes to and imports topology and events from the INCHARGE-AM application.
Every time that the Global Manager is restarted, it automatically initiates a server reconfiguration (that is, calls the reconfigure method) to align the IC domain and domain group configuration objects with the InCharge domain and domain group objects. Because the only IC Domain Configuration object enabled at the initial startup is INCHARGE-AM, the only alignment that is required is the one just described.

If the synchronization with the INCHARGE-AM application fails, or if no IP Availability Manager application named INCHARGE-AM exists in the deployment, the Global Manager writes an error message to its log file.

This section consists of the following procedures:

- “Procedure for specifying the underlying INCHARGE-BGP domain for configuration scenario 1”
- “Procedure for specifying the underlying INCHARGE-EIGRP domain for configuration scenario 1”
- “Procedure for specifying the underlying INCHARGE-ISIS domain for configuration scenario 1”
- “Procedure for specifying the underlying INCHARGE-OSPF domain for configuration scenario 1”
- “Procedure for specifying the underlying INCHARGE-OI domain for configuration scenario 1”
- “Procedure for reconfiguring the Global Manager for configuration scenario 1”

Procedure for specifying the underlying INCHARGE-BGP domain for configuration scenario 1
To specify the underlying INCHARGE-BGP domain for configuration scenario 1:

1. Attach the Global Manager Administration Console to the target Global Manager.
   Instructions for opening the Global Manager Administration Console are presented in Chapter 3, “Opening the Global Console.”
2. In the left panel of the Global Manager Administration Console, expand the configuration tree to display the Domains objects.
3. Select INCHARGE-BGP to display its configuration window.
4. In the configuration window, click the Enabled checkbox.
5. In the configuration window, click Apply to save your configuration changes.
6. In the Server Reconfiguration information dialog box that appears, click OK.

Procedure for specifying the underlying INCHARGE-EIGRP domain for configuration scenario 1
To specify the underlying INCHARGE-EIGRP domain for configuration scenario 1:

1. In the left panel of the Global Manager Administration Console, expand the configuration tree to display the Domains objects.
2. Select INCHARGE-EIGRP to display its configuration window.
3. In the configuration window, click the Enabled checkbox.
Configuring the Global Manager

4. In the configuration window, click **Apply** to save your configuration changes.

5. In the **Server Reconfiguration** information dialog box that appears, click **OK**.

Procedure for specifying the underlying INCHARGE-ISIS domain for configuration scenario 1

To specify the underlying INCHARGE-ISIS domain for configuration scenario 1:

1. In the left panel of the Global Manager Administration Console, expand the configuration tree to display the **Domains** objects.

2. Select **INCHARGE-ISIS** to display its configuration window.

3. In the configuration window, click the **Enabled** checkbox.

4. In the configuration window, click **Apply** to save your configuration changes.

5. In the **Server Reconfiguration** information dialog box that appears, click **OK**.

Procedure for specifying the underlying INCHARGE-OSPF domain for configuration scenario 1

To specify the underlying INCHARGE-OSPF domain for configuration scenario 1:

1. In the left panel of the Global Manager Administration Console, expand the configuration tree to display the **Domains** objects.

2. Select **INCHARGE-OSPF** to display its configuration window.

3. In the configuration window, click the **Enabled** checkbox.

4. In the configuration window, click **Apply** to save your configuration changes.

5. In the **Server Reconfiguration** information dialog box that appears, click **OK**.

Procedure for specifying the underlying INCHARGE-OI domain for configuration scenario 1

To specify the underlying INCHARGE-OI domain for configuration scenario 1:

1. In the left panel of the Global Manager Administration Console, expand the configuration tree to display the **Domains** objects.

2. Select **INCHARGE-OI** to display its configuration window.

3. In the configuration window, click the **Enabled** checkbox.

4. In the configuration window, click **Apply** to save your configuration changes.

5. In the **Server Reconfiguration** information dialog box that appears, click **OK**.

Procedure for reconfiguring the Global Manager for configuration scenario 1

To reconfigure the Global Manager for configuration scenario 1:

1. In the toolbar area of the Global Manager Administration Console, click the **Reconfigure** toolbar button.

2. In the **Server Reconfiguration** confirmation dialog box that appears, click **Yes**.

3. In the **Server Reconfiguration** information dialog box that appears, click **Close**.

In response, the Global Manager:

- Creates an InChargeDomain object named INCHARGE-BGP and starts the appropriate topology and event drivers.
◆ Creates an InChargeDomain object named INCHARGE-EIGRP and starts the appropriate topology and event drivers.

◆ Creates an InChargeDomain object named INCHARGE-ISIS and starts the appropriate topology and event drivers.

◆ Creates an InChargeDomain object named INCHARGE-OSPF and starts the appropriate topology and event drivers.

◆ Creates an InChargeDomain object named INCHARGE-OI and starts the appropriate notification drivers.

◆ Consults the EMC Smarts Broker for the deployment and establishes a connection to the INCHARGE-BGP, INCHARGE-EIGRP, INCHARGE-ISIS, INCHARGE-OSPF, and INCHARGE-OI domains.

◆ Subscribes to and imports topology and events from the INCHARGE-BGP, INCHARGE-EIGRP, INCHARGE-ISIS, INCHARGE-OSPF domains.

◆ Subscribes to and imports notifications from the INCHARGE-OI domain.

The Global Manager will establish an additional connection to the INCHARGE-BGP, INCHARGE-EIGRP, INCHARGE-ISIS, or INCHARGE-OSPF domain under any of the following circumstances:

◆ To obtain the latest object attribute values for display in the Details tab of a routing-protocol Notification Properties dialog box.

◆ To obtain the latest object attribute values for display in a routing-protocol Containment dialog box.
Specify the underlying domains for configuration scenario 2

Figure 19 on page 70 previews the configuration changes for configuration scenario 2.

Figure 19  Before and after completing configuration scenario 2

This section consists of the following procedures:

- “Procedure for specifying the underlying EAST-INCHARGE-BGP domain for configuration scenario 2”
- “Procedure for specifying the underlying EAST-INCHARGE-AM domain for configuration scenario 2”
- “Procedure for specifying the underlying EAST-INCHARGE-OI domain for configuration scenario 2”
- “Procedure for reconfiguring the Global Manager for configuration scenario 2”
Procedure for specifying the underlying EAST-INCHARGE-BGP domain for configuration scenario 2
To specify the underlying EAST-INCHARGE-BGP domain for configuration scenario 2:

1. Attach the Global Manager Administration Console to the target Global Manager.
   Instructions for opening the Global Manager Administration Console are presented in Chapter 3, “Opening the Global Console.”

2. In the left panel of the Global Manager Administration Console, right-click Domains and then click the pop-up menu to launch the Domain Creation Wizard.

3. Consult Figure 20 on page 72 and follow the directions to create a Network Protocol Manager domain named EAST-INCHARGE-BGP.

Procedure for specifying the underlying EAST-INCHARGE-AM domain for configuration scenario 2
To specify the underlying EAST-INCHARGE-AM domain for configuration scenario 2:

1. In the left panel of the Global Manager Administration Console, right-click Domains and then click the pop-up menu to launch the Domain Creation Wizard.

2. Consult Figure 21 on page 73 and follow the directions to create an IP Availability Manager domain named EAST-INCHARGE-AM.

Procedure for specifying the underlying EAST-INCHARGE-OI domain for configuration scenario 2
To specify the underlying EAST-INCHARGE-OI domain for configuration scenario 2:

1. In the left panel of the Global Manager Administration Console, right-click Domains and then click the pop-up menu to launch the Domain Creation Wizard.

2. In the Domain Creation Wizard, select INCHARGE-OI from the Copy Existing drop-down menu, type EAST-INCHARGE-OI in the Domain Name text field, and click Next.

3. Consult Figure 21 on page 73 and use the directions as a guide to create the Adapter Platform domain named EAST-INCHARGE-OI.
An empty Tag String field causes the wizard to skip the Select Domain Tag panel.

This panel is applicable to server component domains only.

Figure 20 Using the Domain Creation Wizard to create the EAST-INCHARGE-BGP domain
An empty Tag String field causes the wizard to skip the Select Domain Tag panel.

This panel is applicable to server component domains only.

---

**Figure 21** Using the Domain Creation Wizard to create the EAST-INCHARGE-AM domain
Procedure for reconfiguring the Global Manager for configuration scenario 2

To reconfigure the Global Manager for configuration scenario 2:

1. In the toolbar area of the Global Manager Administration Console, click the **Reconfigure** toolbar button.
2. In the **Server Reconfiguration** confirmation dialog box that appears, click **Yes**.
3. In the **Server Reconfiguration** information dialog box that appears, click **Close**.

In response, the Global Manager:

- Creates an InChargeDomain object named EAST-INCHARGE-BGP and starts the appropriate topology and event drivers.
- Creates an InChargeDomain object named EAST-INCHARGE-AM and starts the appropriate topology and event drivers.
- Creates an InChargeDomain object named EAST-INCHARGE-OI and starts the appropriate notification drivers.
- Consults the EMC Smarts Broker for the deployment and establishes a connection to the EAST-INCHARGE-BGP, EAST-INCHARGE-AM, and EAST-INCHARGE-OI domains.
- Subscribes to and imports topology and events from the EAST-INCHARGE-BGP and EAST-INCHARGE-AM domains.
- Subscribes to and imports notifications from the EAST-INCHARGE-OI domain.

The Global Manager will establish an additional connection to the EAST-INCHARGE-BGP domain under any of the following circumstances:

- To obtain the latest object attribute values for display in the Details tab of a routing-protocol Notification Properties dialog box.
- To obtain the latest object attribute values for display in a routing-protocol Containment dialog box.

Similarly, the Global Manager will establish an additional connection to the EAST-INCHARGE-AM domain under any of the following circumstances:

- To obtain the latest object attribute values for display in the Details tab of an IP Notification Properties dialog box.
- To obtain the latest object attribute values for display in an IP Containment dialog box.

**NOTICE**

Because no IP Availability Manager application named INCHARGE-AM is running in configuration scenario 2, users should disable the INCHARGE-AM domain for this scenario.
Enabling the display of BGP, EIGRP, IS-IS, and OSPF topology maps

As described in the individual Network Protocol Manager user guides, you can use BGP, EIGRP, IS-IS, and OSPF topology maps to view graphical representations of the Network Protocol Manager topology that is imported by the Global Manager. By default, the display of these maps is disabled.

To enable the display of BGP, EIGRP, IS-IS, and OSPF topology maps and to associate this functionality to user profiles:

1. Attach the Global Manager Administration Console to the target Global Manager.
   Instructions for opening the Global Manager Administration Console are presented in Chapter 3, “Opening the Global Console.”

2. In the left panel of the Global Manager Administration Console, expand the configuration tree to display the User Profiles.

3. Select a user profile (for example, admin-profile, as shown in Figure 22 on page 75) to display its configuration window.

4. In the configuration window, locate Console Operations and click its Modify List button to launch the Console Operations dialog box (Figure 23 on page 76).
5. In the **Console Operations** dialog box, expand the **Map** option and click the following checkboxes:

   - BGP Connectivity
   - OSPF Connectivity
   - OSPF Network Connectivity
   - EIGRP Connectivity
   - EIGRP Network Connectivity
   - ISIS Connectivity
   - ISIS Network Connectivity

   **NOTICE**
   
   The default option at the bottom of the dialog box is Other; do not change this default.

6. Click **OK** to close the **Console Operations** dialog box.

7. In the configuration window, click **Apply** to save your configuration changes.

8. Repeat steps 3 through 7 to enable the display of BGP, EIGRP, IS-IS, and OSPF topology maps for any other user profiles that need to see these maps.

9. Detach and reattach the Global Console to the Global Manager in order to view the BGP, EIGRP, IS-IS, and OSPF maps. Start by selecting **Manager > Detach**.
CHAPTER 6
Configuring SNMP Trap Integration

This chapter provides instructions for configuring the SNMP trap integration in a Network Protocol Manager deployment. It consists of the following sections:

- Configuration overview ................................................................. 78
- SNMP trap-integration components ................................................. 79
- Trap adapter configuration file: trapd.conf ........................................ 81
- Configuring the SNMP trap-integration components ...................... 85
- Starting the SNMP trap-integration components ......................... 91
Configuring SNMP Trap Integration

**Configuration overview**

The recommended SNMP trap-integration design for a Network Protocol Manager deployment is shown in Figure 24 on page 78.

![Figure 24 Recommended trap-integration design](image)

Configuring the SNMP trap integration involves configuring and starting the various components that receive, distribute, and process the traps within a Network Protocol Manager deployment.
SNMP trap-integration components

The SNMP trap integration in a Network Protocol Manager deployment is accomplished by using the following types of components:

- **“Built-in trap receiver”** — part of most EMC Smarts Domain Managers
- **“SNMP Trap Adapter”** — part of the Service Assurance Manager
- **“Adapter Platform”** — part of the Service Assurance Manager

**Built-in trap receiver**

A Network Protocol Manager’s built-in trap receiver receives SNMPv1 and v2c trap messages from managed BGP- or OSPF-enabled devices through the SNMP Trap Adapter that is configured as a trap exploder. The built-in trap receiver forwards these traps to internal processing software, which parses the traps for status updates and applies the updates to attributes of objects in the Network Protocol Manager modeled topology.

By default, the built-in trap receiver is disabled, and should be enabled only if Network Protocol Manager for BGP or Network Protocol Manager for OSPF is running in the deployment:

- Network Protocol Manager for BGP uses received BGP traps to update attributes of the BGP objects in its modeled topology.
- Network Protocol Manager for OSPF uses received OSPF traps to update attributes of OSPF objects in its modeled topology.

The built-in trap receiver is enabled for Network Protocol Manager for BGP or Network Protocol Manager for OSPF by setting the “TrapPort = 0” parameter line in the bgp.conf or ospf.conf file to a valid trap listening port.

**SNMP Trap Adapter**

The SNMP Trap Adapter, which is part of the Service Assurance Manager, can be configured to forward traps, or can be configured to convert traps to EMC Smarts notifications.

Two instances of the SNMP Trap Adapter appear in a Network Protocol Manager deployment:

- One instance, called a “trap exploder,” that is configured to forward traps

  **NOTICE**

  A trap exploder is also known as a “trap forwarder.”

- Another instance, called a “trap receiver,” that is configured to convert traps

**Trap exploder operation**

The *EMC Smarts Service Assurance Manager Adapter Platform User Guide* describes the operation of an SNMP Trap Adapter that is configured as a trap exploder. The operation is based on the parameter settings in the trapd.conf file that is described in “Trap adapter configuration file: trapd.conf” on page 81.
In a Network Protocol Manager deployment (Figure 24 on page 78), the trap exploder receives SNMPv1, v2c, or v3 traps from the managed network devices on its trap listening port (9000 by default), and:

- Forwards copies of received BGP traps to Network Protocol Manager for BGP, to be used by Network Protocol Manager for BGP for analysis purposes.
- Forwards copies of received OSPF traps to Network Protocol Manager for OSPF, to be used by Network Protocol Manager for OSPF for analysis purposes.
- Forwards copies of received network traps to IP Availability Manager, to be used by IP Availability Manager for analysis purposes.
- Forwards copies of received useful or interesting traps to the trap receiver, to be used by users for informational purposes.

When a trap arrives, the trap exploder reads the uncommented FORWARD entries in the trapd.conf file to determine which destinations should receive the forwarded trap. When the criteria of the trap matches the criteria of a FORWARD entry, the trap exploder:

- Translates the trap in accordance to Table 9 on page 80.
- Sends a copy of the forwarded trap to each destination specified in the FORWARD entry.

<table>
<thead>
<tr>
<th>Incoming trap message version</th>
<th>Forwarded trap message version</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1</td>
<td>v1</td>
</tr>
<tr>
<td>v2c</td>
<td>v2c</td>
</tr>
<tr>
<td>v3</td>
<td></td>
</tr>
</tbody>
</table>

The trap exploder authenticates and decrypts received SNMPv3 traps, converts them to SNMPv2c traps, and forwards the SNMPv2c traps to the configured destinations. The trap exploder uses the authentication and privacy credentials obtained from a seed file, which is typically a copy of the seed file maintained by an IP Availability Manager for discovery purposes, to authenticate and decrypt SNMPv3 traps.

Trap receiver operation

The *EMC Smarts Service Assurance Manager Adapter Platform User Guide* describes the operation of a SNMP Trap Adapter that is configured as a trap receiver. The operation is based on the parameter settings in the trap_mgr.conf file in the BASEDIR/smarts/conf/icoi directory in the Service Assurance Manager installation area.

The purpose of the trap receiver is to collect and parse informational traps received from the trap exploder, and to generate EMC Smarts notifications, through the Adapter Platform, for input to the Global Manager. Through the Global Console, administrators and operators view and acknowledge the trap notifications.
Adapter Platform

The Adapter Platform imports and normalizes topology from IP Availability Manager, and imports and normalizes events of interest from EMC Smarts adapters such as the SNMP Trap Adapter. Normalize means to convert topology or event information into a common form that is understood by the Global Manager. The normalized event information is transferred as EMC Smarts notifications to the Global Manager.

Through the Adapter Platform, the Global Manager receives informational traps issued by the devices in the managed network. Informational traps provide information that might be of interest to users.

Trap adapter configuration file: trapd.conf

The trapd.conf file, located in the BASEDIR/smarts/conf/trapd directory of all EMC Smarts product installations, is a global configuration file. It is used to configure most EMC Smarts built-in trap receivers and most trap adapters (sm_trapd). Only the PORT parameter in this file is applicable to built-in trap receivers because the built-in trap receivers are configured to receive and parse traps, but not to forward traps. The other parameters in the file are applicable for configuring trap adapters to forward traps.

**NOTICE**

The built-in trap receiver for Network Protocol Manager is not controlled by the trapd.conf file. The only user-configurable control for the built-in trap receiver is the "TrapPort = 0" parameter line in the bgp.conf and ospf.conf files.

Figure 25 on page 81 shows the trap exploder’s configuration directory, in the Service Assurance Manager installation area, and the trap exploder’s trapd.conf file. A trapd.conf file in the local area takes precedence over the original trapd.conf file, which contains the installed defaults. A seedfile is required only if the trap exploder is to process SNMPv3 traps.
The following portions of the trapd.conf file are of interest to this discussion. Table 10 on page 83 presents detailed descriptions of the configuration parameters in the trapd.conf file.

```
# trapd.conf - Configuration file for SNMP Trap Adapter
#
# Following is a list of parameters with a brief description.
# More information is available at the end of this file.
#
# PORT      UDP port number the trap adapter listens to.
# WINDOW    De-duplication window, in seconds.
# ASCII     Controls formatting of non-printable characters.
# TAG       Enables tagging of varbind values.
# ENABLE_FWD Enables trap forwarding.
# MATCH     Determines whether traps are tested against all forwarding
#           criteria or up to the first criterion that matches.
# FORWARD   Specifies matching criteria for traps and the forwarding
#           destinations for matched traps.
#
# Set the parameters here.
PORT: 9000
#WINDOW: 10
#ASCII: FALSE
#TAG: FALSE
ENABLE_FWD: TRUE
#MATCH: all
#QUEUE_LIMIT_MEGS: 0
#QUEUE_LIMIT_SECONDS: 0

# Traps required by InCharge IP Availability Manager (AM)
# Generic: coldStart, warmStart, LinkUp, LinkDown
#FORWARD: * .* <0-3> * host:port

# Traps required by InCharge IP Performance Manager (PM)
# Cisco: EnvMon Voltage, Temperature, Fan, RedundantSupply
#FORWARD: * .1.3.6.1.4.1.9.9.13.3 6 <2-5> host:port
```
### Table 10 Configuration parameters in the trapd.conf file (page 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORT</td>
<td>UDP port number on which the trap receiver or trap adapter listens for traps. Valid values are 0-65535. The default port is 9000.</td>
</tr>
<tr>
<td>WINDOW</td>
<td>De-duplication window, in seconds. The maximum amount of time between receiving similar traps before the second trap is considered unique. Valid values are nonnegative integers, including 0. The default is 0. If not set or set to 0, the de-duplication feature is disabled, which means that all traps are considered unique.</td>
</tr>
<tr>
<td>ASCII</td>
<td>No longer used; should remain FALSE (default).</td>
</tr>
<tr>
<td>TAG</td>
<td>Enables tagging of variable-binding (varbind) values. Valid values are TRUE and FALSE. The default is FALSE. • When TRUE, the type of the varbind value appears before each value; for example, INTEGER-32 3. • When FALSE, the type of the varbind value does not appear before each value.</td>
</tr>
<tr>
<td>QUEUE_LIMIT_MEGS</td>
<td>Limits the size of internal trap queue to the stated size, in megabytes. Valid values are nonnegative integers, including 0. The default is 0, which means that there is no limit on the size of the internal trap queue. Note: The limit is not exact: The queue may grow slightly larger than the value specified. When the limit is reached, some traps will be discarded.</td>
</tr>
<tr>
<td>QUEUE_LIMIT_SECONDS</td>
<td>Limits the time that a trap can spend in the internal trap queue, in seconds. Valid values are nonnegative integers, including 0. The default is 0, which means that there is no limit on the time that a trap can spend in the internal trap queue. Note: This limit is even less exact than the limit set for QUEUE_LIMIT_MEGS. In general, you should specify values for both QUEUE_LIMIT_MEGS and QUEUE_LIMIT_SECONDS. When the limit is reached, some traps will be discarded.</td>
</tr>
<tr>
<td>ENABLE_FWD</td>
<td>Determines whether uncommented FORWARD parameters are enabled or disabled. Valid values are TRUE and FALSE. The default is TRUE. • When TRUE, uncommented FORWARD parameters are enabled: Trap forwarding statements specified in uncommented FORWARD parameters are read. • When FALSE, uncommented FORWARD parameters are disabled: Trap forwarding statements specified in uncommented FORWARD parameters are not read.</td>
</tr>
<tr>
<td>MATCH</td>
<td>Determines whether traps are tested against all matching criteria that are specified in an uncommented FORWARD parameter, or tested up to the first criterion that matches. Valid values are “all” or “first.” The default is “first.” If no uncommented FORWARD parameters are specified, the MATCH parameter is ignored.</td>
</tr>
</tbody>
</table>
Configuring SNMP Trap Integration

FORWARD

Specifies matching criteria for traps and the forwarding destinations for matched traps.
Valid syntax is:

\(<\text{source device address}\> <\text{OID}\> <\text{generic type}\> <\text{specific type}\> <\text{destination host address}\>[:<\text{port}\>[:<\text{community}\>]] <\text{destination host address}\>[:<\text{port}\>[:<\text{community}\>]] ...

where:
- \(<\text{source device address}\>\) is the IP address of the object (SNMP agent) generating the trap.
- \(<\text{OID}\>\) is the sysObjectID of the type of object generating the trap.
- \(<\text{generic type}\>\) is the generic trap type:
  0 coldStart
  1 warmStart
  2 linkDown
  3 linkUp
  4 authenticationFailure
  5 egpNeighborLoss
  6 enterpriseSpecific
Valid syntax for \(<\text{generic type}\>\) is a generic specific trap number (for example, 3), a range of generic specific trap numbers (for example, \(<3-5>\) ), or any generic specific trap number (for example, \(*\) ). An asterisk is a wildcard character that matches any arbitrary string of characters.
- \(<\text{specific type}\>\) is the specific trap code, present even if \(<\text{generic type}\>\) is not enterpriseSpecific (6).
Valid syntax for \(<\text{specific type}\>\) is an enterprise specific trap number (for example, 733), a range of enterprise specific trap numbers (for example, \(<130-156>\) ) , or any enterprise specific trap number (for example, \(*\) ).
- \(<\text{destination host address}\>\) is the IP address (for example, 192.35.144.12) or the hostname (for example, gifted.mycompany.com) of the destination host.
- \(<\text{port}\>\) is the trap listening port on the destination host. Port is optional; if not specified, port defaults to 162.
- \(<\text{community}\>\) is the community string to be assigned to the community string field in the forwarded traps. Community is optional; if not specified, community defaults to the value specified in the community string field of the incoming v1 or v2c trap, and defaults to an empty string for an incoming v3 trap.
Wildcards are allowed for all fields except destination host address, port, and community. Wildcard syntax is discussed in Appendix A, “Wildcard Patterns.”
Examples:
FORWARD: \(*.*.*.*\) snake:9099:public1
All traps received from all network devices will be sent to port 9099 on a host named “snake”; the community string “public1” will be assigned to the forwarded traps.
FORWARD: 193.20.*.*.* \(<0-5>\) obelix:7000 surya 194.56.78.23:9000
All generic traps (0 to 5) from network devices whose address matches 193.20.*.*.* will be sent to:
- Port 7000 on a host named “obelix.”
- Port 162 on a host named “surya.”
- Port 9000 on a host identified by address 194.56.78.23.
Other trap forwarding examples are presented at the end of the trapd.conf file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| FORWARD   | Specifies matching criteria for traps and the forwarding destinations for matched traps. Valid syntax is: \(<\text{source device address}\> <\text{OID}\> <\text{generic type}\> <\text{specific type}\> <\text{destination host address}\>[:<\text{port}\>[:<\text{community}\>]] <\text{destination host address}\>[:<\text{port}\>[:<\text{community}\>]] ...

where:
- \(<\text{source device address}\>\) is the IP address of the object (SNMP agent) generating the trap.
- \(<\text{OID}\>\) is the sysObjectID of the type of object generating the trap.
- \(<\text{generic type}\>\) is the generic trap type:
  0 coldStart
  1 warmStart
  2 linkDown
  3 linkUp
  4 authenticationFailure
  5 egpNeighborLoss
  6 enterpriseSpecific
Valid syntax for \(<\text{generic type}\>\) is a generic specific trap number (for example, 3), a range of generic specific trap numbers (for example, \(<3-5>\) ), or any generic specific trap number (for example, \(*\) ). An asterisk is a wildcard character that matches any arbitrary string of characters.
- \(<\text{specific type}\>\) is the specific trap code, present even if \(<\text{generic type}\>\) is not enterpriseSpecific (6).
Valid syntax for \(<\text{specific type}\>\) is an enterprise specific trap number (for example, 733), a range of enterprise specific trap numbers (for example, \(<130-156>\) ) , or any enterprise specific trap number (for example, \(*\) ).
- \(<\text{destination host address}\>\) is the IP address (for example, 192.35.144.12) or the hostname (for example, gifted.mycompany.com) of the destination host.
- \(<\text{port}\>\) is the trap listening port on the destination host. Port is optional; if not specified, port defaults to 162.
- \(<\text{community}\>\) is the community string to be assigned to the community string field in the forwarded traps. Community is optional; if not specified, community defaults to the value specified in the community string field of the incoming v1 or v2c trap, and defaults to an empty string for an incoming v3 trap.
Wildcards are allowed for all fields except destination host address, port, and community. Wildcard syntax is discussed in Appendix A, “Wildcard Patterns.”
Examples:
FORWARD: \(*.*.*.*\) snake:9099:public1
All traps received from all network devices will be sent to port 9099 on a host named “snake”; the community string “public1” will be assigned to the forwarded traps.
FORWARD: 193.20.*.*.* \(<0-5>\) obelix:7000 surya 194.56.78.23:9000
All generic traps (0 to 5) from network devices whose address matches 193.20.*.*.* will be sent to:
- Port 7000 on a host named “obelix.”
- Port 162 on a host named “surya.”
- Port 9000 on a host identified by address 194.56.78.23.
Other trap forwarding examples are presented at the end of the trapd.conf file. |
Configuring the SNMP trap-integration components

Before starting the SNMP trap-integration components in a Network Protocol Manager deployment, you must configure them so that they can receive, distribute, and process traps properly at startup.

The configuration steps are:

- **“Configure the trap exploder”** to receive traps from the managed network devices and to distribute BGP and OSPF traps to Network Protocol Manager, network traps to IP Availability Manager, and informational traps to the trap receiver.
- **“Configure the built-in trap receivers”** of Network Protocol Manager and IP Availability Manager to receive the traps forwarded by the trap exploder.
- **“Configure the trap receiver”** to receive the informational traps forwarded by the trap exploder and to convert the traps into EMC Smarts notifications.
- **“Configure the Adapter Platform”** to import topology from IP Availability Manager for the purpose of associating EMC Smarts notifications with the appropriate topology objects.

Configure the trap exploder

Whenever it starts up, the trap exploder reads the trapd.conf file and an optional seed file in the following directory in the Service Assurance Manager installation area:

BASEDIR/smarts/local/conf/trapd

The trap exploder sets its configurations to the configuration settings in its trapd.conf file. It reads all of the uncommented parameters in the trapd.conf file, including the PORT parameter, which is set to 9000 by default.

The trap exploder uses the credentials in its seed file to authenticate and decrypt SNMPv3 traps received from SNMPv3-capable devices in the managed network. This seed file is separate from the seed file used by IP Availability Manager for discovery.

Procedure for configuring the trap exploder

To configure the trap exploder, you open and edit the Service Assurance
BASEDIR/smarts/conf/trapd/trapd.conf file to forward the appropriate traps to Network Protocol Manager, IP Availability Manager, and the trap receiver. You use the FORWARD parameter in the trapd.conf file to determine which incoming traps are sent to what destinations.

In addition to configuring the trapd.conf file, you need to configure the managed network devices to forward SNMP traps to the host where the trap exploder is running, and to the port on which the trap exploder is listening for traps.

If no --port=<port number> option is specified in the trap exploder’s startup command, the trap exploder listens for traps on the port specified by the PORT parameter in the trapd.conf file (port 9000 by default), or port 162 if no PORT value is specified in the trapd.conf file. The trap exploder startup options are described in “Start the trap exploder” on page 92.

Figure 26 on page 86 maps the steps (circled numbers) in the trap exploder configuration procedure to the configured forwarded trap paths.
To configure the trapd.conf file for the trap exploder:

1. Go to the BASEDIR/smarts/bin directory in the Service Assurance Manager installation area and type the following command to open the trapd.conf file:

   `sm_edit conf/trapd/trapd.conf`

   Press Enter.

2. To forward BGP traps to Network Protocol Manager for BGP, add the following FORWARD entries (and comments for usability purposes) to the trapd.conf file:

   ```
   # BGP Snmp v2 traps
   FORWARD: *.*.*.* .1.3.6.1.2.1.15.7 * * <hostname>:<port no>
   # BGP Snmp v1 traps
   FORWARD: *.*.*.* .1.3.6.1.2.1.15 * * host:port
   # CiscoMgmt trap for reconfiguration
   FORWARD: *.*.*.* .1.3.6.1.4.1.9.9.43.2 * * <hostname>:<port no>
   ```

   Specify the <hostname>:<port no> (for example, gifted.mycompany.com:9001) of the Network Protocol Manager for BGP destination that is to receive the BGP trap messages.

   The procedure to enable the Network Protocol Manager for BGP built-in trap receiver and to set a trap listening port is given in “Configure the built-in trap receivers” on page 89.
The traps received by Network Protocol Manager for BGP are described in “Traps processed for BGP” on page 145.

3. To forward OSPF traps to Network Protocol Manager for OSPF, add the following FORWARD entries (and comments for usability purposes) to the trapd.conf file:

```
#       OSPF traps for non-cisco devices
FORWARD: *.*.*.* .1.3.6.1.2.1.14.16.2 * * <hostname>:<port no>
#       CiscoMgmt trap for reconfiguration
FORWARD: *.*.*.* .1.3.6.1.4.1.9.9.43.2 * * <hostname>:<port no>
```

Specify the <hostname>:<port no> of the Network Protocol Manager for OSPF destination that is to receive the OSPF trap messages.

The procedure to enable the Network Protocol Manager for OSPF built-in trap receiver and to set a trap listening port is given in “Configure the built-in trap receivers” on page 89.

The traps received by Network Protocol Manager for OSPF are described in “Traps processed for OSPF” on page 153.

4. To forward network traps to IP Availability Manager, choose which FORWARD entries that you want to use from the following list of predefined FORWARD statements in the trapd.conf file:

```
# Traps required by InCharge IP Availability Manager (AM)
# Generic: coldStart, warmStart, LinkUp, LinkDown
#FORWARD: * .* <0-3> * host:port

# Cisco: STACK module inserted, removed
#FORWARD: * .1.3.6.1.4.1.9.5 6 <3-4> host:port

# 3Com: CoreBuilder 9000 module inserted
#FORWARD: * .1.3.6.1.4.1.43.28.2 6 6 host:port

# AI: SLC card down, up
#FORWARD: * .1.3.6.1.4.1.539 6 10 host:port
#FORWARD: * .1.3.6.1.4.1.539 6 111 host:port
#FORWARD: * .1.3.6.1.4.1.629 6 10 host:port
#FORWARD: * .1.3.6.1.4.1.629 6 111 host:port

# Cisco ISDN demandNbrLayer2Change
#FORWARD: * .1.3.6.1.4.1.9.9.26.2 6 3 host:port

# Cisco chHsrpStateChange
#FORWARD: * .1.3.6.1.4.1.9.9.106.2 6 1 host:port

# Traps required by InCharge IP Performance Manager (PM)
# Cisco: EnvMon Voltage, Temperature, Fan, RedundantSupply
#FORWARD: * .1.3.6.1.4.1.9.9.13.3 6 <2-5> host:port
```

Uncomment the FORWARD statements that you want to use. Then, specify the <host>:<port> (hostname and port number) of the IP Availability Manager destination that is to receive the trap messages.
The procedure to change the trap listening port (port 9000 by default) of the IP Availability Manager built-in trap receiver is given in “Procedure to configure the IP Availability Manager built-in trap receiver” on page 90.

5. To forward informational traps to the trap receiver, add your choice of FORWARD entries to the trapd.conf file:

```
# Traps for Trap Receiver and Adapter Platform
<Add your matching criteria for the traps and the forwarding destination: the IP address and trap port of the trap receiver.>
```

Specify the `<hostname>:<port no>` of the trap receiver destination that is to receive the trap messages.

By default, the trap receiver listens for traps on port 9000. Insight into how to change this port number is given in “Configure the trap receiver” on page 90.

6. Ensure that the ENABLE_FWD parameter is TRUE (default).

7. Save and close the file.

The modified version of the trapd.conf file is saved to the BASEDIR/smarts/local/conf/trapd directory in the Service Assurance Manager installation area.

Any received trap not matching any of the FORWARD entries is discarded.

Procedure for enabling the trap exploder to process SNMPv3 traps

Perform this procedure only if the trap exploder is to process SNMPv3 traps. The procedure consists of placing a copy of an IP Availability Manager seed file in the BASEDIR/smarts/conf/trapd directory in the Service Assurance Manager installation area.

It is assumed that you have already created a seed file for IP Availability Manager discovery purposes. Typically, you create a seed file by using the sm_edit utility to open and add seed entries to a template file named seedfile, located in the BASEDIR/smarts/conf directory in the IP Manager installation area.

IP Availability Manager uses the seed entries and their credentials to contact the seed systems during discovery. The trap exploder uses the entries and their credentials to verify and decrypt SNMPv3 trap messages received from SNMPv3-capable seed systems once the seed systems are discovered.

To enable the trap exploder to process SNMPv3 traps:

1. In the IP Manager installation area, make a copy of the seed file that was created for discovery purposes and save it to the BASEDIR/smarts/conf/trapd directory in the Service Assurance Manager installation area. The seed filename must match the name specified in the --seed option of the trap exploder startup command.

2. In the Service Assurance Manager installation area, go to the BASEDIR/smarts/bin directory and type the following command to open the seed file.

```
sm_edit conf/trapd/<seed file>
```

Press Enter.

3. Modify the seed file as appropriate for your deployment.
4. Save and close the file.

   The modified version of the seed file is saved to the BASEDIR/smarts/local/conf/trapd directory in the Service Assurance Manager installation area.

5. If the trap exploder was running before you edited the seed file, restart the trap exploder.

Configure the built-in trap receivers

By default, the built-in trap receiver for Network Protocol Manager for BGP or Network Protocol Manager for OSPF is disabled. Follow the instructions in the “Procedure to configure the Network Protocol Manager built-in trap receiver” on page 89 to enable the built-in trap receiver and to set its port number to the destination port specified for Network Protocol Manager in the trap exploder’s trapd.conf file.

By default, the built-in trap receiver for IP Availability Manager listens for traps on port 9000. Follow the instructions in the “Procedure to configure the IP Availability Manager built-in trap receiver” on page 90 section to set the port number of the built-in trap receiver to the destination port specified for IP Availability Manager in the trap exploder’s trapd.conf file.

Procedure to configure the Network Protocol Manager built-in trap receiver

To configure the Network Protocol Manager built-in trap receiver:

1. Go to the BASEDIR/smarts/bin directory in the Network Protocol Manager installation area and type the following command to open the bgp.conf or ospf.conf file:

   `sm_edit conf/bgp/bgp.conf`

   -or-

   `sm_edit conf/ospf/ospf.conf`

   Press Enter.

2. Find the following line:

   `TrapPort = 0`

   `TrapPort = 0` disables the built-in trap receiver.

3. Set the port number (0) to the destination port specified for Network Protocol Manager for BGP or Network Protocol Manager for OSPF in the trap exploder’s trapd.conf file.

   A valid port number is 162 or any value in the range 2049 to 65534 inclusive.

4. Save and close the file.

   The modified version of the bgp.conf file is saved to the BASEDIR/smarts/local/conf/bgp directory, or the modified version of the ospf.conf file is saved to the BASEDIR/smarts/local/conf/ospf directory.

5. If Network Protocol Manager was running before you edited the bgp.conf or ospf.conf file, restart Network Protocol Manager.
Configuring SNMP Trap Integration

Procedure to configure the IP Availability Manager built-in trap receiver

To configure the IP Availability Manager built-in trap receiver:

1. Go to the BASEDIR/smarts/bin directory in the IP Manager installation area and type the following command to open the trapd.conf file:

   `sm_edit conf/trapd/trapd.conf`

   Press Enter.

2. Set the port number of the following PORT entry to the destination port specified for IP Availability Manager in the trap exploder's trapd.conf file:

   `PORT: <port number>`

   A valid port number is 162 or any value in the range 2049 to 65534 inclusive.

3. Save and close the file.

   The modified version of the trapd.conf file is saved to the BASEDIR/smarts/local/conf/trapd directory in the IP Manager installation area.

4. If IP Availability Manager was running before you edited the trapd.conf file, restart IP Availability Manager.

Configure the trap receiver

To configure the trap receiver to process informational traps received from the trap exploder, you edit the Service Assurance BASEDIR/smarts/conf/icoi/trap_mgr.conf file to define how the trap receiver processes traps into notifications. Each trap to be transformed into a notification requires a trap definition entry in the trap_mgr.conf file.

The trap_mgr.conf file contains rules that the trap receiver uses to map incoming traps into the data fields of an EMC Smarts notification. The Adapter Platform, in turn, creates the EMC Smarts notification object from the data fields and exports the notification to the Global Manager.

If no `--port=<port number>` option is specified in the trap receiver's startup command, the trap receiver listens for traps on the port specified by the PORT parameter in the Service Assurance BASEDIR/smarts/conf/icoi/trapd.conf file (port 9000 by default), or port 162 if no PORT value is specified in the trapd.conf file. The trap exploder startup options are described in the *EMC Smarts Service Assurance Manager Adapter Platform User Guide* and the *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers*.

To configure the trap_mgr.conf file for the trap receiver:

1. Go to the BASEDIR/smarts/bin directory in the Service Assurance Manager installation area and type the following command to open the trap_mgr.conf file:

   `sm_edit conf/icoi/trap_mgr.conf`

   Press Enter.

2. Define a trap definition for each received trap.

   For each SNMP trap, you must specify how the information in the trap maps to objects in the Global Manager repository and how the notification should appear at the Global Console.
3. Save the file.

   The modified version of the trap_mgr.conf file is saved to the BASEDIR/smarts/local/conf/icoi directory in the Service Assurance Manager installation area.

Configure the Adapter Platform

To configure the Adapter Platform, you attach the Global Manager to the Adapter Platform and specify the underlying IP Availability Manager domain or domains. Doing so enables the Adapter Platform to import hostnames and IP addresses from the underlying IP Availability Manager domains so that it can accurately relate events in received traps to the devices that are associated with the events. The Adapter Platform creates EMC Smarts notification objects from the events, and exports the notifications to the Global Manager.

The procedure to configure the Adapter Platform is identical to the procedure that is presented in "Specifying the underlying domains" on page 65.

To attach the Global Manager Administration Console to your Adapter Platform:

1. In the Global Manager Administration Console, select Manager > Attach to display the Attach Manager dialog box.

2. In the Attach Manager dialog box, enter the Adapter Platform name and the login information (for example, admin and changeme) and click OK.

3. In the Global Manager Administration Console, select the Adapter Platform name from the Manager drop-down menu.

The EMC Smarts Service Assurance Manager Adapter Platform User Guide provides a complete description of the Adapter Platform.

Starting the SNMP trap-integration components

In a Network Protocol Manager deployment, you install the following products as services so that the host system automatically starts them as processes that run in the background each time that the system boots:

- EMC Smarts Broker
- Network Protocol Manager
- IP Availability Manager
- Global Manager
- Global Console
- Adapter Platform
- SNMP Trap Adapter (trap exploder and trap receiver)

The services for these products are described in detail in the EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers.

You cannot install the SNMP Trap Adapter (trap exploder) as a service, but you can use the sm_service command to register this adapter as a service after the installation. This section describes how to create and start a service for the SNMP Trap Adapter that is configured as a trap exploder.
Configuring SNMP Trap Integration

**NOTICE**

Typically, in any EMC Smarts deployment, the order in which the applications are started is not important, except that the Broker must be started first.

**Start the trap exploder**

Use the `sm_service` command to manually create a service for the trap exploder. A typical service command on a UNIX host would look like this:

```
/opt/InCharge/SAM/smarts/bin/sm_service install
  --force
  --unmanaged
  --startmode=runonce
  --name=ic-trap-exploder
  --description="EMC Smarts SNMP Trap Exploder"

/opt/InCharge/SAM/smarts/bin/sm_trapd
  --name=INCHARGE-EXPLODER
  --config=trapd
  --port=162
  --rules=default
  --output
```

where:

- **--name=**<name>
  
  Second **--name** option (**--name=INCHARGE-EXPLODER**) in the service command:
  
  Specifies the trap exploder name to be registered with the Broker for the deployment. Also -n <name>.

- **--config=**<cfg>
  
  Specifies the configuration directory in which the trapd.conf file for the trap exploder is located. The trapd.conf file is loaded from the BASEDIR/smarts/local/conf/<cfg> directory, or from the BASEDIR/smarts/conf/<cfg> directory if the trapd.conf file is not present in the local directory. The default configuration (cfg) directory for the trap exploder is trapd.

**NOTICE**

Ensure that **--config** is set to trapd in the trap exploder service command.

- **--port=**<trap listening port>
  
  Specifies the port number to which the managed network devices send traps and on which the trap exploder listens for traps. Also -p <trap listening port>.

  The default trap listening port is the PORT parameter value in the <cfg>/trapd.conf file (port 9000 by default), or port 162 if no PORT value is specified in the <cfg>/trapd.conf file.
◆ --sport=<Remote API listening port>

Specifies the port number on which the trap exploder listens for Remote API
connections from other EMC Smarts programs, including the Global Console, servers,
and utilities such as dmctl. This option is meaningful only if the --name option is
specified. Also -P <Remote API listening port>.

The --sport option for the sm_trapd program plays the same role as the --port option
plays for any other EMC Smarts program. The --sport option is unique to the sm_trapd
program and defaults to 0.

**NOTICE**

--sport=0 is interpreted by the host operating system as meaning “assign this
program a unique, unused port number.” Typically, the operating system responds by
assigning a unique, unused port number in the range 40000–65535.

◆ --rules=default

Specifies the rule set to be used by the trap exploder. The default rule set is defined in
the BASEDIR/smarts/rules/trapd/trapParse.asl file.

◆ --output

Specifies that the stdout and stderr output for the trap exploder should be redirected
to a log file in the BASEDIR/smarts/local/logs directory. The name of the log file is
INCHARGE-EXPLODER_<locale>_<character encoding>.log; for example,

The command for starting the example service is:

```
/opt/InCharge/SAM/smarts/bin/sm_service start ic-trap-exploder
```

At startup, the trap exploder reads the trapd.conf file and saves the configuration
information in its repository.

The *EMC Smarts System Administration Guide* provides more details about sm_service.
CHAPTER 7
Configuring Syslog Message Processing and Forwarding

This chapter provides instructions for configuring syslog message processing and forwarding in a Network Protocol Manager deployment. It consists of the following sections:

- Configuration overview ................................................................. 96
- Syslog adapters .............................................................................. 97
- Configuring syslog message processing and forwarding ............... 97
- Configuring syslog message processing ....................................... 98
Configuration overview

The recommended syslog message processing and forwarding design for a Network Protocol Manager deployment is shown in Figure 27 on page 96.

Figure 27 Recommended syslog message processing and forwarding design

Configuring the syslog message forwarding involves configuring and starting the syslog adapters that receive, process, and distribute the syslog messages within a Network Protocol Manager deployment.
Syslog adapters

A Network Protocol Manager installation includes a built-in syslog adapter that can be configured to:

- Fetch BGP- or OSPF-related syslog message from a syslog (system log).
- Parse the messages for status updates.
- Distribute the status updates to Network Protocol Manager for BGP or Network Protocol Manager for OSPF.

Network Protocol Manager for BGP uses the status updates to update the attributes of BGP objects in its modeled topology, and Network Protocol Manager for OSPF uses the status updates to update the attributes of OSPF objects in its modeled topology.

The syslog messages that are processed by Network Protocol Manager for BGP and Network Protocol Manager for OSPF are described in Appendix C, “Syslog Messages Processed.”

Configuring syslog message processing and forwarding

For the syslog message processing and forwarding scenario, a syslog daemon that is running on a remote system collects the syslog messages from the managed devices that are running the BGP or OSPF protocols. The daemon then writes the messages to a single syslog file on the remote system.

A user installs a separate instance of the Network Protocol Manager on the remote system and manually starts two instances of the built-in syslog adapter:

- An instance started as a BGP syslog adapter to serve Network Protocol Manager for BGP.
- An instance started as an OSPF syslog adapter to serve Network Protocol Manager for OSPF.

To configure syslog message processing and forwarding:

1. On the local system, where the Network Protocol Manager for BGP or Network Protocol Manager for OSPF reside, ensure that the value of the SyslogName parameter in the BASEDIR/smarts/conf/bgp/bgp.conf file or the BASEDIR/smarts/conf/ospf/ospf.conf file is set to "" (empty string).
2. On the remote system, where the syslog file resides, install an instance of the Network Protocol Manager. During the installation, do not install any of the Network Protocol Manager products as services.
3. On the remote system, go to the BASEDIR/smarts/bin directory in the Network Protocol Manager installation area and start the syslog adapters.

A sample command line for a target Network Protocol Manager for BGP named INCHARGE-BGP is:

```
sm_adapter --name=INCHARGE-BGP-SYSLOG --server=INCHARGE-BGP
            --output=BGP-SYSLOG --daemon --tail=<full path to log file>
             bgp/bgp-syslog.asl
```
A sample command line for a target Network Protocol Manager for OSPF named INCHARGE-OSPF is:

```
sm_adapter --name=INCHARGE-OSPF-SYSLOG --server=INCHARGE-OSPF
    --output=OSPF-SYSLOG --daemon --tail=<full path to log file>
    ospf/ospf-syslog.asl
```

**NOTICE**

The `sm_adapter` command is described in the HTML pages that are located in the BASEDIR/smarts/doc/html/usage directory of any Domain Manager installation area.

## Configuring syslog message processing

In those cases where the syslog daemon and Network Protocol Manager for BGP and Network Protocol Manager for OSPF are running on the same system, a user does not need to install a separate instance of the Network Protocol Manager to start the BGP and OSPF syslog adapters. Instead, a user starts the BGP and OSPF syslog adapters by assigning the full path and name of the local syslog file to the SyslogName parameter in the bgp.conf or ospf.conf file. For this scenario, the syslog adapters are started automatically when Network Protocol Manager for BGP and Network Protocol Manager for OSPF are started.

To configure syslog message processing:

1. Go to the BASEDIR/smarts/bin directory in the Network Protocol Manager installation area and type the following command to open the bgp.conf or ospf.conf file:

   ```
   sm_edit conf/bgp/bgp.conf
   -or-
   sm_edit conf/ospf/ospf.conf
   ```

   Press Enter.

2. Find the following line:

   ```
   SyslogName = ""
   ```

   `SyslogName = ""` disables the built-in syslog adapter.

3. Replace the empty string (""") with the full path and name of the syslog file on the local system. For example:

   ```
   SyslogName = /var/adm/messages
   ```

4. Save and close the file.

   The modified version of the bgp.conf file is saved to the BASEDIR/smarts/local/conf/bgp directory, or the modified version of the ospf.conf file is saved to the BASEDIR/smarts/local/conf/ospf directory.

5. If Network Protocol Manager was running before you edited the bgp.conf or ospf.conf file, restart Network Protocol Manager.
CHAPTER 8
Configuring SSH Security

This chapter presents an overview of Secure Shell (SSH) security and provides instructions for configuring SSH in a Network Protocol Manager deployment. It consists of the following sections:

- SSH overview ........................................................................................................ 100
- CLI modules for Network Protocol Manager ...................................................... 102
- SSH client configuration .................................................................................... 105
- SSH server configuration .................................................................................. 106
SSH overview

Like Telnet, SSH is a protocol for logging in to a remote host and executing commands on the remote host. Unlike Telnet, SSH uses special algorithms to encrypt the data stream, to ensure data stream integrity, and even to perform authentication in a safe and secure way. SSH is a secure, encrypted replacement for Telnet.

SSH provides remote command line interface (CLI) administration over an authenticated, encrypted connection. In a Network Protocol Manager deployment, Network Protocol Manager for EIGRP and Network Protocol Manager for IS-IS use SSH CLI to query EIGRP- and IS-IS-enabled Cisco devices for topology and status information.

SSH1 and SSH2

Two versions of the SSH protocol exist: SSH1 and SSH2. The two versions are different in terms of their underlying workings.

SSH1 is a simpler protocol than SSH2, and is available on a wider variety of platforms than SSH2. SSH1 has more options for authentication than SSH2, and performs better than SSH2.

On the down side, SSH1 has serious structural weaknesses that leave it vulnerable to a broad number of attacks. These weaknesses have been corrected in SSH2. Because the security enhancements in SSH2 would not have been possible if protocol-level compatibility with SSH1 had been retained, SSH1 and SSH2 are not compatible with one another.

SSH Communications Security, the original developer of the SSH protocol, considers the SSH1 protocol deprecated and recommends that SSH1 not be used.

SSH authentication

Figure 28 on page 100 shows an SSH connection between a client and a server.

The client is the SSH client software that connects users to the SSH server on the remote host. The server is the SSH server program, or ssh daemon, that is running on the remote host. In Figure 28 on page 100, the client and server enable a user named NPMUser on a Network Protocol Manager host to log in as ServerUser on a Cisco router.

SSH authentication begins with the authentication of the server to the client, and ends with the authentication of the client to the server.
Authentication of the server to the client

When the client issues an SSH connection request, such as ssh ServerUser@ciscosystem, the server accepts the connection request and responds with the server’s version identification. The client parses the server’s version identification and then sends its own version identification. The purpose of the version-identification exchange is three-fold:

- To validate that the connection is to the correct server port.

**NOTICE**

The standard SSH port is 22.

- To declare the SSH protocol version number that is used by the server and by the client.
- To declare the software version that is used by the server and by the client.

The client and server negotiate which SSH protocol version to use.

The server then sends its public host key and a list of supported ciphers and authentication methods to the client. The client compares the server’s host key to the user’s database of known hosts. If the received host key matches the server’s host key entry in the user’s database, the SSH connection attempt continues.

If the received host key does not match the server’s host key entry, the client terminates the SSH connection attempt, and informs the user where to find the conflicting key in the user’s database.

If no host key entry exists for the server in the user’s database, the client responds in one of three ways, depending on the value of the StrictHostKeyChecking parameter in the client’s configuration file:

- **StrictHostKeyChecking=ask** (default)

  The client asks the user whether to add the server’s host key to the user’s database.

  If the user answers with yes, the client adds the server’s host key to the user’s database and continues the SSH connection attempt.

  If the user answers with no, the client discards the server’s host key and terminates the SSH connection attempt.

- **StrictHostKeyChecking=no**

  The client automatically adds the server’s host key to the user’s database and continues the SSH connection attempt.

- **StrictHostKeyChecking=yes**

  The client discards the server’s host key and terminates the SSH connection attempt.

If the outcome is that the SSH connection attempt should continue, server authentication is established.

The client then generates a session key, encrypts it with the server’s host key, and sends the encrypted session key and selected cipher to the server. Both sides then turn on encryption using the session key and the selected cipher. The server sends an encrypted confirmation message to the client.
Authentication of the client to the server

To authenticate the client to the server, the client may use any of the methods in the list of authentication methods received from the server. Three well-known authentication methods are:

- **Password authentication**

  Password authentication uses the password of the username account (ServerUser, for example) on the remote host to perform client authentication.

  With this method, the user enters the password, and the client encrypts and transmits the password. The server receives and decrypts the password, and the remote host authenticates the password against its password database.

- **Public-key authentication**

  Public-key authentication uses public/private key pairs to perform client authentication, without the need to transmit a password over the network. A user creates a public/private key pair for authentication purposes. The server knows the user's public key, and only the user has the private key.

  With this method, the server generates a random number, uses the user’s public key to encrypt the number, and sends the encrypted number to the client. The client uses the user’s private key to decrypt the number and sends the number back to the server.

- **Host-based authentication**

  Host authentication uses the client’s hostname and the user’s username (NPMUser, for example) on the remote host to perform client authentication.

  With this method, the client sends a signature created with the user’s private key, and the server verifies the signature with the user’s public key. When the user’s identity is established, authorization is performed based on (1) the client’s hostname and (2) the user’s username on both the server and the client.

  When the user's identity has been accepted by the server, the server logs in to the remote host and gives the user a normal shell on the remote host. All CLI commands and responses with/from the remote shell will be encrypted.

**CLI modules for Network Protocol Manager**

Two independent CLI software modules are available in Network Protocol Manager:

- **Voyence Device Access Scripting Language (DASL) CLI**

  Available in a Network Protocol Manager software distribution installed on a Windows system.

- **Open source Practical Extraction and Report Language (Perl) CLI**

  Available in a Network Protocol Manager software distribution installed on a Linux system.

Both CLI modules support SSH CLI and Telnet CLI access to remote hosts.
DASL CLI module

The DASL CLI module includes SSH client and Telnet client libraries. It gathers routing-protocol topology and status information by establishing SSH or Telnet CLI connections to the Cisco devices in the managed network.

A Network Protocol Manager for EIGRP running on a Windows system calls the DASL CLI module to discover and monitor EIGRP topology. Similarly, a Network Protocol Manager for IS-IS running on a Windows system calls the DASL CLI module to discover and monitor IS-IS topology.

SSH protocol version support

The SSH client provided by the DASL CLI module supports SSH protocols 1 and 2. Protocol 2 is primary, with fall back to protocol 1 if the SSH client detects that protocol 2 is not supported by the SSH server.

Both protocols support similar authentication methods, but protocol 2 is preferred because it provides additional components for confidentiality and integrity. Protocol 1 lacks a strong component for ensuring the integrity of the connection.

Cipher support

Ciphers are used to encrypt SSH traffic. Encryption provides confidentiality and protects against spoofed packets.

The DASL CLI module supports the following SSH1 ciphers:
- DES (56-bit CBC)
- Triple-DES (3DES) (CBC)
- Blowfish (128-bit CBC)
- AES (Rijndael) (256, 192, or 128-bit SDCTR)

The DASL CLI module supports the following SSH2 ciphers:
- Triple-DES (3DES) (168-bit SDCTR or CBC)
- Blowfish (256-bit SDCTR or 128-bit CBC)
- AES (Rijndael) (256, 192, or 128-bit SDCTR or CBC)
- Arcfour (RC4) (256 or 128-bit stream cipher)

Message-digest support

Message-digest algorithms, or hashing algorithms, are used to verify both the data integrity and the authenticity of an SSH message.

The DASL CLI module supports a message-digest algorithm named keyed-Hash Message Authentication Code (HMAC).

Authentication support

Authentication is used to protect against security problems such as IP spoofing, fake routes, and DNS spoofing.

The DASL CLI module supports password authentication.
Configuring SSH Security

SSH and Telnet ports

The DASL CLI module uses the standard SSH and Telnet ports:

- Standard SSH port is 22.
- Standard Telnet port is 23.

By default, an SSH or Telnet server listens on these ports for connection requests.

Timeouts

The DASL CLI module uses the following timeouts:

- Ten seconds for responses
- Thirty seconds for longer running operations
- Five minutes for displaying bulk data such as the running configuration

The ten-second timeout is configurable, as explained in Table 8 on page 54.

Perl CLI module

The Perl CLI module interacts with third-party SSH client software and third-party Telnet client software. It gathers routing-protocol topology and status information by establishing SSH or Telnet CLI connections to the Cisco devices in the managed network.

A Network Protocol Manager for EIGRP running on a Linux system calls the Perl CLI module to discover and monitor EIGRP topology. Similarly, a Network Protocol Manager for IS-IS running on a Linux system calls the Perl CLI module to discover and monitor IS-IS topology.

Configuration file

The Perl CLI module for Network Protocol Manager for EIGRP and the Perl CLI module for Network Protocol Manager for IS-IS each have their own configuration file:

- BASEDIR/smarts/conf/eigrp/perl-cli-conf
- BASEDIR/smarts/conf/isis/perl-cli.conf

Third-party Telnet client implementation

A third-party Telnet client implementation is included in the Network Protocol Manager software distribution. The Perl CLI module interacts with that Telnet client.

Third-party SSH client implementation

No third-party SSH client implementation is included in the Network Protocol Manager software distribution. The user must install the SSH client software on the host machine that is hosting the Perl CLI module.

The Perl CLI module requires an SSH client that is comparable to the SSH client in OpenSSH 2.0 or higher. The OpenSSH 2.0 client suite supports SSH protocol versions 1.3, 1.5, and 2.0.
SSH client configuration

Configuring a Network Protocol Manager for EIGRP or a Network Protocol Manager for IS-IS to use SSH CLI starts with the following task:

Create one or more CLI device-access groups that have the device access method set to “SSH2.”

Instructions for creating CLI device-access groups are presented in “Creating CLI device-access groups” on page 53.

What additional configuration tasks are required depends upon the CLI module.

Configuring the SSH client for the DASL CLI module

The SSH client for the DASL CLI module is preconfigured to operate as follows:

◆ Try SSH version 2, and fall back to version 1 if version 2 is not available.
◆ Use password authentication only.
◆ Connect to the standard SSH port number, port 22, on the remote host.
◆ Add a new host to the user’s database of known hosts without prompting the user for confirmation.

In addition, the DASL CLI module is preconfigured to create log files. CLI log files are described in the EMC Smarts Network Protocol Manager Discovery Guide.

No other configurations are required for the DASL CLI module.

Configuring the SSH client for the Perl CLI module

The Perl CLI module requires an SSH client that is comparable to the SSH client in OpenSSH 2.0 or higher. The OpenSSH application is bundled with most UNIX-based operating systems.

Because SSH command-line options take precedence over user-specified or system-wide SSH configuration files, the Perl CLI module includes certain options in its SSH command-line invocations to ensure that the following configurations are not overridden:

◆ Try SSH version 2, and fall back to version 1 if version 2 is not available.
◆ Use password authentication only.
◆ Connect to the standard SSH port number, port 22, on the remote host.
◆ Add a new host to the user’s database of known hosts without prompting the user for confirmation.

After installing the SSH client software, you, as the administrator, perform the following additional configuration tasks:

◆ Specify the path to the SSH client executable (mandatory).
◆ Enable the Perl CLI module to create log files (optional).
You edit the appropriate perl-cli.conf file, BASEDIR/smarts/conf/eigrp/perl-cli.conf or BASEDIR/smarts/conf/isis/perl-cli.conf, to perform these tasks. The name/value entries to be edited are:

```
debug=0
# ssh_client=/usr/bin/ssh
```

To specify the path to the SSH client executable and to enable the creation of log files:

1. Go to the BASEDIR/smarts/bin directory in the Network Protocol Manager installation area and type the following command to open the perl-cli.conf file:

   ```
   sm_edit conf/eigrp/perl-cli.conf
   -or-
   sm_edit conf/isis/perl-cli.conf
   ```

   Press Enter.

2. Find the following entries:

   ```
   debug=0,
   # ssh_client=/usr/bin/ssh
   ```

3. Uncomment the ssh_client entry and set its value to the full path of the SSH client executable.

   For example:

   ```
   ssh_client=/usr/local/openssh/bin/ssh
   ```

   NOTICE

   For any entry in the perl-cli.conf file, do not enclose the name or value in quotes, and do not punctuate the entry with commas, semicolons, or periods.

4. Optional: Set the debug flag to 1 to enable the creation of log files:

   ```
   debug=1
   ```

   CLI log files are described in the *EMC Smarts Network Protocol Manager Discovery Guide*.

5. Save and close the file. The modified version of the perl-cli.conf file is saved to the BASEDIR/smarts/local/conf/eigrp|isis directory.

6. If Network Protocol Manager for EIGRP/ Network Protocol Manager for IS-IS was running before you edited the perl-cli.conf file, restart the manager.

**SSH server configuration**

Configuring a network device to use SSH requires that an administrator perform the following basic steps for each network device that is to be SSH enabled:

- Enable the SSH transport support for the virtual-terminal connections.
- Generate a public/private key pair.

The public key of the generated public/private key pair is referred to as the “public host key” or just “host key.”
To configure the SSH server on a Cisco device:

1. Ensure that the device has a session password and a privileged-mode enable password.

   For example:

   ```
   Router> enable
   Router# configure terminal
   Router(config)# passwd secret
   Router(config)# enable password secret
   Router(config)# exit
   Router#
   ```

2. Verify that the device supports the SSH server feature.

   Run the following command to display the loaded IOS software image:

   ```
   Router# show flash (OR)
   Router# show flash: (Cisco IOS 12.3)
   ```

   The SSH server feature for SSH1 support is available in the following Cisco IOS release trains: 12.0S, 12.0ST, 12.1T, 12.1E, 12.2, 12.2T, and 12.2S. The SSH server feature for SSH2 support is available in the following Cisco IOS release trains: 12.3(4)T, 12.3(2)XE, 12.2(25)S, and 12.3(7)J.

   The *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide* provides information about downloading an IOS software image.

3. Ensure that the device has a hostname and a properly configured host domain.

   For example:

   ```
   Router# configure terminal
   Router(config)# hostname ciscosystem
   ciscosystem(config)# ip domain-name cisco.com
   ```

   The hostname is the name of the device, and the domain name is the host domain that the device services. The IOS software uses the domain name to complete unqualified hostnames.

4. For Cisco IOS release train 12.0S, 12.0ST, 12.1T, 12.1E, 12.2, 12.2T, or 12.2S, enable the SSH server by generating an RSA key pair.

   For example:

   ```
   ciscosystem(config)# crypto key generate rsa
   ```

   Generating an RSA key pair automatically enables the SSH server. Deleting the RSA key pair, by entering the `crypto key zeroize rsa` command, automatically disables the SSH server.

5. For Cisco IOS release train 12.3(4)T, 12.3(2)XE, 12.2(25)S, or 12.3(7)JA, enable the SSH server by generating a DSA key pair.

   For example:

   ```
   ciscosystem(config)# crypto key generate dsa
   ```
Generating an DSA key pair automatically enables the SSH server. Deleting the DSA key pair, by entering the crypto key zeroize dsa command, automatically disables the SSH server.

6. Configure Authentication, Authorization, and Accounting (AAA) for SSH client access control.

When configuring AAA, the administrator specifies usernames and passwords, the session timeout, and the number of retries allowed during an SSH connection attempt. For example:

```
ciscosystem(config)# aaa new-model
ciscosystem(config)# username ServerUser password 0 cisco
ciscosystem(config)# ip ssh timeout 60
ciscosystem(config)# ip ssh authentication-retries 3
ciscosystem(config)# exit
ciscosystem#
```

Authentication timeout is the interval, measured in seconds, that the SSH server waits for the SSH client to respond. Authentication retries is the number of SSH client connection attempts after which the interface is reset.

The Cisco IOS Security Configuration Guide and the Cisco IOS Security Command Reference provide more information about AAA.

7. Verify that the SSH server is enabled and view its configuration.

To view the status, version, and configuration of the SSH server, execute the show ip ssh command. For example:

```
ciscosystem# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 3
```

8. Force the users that were added during the AAA configuration to use SSH instead of Telnet.

Complete this step by specifying SSH as the virtual-terminal (vty) connection of choice. For example:

```
ciscosystem# configure terminal
ciscosystem(config)# line vty 0 4
ciscosystem(config-line)# transport input SSH
ciscosystem(config-line)# exit
ciscosystem(config)#
```

The number of allowable SSH connections is limited to the maximum number of vtys that is configured for the device. Five vtys (0-4) are configured by default. Each SSH connection uses a vty resource.
9. Optional: For Cisco IOS release train 12.3(4)T, 12.3(2)XE, 12.2(25)S, or 12.3(7)JA, specify the version of SSH to be run on the device.

   For example:

   ciscosystem(config)# ip ssh version 2
   ciscosystem(config)# exit
   ciscosystem# exit
   ciscosystem>

   By default, SSH for Cisco 12.3(4)T, 12.3(2)XE, 12.2(25)S, and 12.3(7)JA allows both SSH1 and SSH2 connections to the device. The `ip ssh version 2` command restricts the connections to SSH2 only.

10. Open the SSH server configuration file and check that password authentication is enabled:

    • For a device that is running an OpenSSH server, ensure that `PasswordAuthentication` is set to yes in the `sshd_config` file.

    • For a device that is running an SSH Secure Shell server, ensure that `AllowedAuthentications` is set to password in the `sshd2_config` file.

11. Log out.

    ciscosystem> logout
Configuring SSH Security
CHAPTER 9
Using the Polling and Thresholds Console

This chapter introduces the Polling and Thresholds Console, defines groups and settings, and provides instructions on using the Polling and Thresholds Console to work with groups and settings. It consists of the following sections:

◆ Opening the Polling and Thresholds Console ........................................................ 112
◆ Understanding groups and settings ...................................................................... 114
◆ Working with groups and settings ......................................................................... 115
Opening the Polling and Thresholds Console

The Polling and Thresholds Console is used to display groups and modify their properties. In Figure 29 on page 112, the Polling and Thresholds Console is attached to a Network Protocol Manager for BGP named INCHARGE-BGP.

Instructions for opening the Polling and Thresholds Console are presented in Chapter 3, “Opening the Global Console.”

Layout of the Polling and Thresholds Console

What tabs appear on a Polling and Thresholds Console depends on the type of Domain Manager to which the console is attached. When attached to IP Availability Manager or IP Performance Manager, for example, the Polling and Thresholds Console contains four tabs:

- Polling

  Enables administrators to control the polling of the managed objects for monitoring purposes.
◆ Thresholds
  Enables administrators to set thresholds for the polled data.

◆ Device Access
  Enables administrators to specify an access protocol and credentials (such as login credentials) for device access.

◆ Tagging
  Enables administrators to create IP tagging filters.

**NOTICE**

When attached to other Domain Managers, the Polling and Thresholds Console typically contains the Polling and Thresholds tabs or just the Polling tab.

The Polling and Thresholds Console is divided into two panels.

◆ The left panel displays the icon for the Domain Manager in the upper-left corner and provides one, two, or four tabs, depending on the Domain Manager to which the Polling and Thresholds Console is attached. Selecting a tab shows what groups, settings, and members are available on the tab.

◆ The right panel remains blank until a group, setting, or member is selected in the left panel. When an item is selected in the left panel, the right panel displays additional information regarding that item.

**Polling and Thresholds Console toolbar buttons**

The toolbar of the Polling and Thresholds Console provides quick access to the commands described in Table 11 on page 113.

**Table 11** Polling and Thresholds Console toolbar buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Attach icon]</td>
<td>Attach to a Manager.</td>
</tr>
<tr>
<td>![Detach icon]</td>
<td>Detach from a Manager.</td>
</tr>
<tr>
<td>![Reconfigure icon]</td>
<td>Reconfigure: reapply polling/threshold values, update instrumentation, recompute codebook, and so on.</td>
</tr>
<tr>
<td>![Delete icon]</td>
<td>Delete the selected item.</td>
</tr>
</tbody>
</table>
Understanding groups and settings

A group contains one or more settings, and a setting contains one or more parameters. Managed objects (systems discovered in the managed network) become members of a group based on the matching criteria for the group.

Figure 30 on page 114 illustrates the relationships between managed objects, groups, and settings.

Figure 30 Relating managed objects to groups and settings

- The EMC Smarts core class for group (in the sense of “groups and settings”) is ICIM_Configuration. This class is the parent of all group classes that are used by Network Protocol Manager or any other EMC Smarts Domain Manager.
- The EMC Smarts core class for setting is ICIM_Setting. This class is the parent of all setting classes that are used by Network Protocol Manager or any other EMC Smarts Domain Manager.
- The EMC Smarts core class for managed object is ICIM_ManagedElement. This class is the parent of all managed object classes that are used by Network Protocol Manager or any other EMC Smarts Domain Manager.
Working with groups and settings

You can use the Polling and Thresholds Console to perform any of the following tasks:

- “Assign managed objects to groups”
- “Modify the properties of a group”
- “Add or remove settings”
- “Modify the parameters of a setting”
- “Modify the priority of groups”
- “Edit matching criteria”
- “Create new groups”

Assign managed objects to groups

When Network Protocol Manager performs discovery, it automatically assigns each managed object to one or more groups based on the:

- Matching criteria for a group.
- Priority of a group, which determines membership when an object meets the matching criteria for more than one group within a particular group category.

A managed object may be a member of one and only one group within a particular group category.

Modify the properties of a group

A group’s matching criteria and priority determine which managed objects become members of the group.

When a group is selected in the left panel of the Polling and Thresholds Console, four tabs appear in the right panel of the console:

- Settings
- Priorities
- Matching Criteria
- Description

Modifying the properties in the Settings, Priorities, or Matching Criteria tab changes the configuration of the group.

When you finish editing the properties of a group, perform these steps:

1. Click the Apply button to save the changes.
2. Click the Reconfigure toolbar button, or select Group > Reconfigure, to make the configuration changes take effect.
Add or remove settings

A group’s settings determine what parameters are applied to the managed objects that are members of the group.

The Settings tab is divided into two sections:

- Current Settings
  Lists the settings that are applied to the group.
- Available Settings
  Lists additional available settings.

To add or remove a setting:

1. In the Settings tab, select a setting in the Available Settings list or in the Current Settings list.
2. Click Add to move an available setting to the Current Settings list, or click Remove to move a current setting to the Available Settings list.
3. Click the Apply button to save your changes.
4. Click the Reconfigure toolbar button to make your changes take effect.

Modify the parameters of a setting

The parameters of a setting are changed in one of two ways:

- By choosing a value from a drop-down menu.
- By entering a value in a Value field or adjusting a slider bar that represents a range of values.

Changing the parameters of a setting

To change the parameters of a setting:

1. In the left panel of the Polling and Thresholds Console, select the setting to display the parameters of the setting in the right panel of the console.
2. Change the value of a parameter by using one of the following methods:
   - For a drop-down menu, click the menu and select a value.
   - For a slider bar presentation, do one of the following:
     - Type a value into the Value field and press Enter.
     - Select the slider bar and drag its handle with the mouse to change the value or select the slider bar and use the arrow keys to move its handle to change the value.
3. Click the Apply button to save your changes.
4. Click the Reconfigure toolbar button to make your changes take effect.
Restoring the default values of a setting

To restore the default values of a setting:

1. In the left panel of the Polling and Thresholds Console, select the setting to display the parameters of the setting in the right panel of the console.
2. Click Restore Defaults.
3. Click the Reconfigure toolbar button to make your changes take effect.

Modify the priority of groups

In any group category, you can arrange the groups in a high-to-low priority. A candidate member object is compared against the highest priority group first and becomes a member of the first group for which there is a criteria match.

The Priorities tab shows groups in the order of their priority, from highest to lowest.

To change the priority of a group:

1. In the Priorities tab, select the group for which you want to change the priority.
2. Click the up or down arrow to change its position relative to the other groups.
3. Click the Apply button to save your changes.
4. Click the Reconfigure toolbar button to make your changes take effect.

Edit matching criteria

A group’s matching criteria, which appear at the top of the Matching Criteria tab, are defined by using the attributes of the target class that is associated with the group. Each matching criterion has three fields: Name, Description, and Value.

- Name identifies the name of the target class attribute.
- Description is the description of the target class attribute.
- Value is the value of the target class attribute, which can be any combination of text, integers, and wildcards. The Value field for a matching criterion is not case-sensitive.

As an example of a matching criterion for target class UnitaryComputerSystem:

- If you specify "Router" for the Type attribute, only routers become members of the group.
- If you specify "R1*" for the Name attribute, only routers with names that begin with the string R1 become members of the group.


When a managed object matches a group’s target class and matches all of the attributes that are defined for the target class, the managed object becomes a member of the group.
Adding or removing matching criteria

To add or remove matching criteria:

1. In the Disabled Criteria area of the Matching Criteria tab, select a matching criterion.
2. Click Enable to make the criterion active, moving it to the top of the Matching Criteria tab.
   
   Use Disable to deactivate the criterion, moving it to the Disabled Criteria area of the Matching Criteria tab.
3. If you are adding a matching criterion, type a matching pattern in the Value field.
4. Click the Apply button to save your changes.
5. Click the Reconfigure toolbar button to make your changes take effect.

Changing the value of a matching criterion

To change the value of a matching criterion:

1. In the Matching Criteria tab, select the string in the Value field or double-click the Value field to highlight the current value.
2. Type the new value.
3. Click the Apply button to save your changes.
4. Click the Reconfigure toolbar button to make your changes take effect.

Network Protocol Manager compares a managed object against the matching criteria of the group with the highest priority. If an object matches all the criteria, Network Protocol Manager adds the object as a member of the group. Otherwise, Network Protocol Manager compares the object against the matching criteria of the group with the second highest priority, and so on.

Create new groups

You can create additional groups within any group category.

Creating a new group enables you to customize the settings for a group of managed objects. You can use two methods to create a new group:

- Copy an existing group. The new group contains the same settings and thresholds as the original group. Matching criteria are not copied.
- Create an empty group. The new group does not contain any settings or members. You must add settings and matching criteria, and set the priority of the new group.

After you create a new group, use the procedures described in this chapter to add settings and matching criteria and to set the priority of the new group.
Copying an existing group

To copy an existing group:

1. In the left panel of the Polling and Thresholds Console, right-click the group that you want to copy.
2. Select Copy from the pop-up menu to display the Copy Group dialog box.
3. In the dialog box, type a name and an optional description for the new group and click OK.
4. Edit the settings, matching criteria, and priority of the new group. Change the value of any parameters as necessary.
5. Click the Reconfigure toolbar button to make your changes take effect.

Creating an empty group

To create an empty group:

1. In the left panel of the Polling and Thresholds Console, right-click the group for which you want to create a new group.
2. Select New Group from the pop-up menu to display the New Group dialog box.
3. In the dialog box, type a name and an optional description for the new group and click OK.
4. Add settings and matching criteria, and set the priority of the new group. Change the values of any thresholds or parameters as necessary.
5. Click the Reconfigure toolbar button to make your changes take effect.
Using the Polling and Thresholds Console
CHAPTER 10
Configuring Polling and Threshold Groups

This chapter describes how to configure polling and threshold groups for Network Protocol Manager. It consists of the following sections:

◆ Viewing the Polling and Thresholds tabs ............................................................... 122
◆ Understanding SNMP polling, CLI polling, and thresholds ..................................... 124
◆ Understanding polling groups, threshold groups, and settings.............................. 125
◆ Modifying polling and threshold groups ................................................................ 125
◆ Default polling groups and settings ...................................................................... 126
◆ Default threshold groups and settings ................................................................... 137
Viewing the Polling and Thresholds tabs

Figure 31 on page 122 shows the Polling tab of a Polling and Thresholds Console that is connected to a Network Protocol Manager for BGP named INCHARGE-BGP. The right panel of the console identifies “BGP SNMP Setting” as the setting for the default polling group “BGP.”

Figure 31 Polling tab for Network Protocol Manager for BGP

Figure 32 on page 123 shows the Thresholds tab of the Polling and Thresholds Console that is connected to INCHARGE-BGP. The right panel of the console identifies “BGP Session Flapping” as the setting for the default threshold group “BGP Protocol Endpoints.”
Figure 32 Thresholds tab for Network Protocol Manager for BGP

Instructions for opening the Polling and Thresholds Console are presented in “Opening the Global Console” on page 37
Understanding SNMP polling, CLI polling, and thresholds

As indicated in Figure 33 on page 124, Network Protocol Manager uses SNMP polling and CLI polling to monitor the managed network. The monitoring is controlled by polling-related and threshold-related objects that are created for Network Protocol Manager through the Polling and Thresholds Console.

Network Protocol Manager monitors the health of the network by periodically sending SNMP polls or CLI polls to the routing-enabled devices to gather status information. The polled status information, in addition to the received BGP and OSPF trap messages, received BGP and OSPF syslog messages, and received IP Availability Manager status updates, serves as input to the correlation analysis function of Network Protocol Manager. Appendix E, "SNMP Poller," describes SNMP polling for correlation analysis.

The execution of SNMP polling requires SNMP read credentials, and the execution of CLI polling requires CLI login credentials. The SNMPv1, v2c, or v3 read credentials for a discovered device are stored in the attributes of the SNMPAgent object that is created for the device's SNMP agent. The CLI login credentials for a discovered device are stored in a CLI device-access object. Network Protocol Manager imports SNMPAgent and CLI device-access objects from IP Availability Manager.
Understanding polling groups, threshold groups, and settings

Using the Polling and Thresholds Console, you can customize the SNMP polling and CLI polling for Network Protocol Manager by modifying default polling groups, or by creating new polling groups. The polling groups periodically poll the managed routing-enabled routers to collect protocol session (adjacency) availability data.

Using the Polling and Thresholds Console, you can also customize the polling thresholds for Network Protocol Manager by modifying default threshold groups, or by creating new threshold groups.

Network Protocol Manager uses the settings in a polling or threshold group to assign parameters to the group.

Modifying polling and threshold groups

Procedures for modifying existing groups and creating new ones are given in “Working with groups and settings” on page 115.

When you finish editing the properties of a group, perform these steps:

1. Click the **Apply** button to save your configuration changes to an existing group object or to a newly created group object in the repository of Network Protocol Manager.

2. Click the **Reconfigure** toolbar button to make your configuration changes take effect.

When the reconfiguration completes, Network Protocol Manager imports the group object and saves the group object to its repository. Then, for a polling group object, Network Protocol Manager starts the polling that is configured for the object; for a threshold group object, Network Protocol Manager starts using the polling thresholds that are configured for the object.
Default polling groups and settings

Network Protocol Manager provides five default polling groups. **Table 12 on page 126** through **Table 15 on page 126** list the default polling groups, their target classes, and their settings. The tables also identify the devices that are supported for the polling groups.

**Table 12** Default Network Protocol Manager for BGP polling groups

<table>
<thead>
<tr>
<th>Polling group</th>
<th>Target class and matching criteria</th>
<th>Settings</th>
<th>Supported devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>BGPProtocolEndpoint with attributes: IsManaged = TRUE, SystemName = *</td>
<td>BGP SNMP Setting (default setting), BGP External Setting</td>
<td>Cisco and Juniper</td>
</tr>
<tr>
<td>IPv6 BGP</td>
<td>HasIPv6=TRUE</td>
<td>BGP_Cli_Setting</td>
<td>Cisco and Juniper</td>
</tr>
</tbody>
</table>

**Table 13** Default Network Protocol Manager for EIGRP polling groups

<table>
<thead>
<tr>
<th>Polling group</th>
<th>Target class and matching criteria</th>
<th>Settings</th>
<th>Supported devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP</td>
<td>UnitaryComputerSystem with attributes: IsManaged = TRUE, SystemName = *</td>
<td>EIGRP CLI Setting (default setting), EIGRP EXTERNAL Setting</td>
<td>Cisco</td>
</tr>
</tbody>
</table>

**Table 14** Default Network Protocol Manager for IS-IS polling groups

<table>
<thead>
<tr>
<th>Polling group</th>
<th>Target class and matching criteria</th>
<th>Settings</th>
<th>Supported devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Devices</td>
<td>UnitaryComputerSystem with attributes: IsManaged = TRUE, Vendor = CISCO</td>
<td>ISIS CISCO CLI Setting (default setting), ISIS EXTERNAL Setting</td>
<td>Cisco</td>
</tr>
<tr>
<td>Juniper Devices</td>
<td>UnitaryComputerSystem with attributes: IsManaged = TRUE, Vendor = JUNIPER</td>
<td>ISIS JUNIPER SNMP Setting (default setting), ISIS EXTERNAL Setting</td>
<td>Juniper</td>
</tr>
</tbody>
</table>

**Table 15** Default Network Protocol Manager for OSPF polling groups

<table>
<thead>
<tr>
<th>Polling group</th>
<th>Target class and matching criteria</th>
<th>Settings</th>
<th>Supported devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF</td>
<td>OSPFInterface_Base with attributes: IsManaged = TRUE, SystemName = *</td>
<td>OSPF SNMP Setting (default setting), OSPF External Setting</td>
<td>Cisco and Juniper</td>
</tr>
</tbody>
</table>

Three things to note about **Table 12 on page 126** through **Table 15 on page 126**:

- Only discovered objects that match the type and attribute values in the “Target class and matching criteria” column can become members of the group.
• By default, all discovered objects that match the type and attribute values in the “Target class and matching criteria” column become members of the group.

You can specify matching criteria for a polling group to limit its membership, as explained in “Edit matching criteria” on page 117.

• The availability of a license for the EMC Smarts Adapter for Alcatel-Lucent 5620 SAM EMS (the Adapter) determines whether the following additional polling groups appear:
  • 5620 SAM BGP
  • 5620 SAM Devices
  • 5620 SAM OSPF

The 5620 SAM polling groups appear only if the Adapter license is available. The 5620 SAM polling groups are described in the EMC Smarts Adapter for Alcatel-Lucent 5620 SAM EMS User Guide.

### BGP polling group

The BGP default polling group is used by Network Protocol Manager for BGP to monitor the availability of BGP sessions. Network Protocol Manager for BGP monitors the availability by monitoring the BGPProtocolEndpoints that are discovered on Cisco or Juniper devices.

**NOTICE**

Because the standards-based BGP4 MIB (defined in RFC 1657) is used by both Cisco and Juniper devices, Network Protocol Manager for BGP uses SNMP to discover and monitor the BGP topology for Cisco and Juniper devices. The BGP polling group uses SNMP polling to monitor BGP sessions by monitoring the BGPProtocolEndpoints on the discovered devices.

The BGP polling group has a default setting and an optional setting:

• BGP SNMP Setting (default)
• BGP External Setting (optional)

The two settings are mutually exclusive, which means that only one or the other (but not both) can be specified for a BGP polling group at any given time.

#### BGP SNMP Setting

The BGP SNMP Setting determines the polling intervals that are used by Network Protocol Manager for BGP to monitor BGP protocol endpoints. Network Protocol Manager for BGP monitors the endpoints by probing the SNMP tables on the BGP-enabled devices.

Table 16 on page 128 lists the BGP SNMP Setting parameters.
### Table 16  BGP SNMP Setting parameters and their values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnalysisMode</td>
<td>ENABLED</td>
<td>Enables or disables:</td>
</tr>
<tr>
<td></td>
<td>DISABLED</td>
<td>1. The Network Protocol Manager for BGP polling of BGP endpoint</td>
</tr>
<tr>
<td></td>
<td>Default: ENABLED</td>
<td>(BGPProtocolEndpoint) data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. The subsequent analysis of the polled data to determine the status of BGP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sessions.</td>
</tr>
<tr>
<td>PollingInterval</td>
<td>30 to 3600 seconds</td>
<td>Sets the time between successive polls.</td>
</tr>
<tr>
<td></td>
<td>Default: 240 seconds</td>
<td></td>
</tr>
<tr>
<td>Retries</td>
<td>0 to 10 retries</td>
<td>Sets the number of retry polls to perform when the initial poll fails.</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
<td></td>
</tr>
<tr>
<td>Timeout</td>
<td>10 to 10000 milliseconds</td>
<td>Sets the amount of time to wait for the poll response before the first poll</td>
</tr>
<tr>
<td></td>
<td>Default: 700 milliseconds</td>
<td>response times out. The timeout value doubles for each successive retry.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Timeout=700 msec (0.7 sec) and Retries=3:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0.7 seconds for first retry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1.4 seconds for second retry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2.8 seconds for third retry</td>
</tr>
</tbody>
</table>

### BGP External Setting

The BGP External Setting serves two purposes:

- Provides a means of testing the BGP endpoint instrumentation and analysis functionality of Network Protocol Manager for BGP.
- Provides a means for Network Protocol Manager for BGP to import BGP endpoint status updates from an EMC Smarts adapter, such as the EMC Smarts Adapter for Alcatel-Lucent 5620 SAM EMS.

Table 17 on page 129 lists the BGP External Setting parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnalysisMode</td>
<td>ENABLED, DISABLED, Default: ENABLED</td>
<td>Enables or disables the availability analysis of the BGP endpoint (BGPProtocolEndpoint) data collected from an external source.</td>
</tr>
<tr>
<td>PeerState</td>
<td>UNKNOWN, IDLE, CONNECT, ACTIVE, OPENSENT, OPENCONFIRM, ESTABLISHED, Default: ESTABLISHED</td>
<td>Determines the initial peer state for the stored instrumentation objects that represent BGPProtocolEndpoints.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>UNKNOWN</strong> is the default PeerState value before Network Protocol Manager for BGP sends SNMP polls to the device that is hosting the BGP endpoint.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>IDLE</strong> indicates that the BGP service for the BGP endpoint refuses all incoming BGP connections. No resources are allocated to the peer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>CONNECT</strong> indicates that the BGP service for the BGP endpoint is waiting for the transport protocol connection to be completed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>ACTIVE</strong> indicates that the BGP service for the BGP endpoint is trying to acquire a peer by initiating a transport protocol connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>OPENSENT</strong> indicates that the BGP service for the BGP endpoint is waiting for an OPEN message from its peer. When an OPEN message is received, the BGP service checks all fields for correctness.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>OPENCONFIRM</strong> indicates that the BGP service for the BGP endpoint is waiting for a KEEPALIVE or NOTIFICATION message. If the host device receives a KEEPALIVE message, the BGP service changes the state to Established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>ESTABLISHED</strong> indicates that the BGP service for the BGP endpoint can exchange UPDATE, NOTIFICATION, and KEEPALIVE messages with its peer.</td>
</tr>
</tbody>
</table>
EIGRP polling group

The EIGRP default polling group is used by Network Protocol Manager for EIGRP to monitor the availability of EIGRP sessions. Network Protocol Manager for EIGRP monitors the availability by monitoring the EIGRPProtocolEndpoints that are discovered on Cisco devices.

**NOTICE**

Because the enterprise EIGRP MIB is typically not used by Cisco devices, Network Protocol Manager for EIGRP uses CLI to discover and monitor the EIGRP topology for Cisco devices. The EIGRP polling group uses CLI polling to monitor EIGRP sessions by monitoring the EIGRPProtocolEndpoints on the discovered Cisco devices.

The EIGRP polling group has a default setting and an optional setting:

- EIGRP CLI Setting (default)
- EIGRP EXTERNAL Setting (optional)

The two settings are mutually exclusive, which means that only one or the other (but not both) can be specified for an EIGRP polling group at any given time.

**EIGRP CLI Setting**

The EIGRP CLI Setting determines the polling intervals that are used by Network Protocol Manager for EIGRP to establish Telnet, SSH1, or SSH2 sessions to the Cisco devices and invoke the following CLI command:

```
show ip eigrp neighbors
```

The command provides the IP address of the target device's EIGRP neighbor (remote) and the local interface by which the neighbor can be reached.

**Table 18 on page 130** lists the EIGRP CLI Setting parameters.

**Table 18** EIGRP CLI Setting parameters and their values (page 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnalysisMode</td>
<td>ENABLED, DISABLED</td>
<td>Enables or disables: 1. The Network Protocol Manager for EIGRP polling of EIGRP endpoint (EIGRPProtocolEndpoint) data. 2. The subsequent analysis of the polled data to determine the status of EIGRP sessions.</td>
</tr>
<tr>
<td>PollingInterval</td>
<td>30 to 3600 seconds, Default: 240 seconds</td>
<td>Sets the time between successive polls.</td>
</tr>
<tr>
<td>Retries</td>
<td>0 to 10 retries, Default: 3</td>
<td>Sets the number of retry polls to perform when the initial poll fails.</td>
</tr>
</tbody>
</table>
Configuring Polling and Threshold Groups

EIGRP EXTERNAL Setting

The EIGRP EXTERNAL Setting serves two purposes:

- Provides a means of testing the EIGRP endpoint instrumentation and analysis functionality of Network Protocol Manager for EIGRP.
- Provides a means for Network Protocol Manager for EIGRP to import EIGRP endpoint status updates from an EMC Smarts adapter, such as the EMC Smarts Adapter for Alcatel-Lucent 5620 SAM EMS.
- Table 19 on page 131 lists the EIGRP EXTERNAL Setting parameters.

Table 19  EIGRP EXTERNAL Setting parameters and their values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eigrpPeerAdminStatus</td>
<td>UNKNOWN, UP, DOWN, Default: UNKNOWN</td>
<td>Determines the initial peer administrative state for the stored instrumentation objects that represent EIGRPProtocolEndpoints.</td>
</tr>
<tr>
<td>PeerState</td>
<td>UNKNOWN, IDLE, CONNECT, ACTIVE, OPENSENT, OPENCONFIRM, ESTABLISHED, Default: UNKNOWN</td>
<td>Determines the initial peer state for the stored instrumentation objects that represent EIGRPProtocolEndpoints.</td>
</tr>
</tbody>
</table>

Cisco Devices polling group

The Cisco Devices default polling group is used by Network Protocol Manager for IS-IS to monitor the availability of IS-IS sessions (IS-IS adjacencies). Network Protocol Manager for IS-IS monitors the availability by monitoring the ISISInterfaces that are discovered on Cisco devices.

**NOTICE**

Because the standards-based IS-IS MIB (defined in RFC 1195) is not used by Cisco devices, Network Protocol Manager for IS-IS uses CLI to discover and monitor the IS-IS topology for Cisco devices. The Cisco Devices polling group uses CLI polling to monitor IS-IS sessions by monitoring the ISISInterfaces on the discovered Cisco devices.
Configuring Polling and Threshold Groups

The Cisco Devices polling group has a default setting and an optional setting:

- **ISIS CISCO CLI Setting** (default)
- **ISIS EXTERNAL Setting** (optional)

The two settings are mutually exclusive, which means that only one or the other (but not both) can be specified for a Cisco Devices polling group at any given time.

### ISIS CISCO CLI Setting

The ISIS CISCO CLI Setting determines the polling intervals that are used by Network Protocol Manager for IS-IS to establish Telnet, SSH1, or SSH2 sessions to the Cisco devices and invoke the following CLI command:

```
show clns neighbors detail
```

The command provides the target device's CLNS neighbor interface connections (neighbor IP addresses).

Table 20 on page 132 lists the ISIS CISCO CLI Setting parameters.

#### Table 20 ISIS CISCO CLI Setting parameters and their values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnalysisMode</td>
<td>ENABLED DISABLED</td>
<td>Enables or disables: 1. The Network Protocol Manager for IS-IS polling of IS-IS interface (ISISInterface) data. 2. The subsequent analysis of the polled data to determine the status of IS-IS sessions.</td>
</tr>
<tr>
<td>PollingInterval</td>
<td>30 to 3600 seconds Default: 240 seconds</td>
<td>Sets the time between successive polls.</td>
</tr>
<tr>
<td>Retries</td>
<td>0 to 10 retries Default: 3</td>
<td>Sets the number of retry polls to perform when the initial poll fails.</td>
</tr>
<tr>
<td>Timeout</td>
<td>10 to 10000 milliseconds Default: 700 milliseconds</td>
<td>Sets the amount of time to wait for the poll response before the first poll request times out. The timeout value doubles for each successive retry. For Timeout=700 msec (0.7 sec) and Retries=3: 0.7 seconds for first retry 1.4 seconds for second retry 2.8 seconds for third retry</td>
</tr>
</tbody>
</table>
ISIS EXTERNAL Setting

The ISIS EXTERNAL Setting serves two purposes:

- Provides a means of testing the IS-IS interface instrumentation and analysis functionality of Network Protocol Manager for IS-IS.
- Provides a means for Network Protocol Manager for IS-IS to import IS-IS interface status updates from an EMC Smarts adapter, such as the EMC Smarts Adapter for Alcatel-Lucent 5620 SAM EMS.

Table 21 on page 133 lists the ISIS EXTERNAL Setting parameters.

### Table 21  ISIS EXTERNAL Setting parameters and their values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NeighborState</td>
<td>UNKNOWN, UP, INIT, DOWN, FAILED, Default: UP</td>
<td>Determines the initial neighbor state for the stored instrumentation objects that represent IS-IS interfaces (ISISInterfaces).</td>
</tr>
</tbody>
</table>

Juniper Devices polling group

The Juniper Devices default polling group is used by Network Protocol Manager for IS-IS to monitor the availability of IS-IS sessions (IS-IS adjacencies). Network Protocol Manager for IS-IS monitors the availability by monitoring the ISISInterfaces that are discovered on Juniper devices.

**NOTICE**

Because the standards-based IS-IS MIB (defined in RFC 1195) is used by Juniper devices, Network Protocol Manager for IS-IS uses SNMP to discover and monitor IS-IS topology for Juniper devices. The Juniper Devices polling group uses SNMP polling to monitor IS-IS sessions by monitoring the ISISInterfaces on the discovered Juniper devices.

The Juniper Devices polling group has a default setting and an optional setting:

- **ISIS JUNIPER SNMP Setting** (default)
- **ISIS EXTERNAL Setting** (optional)

The two settings are mutually exclusive, which means that only one or the other (but not both) can be specified for a Juniper Devices polling group at any given time.

**ISIS JUNIPER SNMP Setting**

The ISIS JUNIPER SNMP Setting determines the polling intervals that are used by Network Protocol Manager for IS-IS to monitor IS-IS interfaces. Network Protocol Manager for IS-IS monitors the interfaces by probing the SNMP tables on the IS-IS-enabled devices.

The parameters for the ISIS JUNIPER SNMP Setting parameters are identical to the parameters for the ISIS CISCO CLI Setting parameters, which are listed in Table 20 on page 132.
ISIS EXTERNAL Setting

The parameters for the ISIS EXTERNAL Setting parameters are listed in Table 21 on page 133 lists those parameters.

OSPF polling group

The OSPF default polling group is used by Network Protocol Manager for OSPF to monitor the availability of OSPF sessions (OSPF neighbor relationships, OSPF virtual links). Network Protocol Manager for OSPF monitors the availability by monitoring the OSPFInterfaces and OSPFVirtualInterfaces that are discovered on Cisco or Juniper devices.

Because the standards-based OSPF MIB (defined in RFC 1253) is used by both Cisco and Juniper devices, Network Protocol Manager for OSPF uses SNMP to discover and monitor OSPF topology for Cisco and Juniper devices. The OSPF polling group uses SNMP polling to monitor the OSPF sessions by monitoring the OSPFInterfaces and OSPFVirtualInterfaces on the discovered devices.

The OSPF polling group has a default setting and an optional setting:

- OSPF SNMP Setting (default)
- OSPF External Setting (optional)

The two settings are mutually exclusive, which means that only one or the other (but not both) can be specified for an OSPF polling group at any given time.

OSPF SNMP Setting

The OSPF SNMP Setting determines the polling intervals that are used by Network Protocol Manager for OSPF to monitor OSPF interfaces. Network Protocol Manager for OSPF monitors the interfaces by probing the SNMP tables on the OSPF-enabled devices.

Table 22 on page 134 lists the OSPF SNMP Setting parameters.

**Table 22** OSPF SNMP Setting parameters and their values (page 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnalysisMode</td>
<td>ENABLED</td>
<td>Enables or disables: 1. The Network Protocol Manager for OSPF polling of OSPF interface (OSPFInterface, OSPFVirtualInterface) data. 2. The subsequent analysis of the polled data to determine the status of OSPF sessions.</td>
</tr>
<tr>
<td>PollingInterval</td>
<td>30 to 3600 seconds</td>
<td>Sets the time between successive polls.</td>
</tr>
<tr>
<td></td>
<td>Default: 240 seconds</td>
<td></td>
</tr>
<tr>
<td>Retries</td>
<td>0 to 10 retries</td>
<td>Sets the number of retry polls to perform when the initial poll fails.</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
<td></td>
</tr>
</tbody>
</table>
OSPF External Setting

The OSPF External Setting serves two purposes:

- Provides a means of testing the OSPF interface instrumentation and analysis functionality of Network Protocol Manager for OSPF.
- Provides a means for Network Protocol Manager for OSPF to import OSPF interface status updates from an EMC Smarts adapter, such as the EMC Smarts Adapter for Alcatel-Lucent 5620 SAM EMS.

Table 23 on page 135 lists the OSPF External Setting parameters.

### Table 23 OSPF External Setting parameters and their values (page 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnalysisMode</td>
<td>ENABLED, DISABLED</td>
<td>Enables or disables the availability analysis of OSPF interface (OSPFInterface, OSPFVirtualInterface) data collected from an external source.</td>
</tr>
<tr>
<td>InitialAdminStatus</td>
<td>UNKNOWN, ENABLED, DISABLED</td>
<td>Determines the initial administrative state for the stored instrumentation objects that represent OSPF interfaces.</td>
</tr>
<tr>
<td>InitialIfState</td>
<td>UNKNOWN, DOWN, LOOPBACK, WAITING, POINT_TO_POINT, DESIGNATED_ROUTER, BACKUP_DESIGNATED_ROUTER, OTHER_DESIGNATED_ROUTER</td>
<td>Determines the initial connection state for the stored instrumentation objects that represent OSPF interfaces.</td>
</tr>
<tr>
<td>InitialMulticastIfState</td>
<td>UNKNOWN, DOWN, LOOPBACK, WAITING, POINT_TO_POINT, DESIGNATED_ROUTER, BACKUP_DESIGNATED_ROUTER, OTHER_DESIGNATED_ROUTER</td>
<td>Determines the initial multicast IF state for the stored instrumentation objects that represent OSPF interfaces.</td>
</tr>
</tbody>
</table>

---

Table 22 OSPF SNMP Setting parameters and their values (page 2 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>10 to 10000 milliseconds Default: 700 milliseconds</td>
<td>Sets the amount of time to wait for the poll response before the first poll request times out. The timeout value doubles for each successive retry. For Timeout=700 msec (0.7 sec) and Retries=3: 0.7 seconds for first retry, 1.4 seconds for second retry, 2.8 seconds for third retry.</td>
</tr>
</tbody>
</table>
### Table 23  OSPF External Setting parameters and their values (page 2 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InitialNeighborState</td>
<td>UNKNOWN, DOWN, ATTEMPT, INIT, TWO_WAY, EXCHANGE_START, EXCHANGE, LOADING, FULL</td>
<td>Determines the initial neighbor state for the stored instrumentation objects that represent OSPF interfaces.</td>
</tr>
<tr>
<td>InitialNonMulticastIfState</td>
<td>UNKNOWN, DOWN, LOOPBACK, WAITING, POINT_TO_POINT, DESIGNATED_ROUTER, BACKUP_DESIGNATED_ROUTER, OTHER_DESIGNATED_ROUTER, Default: POINT_TO_POINT</td>
<td>Determines the initial non-multicast IF state for the stored instrumentation objects that represent OSPF interfaces.</td>
</tr>
<tr>
<td>InitialVirtualIfState</td>
<td>UNKNOWN, DOWN, LOOPBACK, WAITING, POINT_TO_POINT, DESIGNATED_ROUTER, BACKUP_DESIGNATED_ROUTER, OTHER_DESIGNATED_ROUTER, Default: POINT_TO_POINT</td>
<td>Determines the initial virtual state for the stored instrumentation objects that represent OSPF virtual interfaces.</td>
</tr>
<tr>
<td>InitialVirtualNeighborState</td>
<td>UNKNOWN, DOWN, ATTEMPT, INIT, TWO_WAY, EXCHANGE_START, EXCHANGE, LOADING, FULL</td>
<td>Determines the initial virtual neighbor state for the stored instrumentation objects that represent OSPF virtual interfaces.</td>
</tr>
</tbody>
</table>
Default threshold groups and settings

Network Protocol Manager provides one default threshold group. Table 24 on page 137 lists the default threshold group, its target class, and its setting. The table also identifies the devices that are supported for the threshold group.

Table 24  Default Network Protocol Manager for BGP threshold groups

<table>
<thead>
<tr>
<th>Threshold group</th>
<th>Target class and matching criteria</th>
<th>Settings</th>
<th>Supported devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Protocol Endpoints</td>
<td>BGPProtocolEndpoint (no specified attributes)</td>
<td>BGP Session Flapping</td>
<td>Cisco and Juniper</td>
</tr>
</tbody>
</table>

Two things to note about Table 24 on page 137:

◆ Only discovered objects that match the type and attribute values in the “Target class and matching criteria” column can become members of the group.

◆ By default, all discovered objects that match the type and attribute values in the “Target class and matching criteria” column become members of the group.

You can specify matching criteria for a threshold group to limit its membership, as explained in “Edit matching criteria” on page 117.

BGP Protocol Endpoints threshold group

The BGP Protocol Endpoints default threshold group is used by Network Protocol Manager for BGP to configure parameters for flapping analysis of BGP protocol endpoints. (A flapping endpoint is an endpoint that is continually going up and down.) Flapping analysis monitors SNMP bgpEstablished traps to identify a flapping endpoint, and then generates a Flapping event for the associated BGP session to report that the endpoint is flapping.

The EMC Smarts Network Protocol Manager for BGP User Guide provides information about how the Network Protocol Manager for BGP determines that a BGP protocol endpoint is flapping.

BGP Session Flapping setting

The BGP Session Flapping setting for the BGP Protocol Endpoints threshold group controls the flapping analysis. Table 25 on page 138 lists the BGP Session Flapping setting parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLAP_Clear_Window</td>
<td>0 to any positive integer in minutes</td>
<td>Length of time to wait before clearing a Flapping event for a BGP session. The length of time should be set to a value that is greater than the value of the Trap_Time_Window. Exception: A value of 0 disables the clearing of Flapping events, meaning that Flapping events will remain active indefinitely.</td>
</tr>
<tr>
<td></td>
<td>Default: 60 minutes</td>
<td>Note: You can manually clear Flapping events at any time by setting the Trap_Count_Threshold or Trap_Time_Window parameter to 0 and then clicking the Reconfigure toolbar button. The Reconfigure toolbar button is described in Table 11 on page 113.</td>
</tr>
<tr>
<td>Trap_Count_Threshold</td>
<td>0 to any positive integer</td>
<td>Number of SNMP bgpEstablished traps that must be received within the Trap_Time_Window for Network Protocol Manager for BGP to consider a BGP protocol endpoint flapping. A value of 0 disables flapping analysis.</td>
</tr>
<tr>
<td></td>
<td>Default: 0</td>
<td></td>
</tr>
<tr>
<td>Trap_Time_Window</td>
<td>0 to any positive integer in seconds</td>
<td>Window of time within which the minimum number of bgpEstablished traps must be received for Network Protocol Manager for BGP to consider a BGP protocol endpoint flapping. When the number of received bgpEstablished traps equals or exceeds the Trap_Count_Threshold during this window of time, the endpoint is considered to be flapping. A value of 0 disables flapping analysis.</td>
</tr>
<tr>
<td></td>
<td>Default: 30 seconds</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX A
Wildcard Patterns

This appendix shows you how to use a wildcard pattern in a text field to match a number of objects instead of specifying each object by name. It consists of the following sections:

◆ Types of wildcard patterns .............................................................................. 140
Types of wildcard patterns

A wildcard pattern is a series of characters that are matched against incoming character strings. You can use these patterns when you define pattern matching criteria.

Matching is done strictly from left to right, one character or basic wildcard pattern at a time. Basic wildcard patterns are defined in Table 26 on page 140. Characters that are not part of match constructs match themselves. The pattern and the incoming string must match completely. For example, the pattern abcd does not match the input abcd or abc.

A compound wildcard pattern consists of one or more basic wildcard patterns separated by ampersand (&) or tilde (~) characters. A compound wildcard pattern is matched by attempting to match each of its component basic wildcard patterns against the entire input string. Compound wildcard patterns are listed in Table 27 on page 141.

If the first character of a compound wildcard pattern is an ampersand (&) or tilde (~) character, the compound is interpreted as if an asterisk (*) appeared at the beginning of the pattern. For example, the pattern ~*[0-9]* matches any string that does not contain any digits. A trailing instance of an ampersand character (&) can only match the empty string. A trailing instance of a tilde character (~) can be read as “except for the empty string.”

NOTICE

Spaces are interpreted as characters and are subject to matching even if they are adjacent to operators like “&”.

Table 26 Basic wildcard patterns (page 1 of 2)

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Matches any single character. For example, server?.example.com matches server3.example.com and server8.example.com, but not server10.example.com.</td>
</tr>
<tr>
<td>*</td>
<td>Matches an arbitrary string of characters. The string can be empty. For example, server*.example.com matches server-ny.example.com and server.example.com (an empty match).</td>
</tr>
<tr>
<td>[set]</td>
<td>Matches any single character that appears within [set]; or, if the first character of [set] is (^), any single character that is not in the set. A hyphen (-) within [set] indicates a range, so that [a-d] is equivalent to [abcd]. The character before the hyphen (-) must precede the character after it or the range will be empty. The character (^) in any position except the first, or a hyphen (-) at the first or last position, has no special meaning. For example, server[789:].example.com matches server7.example.com through server9.example.com, but not server6.example.com. It also matches server-.example.com. For example, server[^12].example.com does not match server1.example.com or server2.example.com, but will match server8.example.com.</td>
</tr>
</tbody>
</table>
Table 26  Basic wildcard patterns (page 2 of 2)

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;n1-n2&gt;</td>
<td>Matches numbers in a given range. Both n1 and n2 must be strings of digits, which represent nonnegative integer values. The matching characters are a non-empty string of digits whose value, as a nonnegative integer, is greater than or equal to n1 and less than or equal to n2. If either end of the range is omitted, no limitation is placed on the accepted number. For example, 98.49.&lt;1-100&gt;.10 matches a range of IPv4 addresses from 98.49.1.10 through 98.49.100.10. Example of an omitted high end of the range: &lt;50-&gt; matches any string of digits with a value greater than or equal to 50. Example of an omitted low end of the range: &lt;-150&gt; matches any value between zero and 150. For a more subtle example: The pattern &lt;1-10&gt;* matches 1, 2, up through 10, with * matching no characters. Similarly, it matches strings like 9x, with * matching the trailing x. However, it does not match 11, because &lt;1-10&gt; always extracts the longest possible string of digits (11) and then matches only if the number it represents is in range.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Matches alternatives. For example, &quot;ab</td>
</tr>
<tr>
<td>\</td>
<td>Removes the special status, if any, of the following character. Backslash () has no special meaning within a set ([set]) or range (n1-n2) construct.</td>
</tr>
</tbody>
</table>

Special characters for compound wildcard patterns are summarized in Table 27 on page 141.

Table 27  Compound wildcard patterns

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;</td>
<td>“And Also” for a compound wildcard pattern. If a component basic wildcard pattern is preceded by &amp; (or is the first basic wildcard pattern in the compound wildcard pattern), it must successfully match. Example: <em>NY</em>&amp;<em>Router</em> matches all strings that contain NY and also contain Router. Example: &lt;1-100&gt;*[02468] matches even numbers between 1 and 100 inclusive. The &lt;1-100&gt; component only passes numbers in the correct range and the *[02468] component only passes numbers that end in an even digit. Example: <em>A</em></td>
</tr>
<tr>
<td>~</td>
<td>“Except” for a compound wildcard pattern (opposite function of &amp;). If a component basic wildcard pattern is preceded by ~, it must not match. Example: 10.20.30.<em><del>10.20.30.50 matches all devices on network 10.20.30 except 10.20.30.50. Example: <em>Router</em></del></em>Cisco*&amp;<em>10.20.30.</em>~10.20.30.&lt;10-20&gt;* matches a Router, except a Cisco router, with an address on network 10.20.30, except not 10.20.30.10 through 10.20.30.20.</td>
</tr>
</tbody>
</table>
Wildcard Patterns
APPENDIX B
MIBs Polled and Traps Processed

This appendix identifies the SNMP MIBs polled and the SNMP traps that are processed by Network Protocol Manager to monitor the discovered routing topology. It consists of the following sections:

- MIBs polled and traps processed for BGP monitoring ............................................ 144
- MIBs polled and traps processed for OSPF monitoring .......................................... 147
- MIBs polled for IS-IS monitoring ............................................................................ 155
MIBs polled and traps processed for BGP monitoring

Network Protocol Manager for BGP supports SNMPv1, v2c, and v3 for the BGP4 MIB objects and traps that are defined in RFC 1657. It reads the BGP4 MIB objects that are identified in the *EMC Smarts Network Protocol Manager Discovery Guide* to discover the following BGP objects:

- BGP autonomous systems
- BGP services
- BGP protocol endpoints
- BGP sessions
- BGP session groups

Network Protocol Manager for BGP then proceeds to monitor the discovered BGP objects by:

- Polling the BGP4 MIBs on the managed devices (described in “MIBs polled by BGP” on page 144).
- Processing BGP-related SNMP traps issued by the managed devices (optional and described in “Traps processed for BGP” on page 145).
- Processing BGP-related syslog messages issued by the managed devices (optional and described in “Syslog messages processed for BGP monitoring” on page 160).

MIBs polled by BGP

After discovering and creating the BGP topology objects in its repository, Network Protocol Manager for BGP monitors the status of the BGP objects by periodically establishing SNMP sessions to the managed devices and polling the BGP4 MIB objects that are listed in Table 28 on page 144.

**Table 28** Instrumentation MIB objects polled by NPM for BGP (IPv4) (page 1 of 2)

<table>
<thead>
<tr>
<th>MIB object</th>
<th>OID</th>
<th>Description</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpPeerIdentifier</td>
<td>.1.3.6.1.2.1.15.3.1.1</td>
<td>BGP Identifier of this entry’s BGP peer.</td>
<td>BGP4 MIB</td>
</tr>
<tr>
<td>bgpPeerState</td>
<td>.1.3.6.1.2.1.15.3.1.2</td>
<td>BGP peer connection state.</td>
<td>BGP4 MIB</td>
</tr>
<tr>
<td>bgpPeerAdminStatus</td>
<td>.1.3.6.1.2.1.15.3.1.3</td>
<td>BGP peer administrative status.</td>
<td>BGP4 MIB</td>
</tr>
<tr>
<td>bgpPeerNegotiatedVersion</td>
<td>.1.3.6.1.2.1.15.3.1.4</td>
<td>Negotiated version of BGP that is running between two BGP peers.</td>
<td>BGP4 MIB</td>
</tr>
<tr>
<td>bgpPeerLocalAddr</td>
<td>.1.3.6.1.2.1.15.3.1.5</td>
<td>Local IP address of this entry’s BGP connection.</td>
<td>BGP4 MIB</td>
</tr>
<tr>
<td>bgpPeerLocalPort</td>
<td>.1.3.6.1.2.1.15.3.1.6</td>
<td>Local port for the TCP connection between the BGP peers.</td>
<td>BGP4 MIB</td>
</tr>
<tr>
<td>bgpPeerRemotePort</td>
<td>.1.3.6.1.2.1.15.3.1.8</td>
<td>Remote port for the TCP connection between the BGP peers.</td>
<td>BGP4 MIB</td>
</tr>
<tr>
<td>bgpPeerRemoteAS</td>
<td>.1.3.6.1.2.1.15.3.1.9</td>
<td>Remote autonomous system (AS) number.</td>
<td>BGP4 MIB</td>
</tr>
</tbody>
</table>
Network Protocol Manager for BGP parses the SNMP response to obtain the status information, and then updates in real time the status of the appropriate BGP objects in its repository.

**Traps processed for BGP**

Network Protocol Manager for BGP supports BGP standard SNMPv1, v2, and v3 traps that are defined in RFC 1657. It processes data found in the following fields of each trap message:

- Enterprise
- Generic Trap Identifier
- Specific Trap Identifier
- Variable-Bindings
- IP address of the SNMP agent
Network Protocol Manager for BGP extracts the information from the trap messages and updates the appropriate device attributes. In addition, for any trap message that contains at least one BGP endpoint (BGP protocol endpoint) that is not currently in its repository, Network Protocol Manager for BGP sends SNMP polls to the appropriate device to rediscover the device's BGP-related objects.

Table 29 on page 146 lists the SNMP traps that are processed by Network Protocol Manager for BGP.

<table>
<thead>
<tr>
<th>Trap name</th>
<th>OID</th>
<th>Description</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpEstablished</td>
<td>.1.3.6.1.2.1.15.7.1</td>
<td>Generated when the BGP finite state machine (FSM) enters the ESTABLISHED state.</td>
<td>BGP4 MIB</td>
</tr>
<tr>
<td>bgpBackwardTransition</td>
<td>.1.3.6.1.2.1.15.7.2</td>
<td>Generated when the BGP FSM moves from a higher numbered state to a lower numbered state.</td>
<td>BGP4 MIB</td>
</tr>
</tbody>
</table>
Cisco configuration traps processed and devices rediscovered

Network Protocol Manager for BGP also processes the following Cisco configuration traps:

- `ciscoConfigManEvent .1.3.6.1.4.1.9.9.43.2` specific Trap ID: 1
- `ciscoConfigManEvent .1.3.6.1.4.1.9.9.43.2.0.1`

For every Cisco configuration trap received, Network Protocol Manager for BGP sends SNMP polls to the appropriate device to rediscover the device's BGP-related elements.

Limitation if traps are not used

If neither SNMP traps nor syslog messages are received by Network Protocol Manager for BGP, immediate asynchronous notification of status change is not available. Instead, the response time is determined by the length of the SNMP polling interval (240 seconds by default).

**MIBs polled and traps processed for OSPF monitoring**

Network Protocol Manager for OSPF supports SNMPv1, v2c, and v3 for the OSPF MIB objects that are defined in RFC 1253 and the OSPF traps that are defined in RFC 1850. It reads the OSPF MIB objects that are identified in the *EMC Smarts Network Protocol Manager Discovery Guide* to discover the following OSPF objects:

- OSPF areas
- OSPF area configurations
- OSPF services
- OSPF networks
- OSPF interfaces
- OSPF virtual interfaces
- OSPF neighbor endpoints
- OSPF virtual neighbor endpoints
- OSPF neighbor relationships
- OSPF virtual links

Network Protocol Manager for OSPF then proceeds to monitor the discovered OSPF objects by:

- Polling the OSPF MIBs on the managed devices (described in “MIBs polled by OSPF” on page 148).
- Processing OSPF-related SNMP traps issued by the managed devices (optional and described in “Traps processed for OSPF” on page 153).
- Processing OSPF-related syslog messages issued by the managed devices (optional and described in “Enabling BGP Max Route (Prefix) threshold monitoring” on page 161).
MIBs polled by OSPF

After discovering and creating the OSPF topology objects in its repository, Network Protocol Manager for OSPF monitors the status of the OSPF objects by periodically establishing SNMP sessions to the managed devices and polling the OSPF MIB objects that are listed in Table 30 on page 148.

**NOTICE**

Cisco devices that support RFC 5643 are supported for IPv6 discovery and monitoring.

<table>
<thead>
<tr>
<th>MIB object</th>
<th>Object ID</th>
<th>Description</th>
<th>Module</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospfIfRtrPriority</td>
<td>.1.3.6.1.2.1.14.7.1.6</td>
<td>Priority of this OSPF interface. In multi-access networks, used in the designated router (DR) election algorithm.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfIfHelloInterval</td>
<td>.1.3.6.1.2.1.14.7.1.9</td>
<td>Length of time, in seconds, between the Hello packets that the router sends on this OSPF interface.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfIfRtrDeadInterval</td>
<td>.1.3.6.1.2.1.14.7.1.10</td>
<td>Number of seconds that a router's Hello packets have not been received before its neighbors declare the router down.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfIfAuthKey</td>
<td>.1.3.6.1.2.1.14.7.1.16</td>
<td>Authentication key used to authenticate OSPF interfaces.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfIfAuthType</td>
<td>.1.3.6.1.2.1.14.7.1.20</td>
<td>Authentication type specified for an OSPF interface.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfIfAdminStat</td>
<td>.1.3.6.1.2.1.14.7.1.5</td>
<td>OSPF interface's administrative status. The value formed on the interface is advertised as an internal route to some area.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfIfState</td>
<td>.1.3.6.1.2.1.14.7.1.12</td>
<td>OSPF interface state.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfIfDesignatedRouter</td>
<td>.1.3.6.1.2.1.14.7.1.13</td>
<td>IP Address of the DR.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfIfBackupDesignatedRouter</td>
<td>.1.3.6.1.2.1.14.7.1.14</td>
<td>IP Address of the BDR.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfIfEvents</td>
<td>.1.3.6.1.2.1.14.7.1.15</td>
<td>Number of state changes or error events on this OSPF interface.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfVirtIfHelloInterval</td>
<td>.1.3.6.1.2.1.14.9.1.5</td>
<td>Length of time, in seconds, between the Hello packets that the router sends on this OSPF virtual interface.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfVirtIfRtrDeadInterval</td>
<td>.1.3.6.1.2.1.14.9.1.6</td>
<td>Number of seconds that a router's Hello packets have not been received before its neighbors declare the router down.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfVirtIfState</td>
<td>.1.3.6.1.2.1.14.9.1.7</td>
<td>OSPF virtual interface states.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ospfVirtIfEvents</td>
<td>.1.3.6.1.2.1.14.9.1.8</td>
<td>Number of state changes or error events on this virtual link.</td>
<td>OSPF MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>MIB object</td>
<td>Object ID</td>
<td>Description</td>
<td>Module</td>
<td>Protocol</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>ospfv3AreaSummary</td>
<td>.1.3.6.1.2.1.1.9.1.7.1.3</td>
<td>A 32-bit integer uniquely identifying the area to which the interface connects. Area ID 0 is used for the OSPFv3 backbone.</td>
<td>OSPF v3</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3AdminStatus</td>
<td>.1.3.6.1.2.1.191.1.1.1.2</td>
<td>The administrative status of OSPFv3 in the router. The value \enabled\ denotes that the OSPFv3 Process is active on at least one interface; \disabled\ disables it on all interfaces. This object is persistent, and when written, the entity SHOULD save the change to non-volatile storage.</td>
<td>OSPF v3</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfAreaId</td>
<td>.1.3.6.1.2.1.191.1.1.1.3</td>
<td>A 32-bit integer uniquely identifying the area to which the interface connects. Area ID 0 is used for the OSPFv3 backbone.</td>
<td>OSPF v3</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfType</td>
<td>.1.3.6.1.2.1.191.1.1.1.4</td>
<td>The OSPFv3 interface type.</td>
<td>OSPF v3</td>
<td>IPv6</td>
</tr>
</tbody>
</table>
Table 30  Instrumentation MIB objects polled by Network Protocol Manager for OSPF (page 3 of 5)

<table>
<thead>
<tr>
<th>MIB object</th>
<th>Object ID</th>
<th>Description</th>
<th>Module</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospfv3IfAdminStatus</td>
<td>.1.3.6.1.2.1.191.1.7.1.5</td>
<td>The OSPFv3 interface’s administrative status. The value formed on the interface; the interface will be advertised as an internal route to some area. The value <code>disabled</code> denotes that the interface is external to OSPFv3. Note that a value of <code>disabled</code> for the object ospfv3AdminStatus will override a value of <code>enabled</code> for the interface.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfRtrPriority</td>
<td>.1.3.6.1.2.1.191.1.7.1.6</td>
<td>The priority of this interface. Used in multi-access networks, this field is used in the designated-router election algorithm. The value 0 signifies that the router is not eligible to become the Designated Router on this particular network. In the event of a tie in this value, routers will use their Router ID as a tie breaker.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfTransitDelay</td>
<td>.1.3.6.1.2.1.191.1.7.1.7</td>
<td>The estimated number of seconds it takes to transmit a Link State Update packet over this interface. LSAs contained in the update packet must have their age incremented by this amount before transmission. This value should take into account the transmission and propagation delays of the interface.</td>
<td>OSPF MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfRetransInterval</td>
<td>.1.3.6.1.2.1.191.1.7.1.8</td>
<td>The number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface. This value is also used when retransmitting database description and Link State Request packets.</td>
<td>OSPF MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfPollInterval</td>
<td>.1.3.6.1.2.1.191.1.7.1.11</td>
<td>The larger time interval, in seconds, between the Hello packets sent to an inactive, non-broadcast multi-access neighbor.</td>
<td>OSPF MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfState</td>
<td>.1.3.6.1.2.1.191.1.7.1.12</td>
<td>The OSPFv3 interface state. An interface may be in standby state if there are multiple interfaces on the link and another interface is active. The interface may be in Down state if the underlying IPv6 interface is down or if the admin status is <code>disabled</code> either globally or for the interface.</td>
<td>OSPF MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfDemand</td>
<td>.1.3.6.1.2.1.191.1.7.1.17</td>
<td>Indicates whether Demand OSPFv3 procedures (Hello suppression to FULL neighbors and setting the DoNotAge flag on propagated LSAs) should be performed on this interface.</td>
<td>OSPF MIB</td>
<td>IPv6</td>
</tr>
</tbody>
</table>
### Table 30: Instrumentation MIB objects polled by Network Protocol Manager for OSPF (page 4 of 5)

<table>
<thead>
<tr>
<th>MIB object</th>
<th>Object ID</th>
<th>Description</th>
<th>Module</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospfv3CfgNbrRowStatus</td>
<td>.1.3.6.1.2.1.191.1.10.1.6</td>
<td>This object permits management of the table by facilitating actions such as row creation, construction, and destruction. The value of this object has no effect on whether other objects in this conceptual row can be modified.</td>
<td>OSPF MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3NbrAddress</td>
<td>.1.3.6.1.2.1.191.1.9.1.5</td>
<td>The IPv6 address of the neighbor associated with the local link.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3NbrState</td>
<td>.1.3.6.1.2.1.191.1.9.1.8</td>
<td>The state of the relationship with this neighbor.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3NbrIfId</td>
<td>.1.3.6.1.2.1.191.1.9.1.12</td>
<td>The Interface ID that the neighbor advertises in its Hello packets on this link, that is, the neighbor's local interface index.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>oipv3NbrHelloSuppressed</td>
<td>.1.3.6.1.2.1.191.1.9.1.11</td>
<td>Indicates whether Hellos are being suppressed to the neighbor.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>oipv3VirtIfTransitDelay</td>
<td>.1.3.6.1.2.1.191.1.8.1.5</td>
<td>The estimated number of seconds it takes to transmit a Link State Update packet over this interface.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>oipv3VirtIfRetransInterval</td>
<td>.1.3.6.1.2.1.191.1.8.1.6</td>
<td>The number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface. This value is also used when retransmitting database description and Link State Request packets. This value should be well over the expected round-trip time.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>oipv3VirtNbrIfIndex</td>
<td>.1.3.6.1.2.1.191.1.11.1.3</td>
<td>The local Interface ID for the virtual link over which the neighbor can be reached.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>oipv3VirtNbrAddress</td>
<td>.1.3.6.1.2.1.191.1.11.1.6</td>
<td>The IPv6 address advertised by this virtual neighbor. It must be a global scope address.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>oipv3VirtNbrLsRetransQLen</td>
<td>.1.3.6.1.2.1.191.1.11.1.10</td>
<td>The current length of the retransmission queue.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>oipv3VirtNbrHelloSuppressed</td>
<td>.1.3.6.1.2.1.191.1.11.1.11</td>
<td>Indicates whether Hellos are being suppressed to the neighbor.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>oipv3IfAdminStatus</td>
<td>.1.3.6.1.2.1.191.1.7.1.5</td>
<td>The OSPFv3 interface's administrative status. The value formed on the interface; the interface will be advertised as an internal route to some area. The value 'disabled' denotes that the interface is external to OSPFv3. Note that a value of 'disabled' for the object oipv3AdminStatus will override a value of 'enabled' for the interface.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
</tbody>
</table>
Network Protocol Manager for OSPF parses the SNMP response to obtain the status information, and then updates in real time the status of the appropriate OSPF objects in its repository.

<table>
<thead>
<tr>
<th>MIB object</th>
<th>Object ID</th>
<th>Description</th>
<th>Module</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospfv3IfState</td>
<td>.1.3.6.1.2.1.191.1.7.1.12</td>
<td>The OSPFv3 interface state. An interface may be in standby state if there are multiple interfaces on the link and another interface is active. The interface may be in Down state if the underlying IPv6 interface is down or if the admin status is \disabled\ either globally or for the interface.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfDesignatedRouter</td>
<td>.1.3.6.1.2.1.191.1.7.1.13</td>
<td>The Router ID of the Designated Router.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfBackupDesignatedRouter</td>
<td>.1.3.6.1.2.1.191.1.7.1.14</td>
<td>The Router ID of the Backup Designated Router.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfEvents</td>
<td>.1.3.6.1.2.1.191.1.7.1.15</td>
<td>The number of times this OSPFv3 interface has changed its state or an error has occurred. Discontinuities in the value of this counter can occur at re-initialization of the management system and at other times as indicated by the value of ospfv3DiscontinuityTime.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfRtrPriority</td>
<td>.1.3.6.1.2.1.191.1.7.1.6</td>
<td>The priority of this interface. Used in multi-access networks, this field is used in the designated-router election algorithm. The value 0 signifies that the router is not eligible to become the Designated Router on this particular network. In the event of a tie in this value, routers will use their Router ID as a tie breaker.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfHelloInterval</td>
<td>.1.3.6.1.2.1.191.1.7.1.9</td>
<td>The length of time, in seconds, between the Hello packets that the router sends on the interface. This value must be the same for all routers attached to a common network.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ospfv3IfRtrDeadInterval</td>
<td>.1.3.6.1.2.1.191.1.7.1.10</td>
<td>The number of seconds that a router's Hello packets have not been seen before its neighbors declare the router down on the interface. This should be some multiple of the Hello interval. This value must be the same for all routers attached to a common network.</td>
<td>OSPF v3 MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>snmpCommunityContextName</td>
<td>.1.3.6.1.6.3.18.1.1.1.5</td>
<td>Name of the VRF.</td>
<td>SNMP-COMMUNITY-MIB</td>
<td>IPv4, IPv6</td>
</tr>
</tbody>
</table>
Traps processed for OSPF

Network Protocol Manager for OSPF supports OSPF standard SNMPv1, v2, and v3 traps that are defined in RFC 1850. It processes data found in the following fields of each trap message:

- Enterprise
- Generic Trap Identifier
- Specific Trap Identifier
- Variable-Bindings
- IP address of the SNMP agent

Network Protocol Manager for OSPF extracts the information from the trap messages and updates the appropriate device attributes. In addition, for any trap message that contains at least one OSPF endpoint (OSPF neighbor endpoint, OSPF virtual neighbor endpoint) that is not currently in its repository, Network Protocol Manager for OSPF sends SNMP polls to the appropriate device to rediscover the device’s OSPF-related objects.

Table 31 on page 153 lists the SNMP traps that are processed by Network Protocol Manager for OSPF.

Table 31  SNMP traps processed by Network Protocol Manager for OSPF (page 1 of 2)

<table>
<thead>
<tr>
<th>Trap name</th>
<th>OID</th>
<th>Description</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospfVirtIfStateChange</td>
<td>.1.3.6.1.2.1.14.16.2.1</td>
<td>Signifies a change in the state of an OSPF virtual interface. This trap should be generated when the interface state regresses (for example, goes from Point-to-Point to Down) or progresses to a terminal state (that is, Point-to-Point).</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfNbrStateChange</td>
<td>.1.3.6.1.2.1.14.16.2.2</td>
<td>Signifies a change in the state of a non-virtual OSPF neighbor. This trap should be generated when the neighbor state regresses or progresses to a terminal state.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfVirtNbrStateChange</td>
<td>.1.3.6.1.2.1.14.16.2.3</td>
<td>Signifies a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses or progresses to a terminal state.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfIfConfigError</td>
<td>.1.3.6.1.2.1.14.16.2.4</td>
<td>Signifies that a packet has been received on a non-virtual interface from a router whose configuration parameters conflict with this router’s configuration parameters.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfVirtIfConfigError</td>
<td>.1.3.6.1.2.1.14.16.2.5</td>
<td>Signifies that a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router’s configuration parameters.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfIfAuthFailure</td>
<td>.1.3.6.1.2.1.14.16.2.6</td>
<td>Signifies that a packet has been received on a non-virtual interface from a router whose authentication key or authentication type conflicts with this router’s authentication key or authentication type.</td>
<td>OSPF MIB</td>
</tr>
</tbody>
</table>
### Cisco configuration traps processed and devices rediscovered

Network Protocol Manager for OSPF also processes the following Cisco configuration traps:

- `ciscoConfigManEvent.1.3.6.1.4.1.9.9.43.2` specific Trap ID: 1
- `ciscoConfigManEvent.1.3.6.1.4.1.9.9.43.2.0.1`

For every Cisco configuration trap received, Network Protocol Manager for OSPF sends SNMP polls to the appropriate device to rediscover the device's OSPF-related objects.

#### Table 31  SNMP traps processed by Network Protocol Manager for OSPF (page 2 of 2)

<table>
<thead>
<tr>
<th>Trap name</th>
<th>OID</th>
<th>Description</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospfVirtIfAuthFailure</td>
<td>.1.3.6.1.2.1.14.16.2.7</td>
<td>Signifies that a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router’s authentication key or authentication type.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfIfRxBadPacket</td>
<td>.1.3.6.1.2.1.14.16.2.8</td>
<td>Signifies that an OSPF packet has been received on a non-virtual interface that cannot be parsed.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfVirtIfRxBadPacket</td>
<td>.1.3.6.1.2.1.14.16.2.9</td>
<td>Signifies that an OSPF packet has been received on a virtual interface that cannot be parsed.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfTxRetransmit</td>
<td>.1.3.6.1.2.1.14.16.2.10</td>
<td>Signifies that an OSPF packet has been retransmitted on a non-virtual interface.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfVirtIfTxRetransmit</td>
<td>.1.3.6.1.2.1.14.16.2.11</td>
<td>Signifies that an OSPF packet has been retransmitted on a virtual interface. All packets that may be retransmitted are associated with a link-state database entry.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfOriginLsa</td>
<td>.1.3.6.1.2.1.14.16.2.12</td>
<td>Signifies that a new link-state advertisement (LSA) has been originated by this router. This trap should not be invoked for simple refreshes of LSAs (which happens every 30 minutes), but instead is invoked only when an LSA is originated (or re-originated) due to a topology change.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfMaxAgeLsa</td>
<td>.1.3.6.1.2.1.14.16.2.13</td>
<td>Signifies that one of the LSAs in the router’s link-state database has aged to MaxAge.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfLsdbOverflow</td>
<td>.1.3.6.1.2.1.14.16.2.14</td>
<td>Signifies that the number of LSAs in the router’s link-state database has exceeded <code>ospfExtLsdbLimit</code>.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfLsdbApproachingOverflow</td>
<td>.1.3.6.1.2.1.14.16.2.15</td>
<td>Signifies that the number of LSAs in the router’s link-state database has exceeded 90 percent of <code>ospfExtLsdbLimit</code>.</td>
<td>OSPF MIB</td>
</tr>
<tr>
<td>ospfIfStateChange</td>
<td>.1.3.6.1.2.1.14.16.2.16</td>
<td>Signifies a change in the state of a non-virtual OSPF interface. This trap should be generated when the interface state regresses or progresses to a terminal state.</td>
<td>OSPF MIB</td>
</tr>
</tbody>
</table>
Limitation if traps are not used

If neither SNMP traps nor syslog messages are received by Network Protocol Manager for OSPF, immediate asynchronous notification of status change is not available. Instead, the response time is determined by the length of the SNMP polling interval (240 seconds by default).

**MIBs polled for IS-IS monitoring**

Network Protocol Manager for IS-IS supports the IS-IS MIB objects that are defined in RFC 1195 and in RFC 4444.

**IS-IS MIB objects that are defined in RFC 1195**

Network Protocol Manager for IS-IS supports SNMPv1, v2c, and v3 for the IS-IS MIB objects that are defined in RFC 1195. It does not receive or process SNMP traps.

Because the IS-IS MIB is used by Juniper devices but not by Cisco devices, Network Protocol Manager for IS-IS uses:

- SNMP discovery and SNMP polling to discover and monitor the IS-IS topology for Juniper devices.
- CLI discovery and CLI polling to discover and monitor the IS-IS topology for Cisco devices.

The CLI commands that are invoked for IS-IS discovery are identified in the *EMC Smarts Network Protocol Manager Discovery Guide*, and the CLI commands that are invoked for IS-IS monitoring are described in “CLI commands for IS-IS monitoring” on page 166.

For Juniper devices, Network Protocol Manager for IS-IS reads the IS-IS MIB objects that are identified in the *EMC Smarts Network Protocol Manager Discovery Guide* to discover the following IS-IS objects:

- IS-IS areas
- IS-IS services
- IS-IS networks
- IS-IS interfaces
- IS-IS neighbor endpoints
- IS-IS adjacencies

Network Protocol Manager for IS-IS then proceeds to monitor the discovered IS-IS objects by polling the IS-IS MIBs on the managed devices.
MIBs Polled and Traps Processed

MIBs polled for IS-IS (RFC 1195)

After discovering and creating the IS-IS topology objects in its repository, Network Protocol Manager for IS-IS monitors the status of the IS-IS objects by periodically establishing SNMP sessions to the Juniper devices and polling the IS-IS MIB objects that are listed in Table 32 on page 156.

Table 32 MIB object polled for instrumentation by Network Protocol Manager for IS-IS (page 1 of 2)

<table>
<thead>
<tr>
<th>MIB object</th>
<th>OID</th>
<th>Description</th>
<th>Module</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>isisISAdjState</td>
<td>1.3.6.1.3.37.1.5.1.1.2</td>
<td>The state of the adjacency: 1 (DOWN) 2 (INITIALIZING) 3 (UP) 4 (FAILED)</td>
<td>IS-IS MIB</td>
<td>IPv4</td>
</tr>
<tr>
<td>ciiAreaAddr</td>
<td>1.3.6.1.4.1.9.10.118.1.1.3.1.1</td>
<td>The area address reported in a Level 1 link-state packet (LSP).</td>
<td>Cisco IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ciiSysType</td>
<td>1.3.6.1.4.1.9.10.118.1.1.1.2</td>
<td>The level running on Intermediate System. This object follows the behavior of replaceOnlyWhileDisabled.</td>
<td>Cisco IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ciiISAdjIPAddrAddress</td>
<td>1.3.6.1.4.1.9.10.118.1.6.3.1.3</td>
<td>The IP address received by the Intermediate System-to-Intermediate System Hello (IIH) Protocol data units (PDU) from the neighboring router.</td>
<td>Cisco IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ciiCircIfIndex</td>
<td>1.3.6.1.4.1.9.10.118.1.3.2.1.2</td>
<td>The ID for this Intermediate System. The object value derived is implementation-specific. Some implementations may automatically assign values and not permit an SNMP write, while others may require the value to be set manually.</td>
<td>Cisco IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ciiISAdjNeighPriority</td>
<td>1.3.6.1.4.1.9.10.118.1.6.1.1.10</td>
<td>Priority of the neighboring Intermediate System for becoming the designated Intermediate System.</td>
<td>Cisco IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>ciiISAdjState</td>
<td>1.3.6.1.4.1.9.10.118.1.6.1.1.2</td>
<td>The state of the adjacency: 1 (DOWN) 2 (INITIALIZING) 3 (UP) 4 (FAILED)</td>
<td>Cisco IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>isisISAdjState</td>
<td>1.3.6.1.4.1.9.10.118.1.6.1.1.2</td>
<td>The state of the adjacency: 1 (DOWN) 2 (INITIALIZING) 3 (UP) 4 (FAILED)</td>
<td>Cisco IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>isisAreaAddr</td>
<td>1.3.6.1.2.1.138.1.1.3.1.1</td>
<td>The area address reported in a Level 1 LSP.</td>
<td>Juniper IS-IS MIB</td>
<td>IPv6</td>
</tr>
</tbody>
</table>
MIBs polled for IS-IS monitoring

### MIBs Polled for IS-IS Monitoring

The Network Protocol Manager for IS-IS parses the SNMP response to obtain the status information, and then updates in real time the status of the appropriate IS-IS objects in its repository.

#### IS-IS MIB objects that are defined in RFC 4444

The RFC 4444 support is only for IPv6 IS-IS.

**NOTICE**

IS-IS RFC 4444 MIB support is verified and validated for devices only with IPv6 configured in them. For pure IPv4 devices with RFC 4444 IS-IS-MIB support, the devices get discovered by the IP Manager but will not be listed as part of ISIS_TopologyCollection and hence the Network Protocol Manager for IS-IS will not discover the devices.

RFC 4444 followed devices (IS-IS IPv6 MIB) are fully supported regardless of device vendors (Cisco and Juniper). Discovery and monitoring support is complete and the Network Protocol Manager for IS-IS is able to stitch topologies discovered using RFC 4444 MIBs.

Following is the complete OID information for RFC 4444:

```
# ISIS-MIB - RFC 4444
```

<table>
<thead>
<tr>
<th>MIB object</th>
<th>OID</th>
<th>Description</th>
<th>Module</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>isisRouterLevel</td>
<td>.1.3.6.1.2.1.138.1.1.6.1.2</td>
<td>The level at which the information about this Intermediate System is received.</td>
<td>Juniper IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>isisISAdjIPAddrAddress</td>
<td>.1.3.6.1.2.1.138.1.6.3.1.3</td>
<td>The IP address received by the IIH PDUs from the neighboring router. The type of this address is determined by the value of the isisISAdjIPAddrType object.</td>
<td>Juniper IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>isisRouterSysID</td>
<td>.1.3.6.1.2.1.138.1.1.6.1.1</td>
<td>The System ID of the Intermediate System.</td>
<td>Juniper IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>isisISAdjNeighPriority</td>
<td>.1.3.6.1.2.1.138.1.6.1.1.10</td>
<td>Priority of the neighboring Intermediate System for becoming the designated Intermediate System.</td>
<td>Juniper IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td>isisISAdjState</td>
<td>.1.3.6.1.2.1.138.1.6.1.1.2</td>
<td>The state of the adjacency:</td>
<td>Juniper IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 (DOWN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 (INITIALIZING)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 (UP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 (FAILED)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>isisISAdjState</td>
<td>.1.3.6.1.2.1.138.1.6.1.1.2</td>
<td>The state of the adjacency:</td>
<td>Juniper IS-IS MIB</td>
<td>IPv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 (DOWN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 (INITIALIZING)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 (UP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 (FAILED)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MIBs Polled and Traps Processed

#isisAreaAddr {40, "1.3.6.1.2.1.138.1.3.1.1"},
#isisSysLevelType {45, "1.3.6.1.2.1.138.1.1.1.2"},
#isisISAdjIPAddrAddress {50, "1.3.6.1.2.1.138.1.6.3.1.3"},
#isisCircIfIndex {51, "1.3.6.1.2.1.138.1.3.2.1.2"},
#isisRouterSysID {55, "1.3.6.1.2.1.138.1.1.1.3"},
#isisISAdjNeighPriority {60, "1.3.6.1.2.1.138.1.6.1.1.10"},
#isisISAdjState {65, "1.3.6.1.2.1.138.1.6.1.1.2"}
APPENDIX C
Syslog Messages Processed

This appendix identifies the syslog messages that are processed by Network Protocol Manager to monitor the discovered routing topology. It consists of the following sections:

◆ Syslog messages processed for BGP monitoring .............................................. 160
◆ Syslog messages processed for OSPF monitoring ............................................. 162
Syslog messages processed for BGP monitoring

When syslog message processing is enabled for BGP, Network Protocol Manager for BGP obtains configuration, change, and BGP session status information for the managed devices from syslog messages that are sent by the devices. Network Protocol Manager for BGP extracts the information from the syslog messages and updates the attributes of the appropriate topology objects in its repository.

Processing syslog messages is recommended for BGP, but not required, because Network Protocol Manager for BGP polls the network for status information. However, if neither syslog messages nor SNMP traps are received by Network Protocol Manager for BGP, immediate asynchronous notification of status change is not available; instead, the response time is determined by the length of the SNMP polling interval (240 seconds by default).

Syslog message format

Network Protocol Manager for BGP reads and parses syslog messages that have the following format:

Time [Source] [Application]:
%Facility[-Subfacility]-Severity-Mnemonic: Message Text

Sample syslog message

A sample syslog message that are processed by Network Protocol Manager for BGP is:

Jan 29 15:49:48.699: %BGP-3-NOTIFICATION: sent to neighbor 10.0.1.101 4/0 (hold time expired) 0 bytes

Syslog messages processed and actions taken

Table 33 on page 161 identifies which syslog messages are processed by Network Protocol Manager for BGP and what actions are taken by Network Protocol Manager for BGP. As indicated in Table 33 on page 161, candidate syslog messages have one of the following Facility-Mnemonic name combinations:

- BGP & NOTIFICATION
- BGP & ADJCHANGE
- BGP & MAXPFEXCEED
- SYS & CONFIG_1
Table 33  Syslog messages processed and actions taken

<table>
<thead>
<tr>
<th>Facility name</th>
<th>Mnemonic name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>NOTIFICATION</td>
<td>• Extracts the BGP configuration, change, and session status information from the message and updates the appropriate router attributes.</td>
</tr>
<tr>
<td></td>
<td>ADJCHANGE</td>
<td>• If the message contains at least one BGP endpoint that is not currently in the topology database, Network Protocol Manager for BGP sends SNMP polls to the appropriate device to rediscover the device's BGP-related objects.</td>
</tr>
<tr>
<td></td>
<td>MAXPFXEXCEED</td>
<td>• Parses the relevant syslog message originating from Cisco or Juniper devices after exceeding the threshold for receiving maximum routes from a neighbor over a BGP session. When the bMaxPrefixExceed setting for BGPProtocolEndPoint is set to TRUE as a result of threshold being crossed, a notification (PrefixThresholdCrossed) is generated.</td>
</tr>
<tr>
<td>SYS</td>
<td>CONFIG_I</td>
<td>• Does not extract any status information from the message. • Sends SNMP polls to the appropriate device to rediscover the device's BGP-related objects.</td>
</tr>
</tbody>
</table>

### Enabling BGP Max Route (Prefix) threshold monitoring

Network Protocol Manager for BGP monitors syslog messages from Cisco and Juniper devices to determine when the BGP Max Route (Prefix) threshold is exceeded. When Network Protocol Manager for BGP detects the threshold has been exceeded, the BGP application generates a PrefixThresholdCrossed notification for that BGP session and correlates it to the BGPsession “Down” notification.

Juniper syslog messages are not parsed for Facility-Mnemonic. Juniper syslog messages are processed based on the source device information in the message.

To receive the PrefixThresholdCrossed notification in the Notification Log Console, use sm_edit to modify the dxa-bgp.conf file available in the Service Assurance Manager deployment. Add the following lines:

```plaintext
sev BGPSession PrefixThresholdCrossed Operational 2
sub BGPSession::.*::PrefixThresholdCrossed/e
```

For example:

```plaintext
./sm_edit conf/ics/dxa-bgp.conf
22 sev BGPSession Disconnected Operational 3
23 sev BGPSession Flapping Operational 3
24 sev BGPSessionGroup Impacted Impacted 3
25 sev BGPSession PrefixThresholdCrossed Operational 2
```

56 # Send events List Subscription
```
57 sub .*::.*::*\/*p
58 sub BGPSession::.*::Disconnected/e
59 sub BGPSession::.*::Flapping/e
60 sub BGPSessionGroup::.*::Impacted/e
```
The PrefixThresholdCrossed notification clears after a configured time interval, SysCleanTime, is reached. SysCleanTime default value is 86,400 seconds (24 hours). SysCleanTime is specified in <BASEDIR>/conf/bgp/bgp.conf and the value may be changed in the Domain Manager Administration Console.

Syslog messages processed for OSPF monitoring

When syslog message processing is enabled for OSPF, Network Protocol Manager for OSPF obtains configuration, change, and OSPF adjacency status information for the managed devices from syslog messages that are sent by the devices. Network Protocol Manager for OSPF extracts the information from the syslog messages and updates the attributes of the appropriate topology objects in its repository.

Processing syslog messages is recommended for OSPF, but not required, because Network Protocol Manager for OSPF polls the network for status information. However, if neither syslog messages nor SNMP traps are received by Network Protocol Manager for OSPF, immediate asynchronous notification of status change is not available; instead, the response time is determined by the length of the SNMP polling interval (240 seconds by default).

Syslog message format

Network Protocol Manager for OSPF reads and parses syslog messages that have the following format:

Time [Source] [Application]:
%Facility[-Subfacility]-Severity-Mnemonic: Message Text

Network Protocol Manager for OSPF also reads and parses Mismatch Authentication Key syslog messages sent by Cisco devices to detect Message Digest 5 (MD5) authentication failures.

Sample syslog messages

Sample syslog messages that are processed by Network Protocol Manager for OSPF are:

Jan 29 14:11:47.566: %OSPF-5-ADJCHG: Process 100, Nbr 10.0.0.110 on XTagATM51212 from LOADING to FULL, Loading Done
Sep 11 18:27:23 ins-2.smarts.com 74: 3d00h: OSPF: Rcv pkt from 172.16.2.1, Ethernet0/0: Mismatch Authentication Key - Message Digest Key 1

The message text portion of a syslog message is sometimes quite lengthy. For example, the message text portion of an OSPF-related syslog message might look like this:

Process 100, Nbr 10.0.0.100 on Switch1.1 from FULL to DOWN, Neighbor Down: Interface down or detached Process 100, Nbr 10.0.0.110 on XTagATM51212 from FULL to DOWN, Neighbor Down: Dead timer expired Process 100, Nbr 10.0.0.110 on XTagATM51212 from LOADING to FULL, Loading Done
Syslog messages processed and actions taken

Table 34 on page 163 identifies which syslog messages are processed by Network Protocol Manager for OSPF and what actions are taken by Network Protocol Manager for OSPF. As indicated in Table 34 on page 163, candidate syslog messages have one of the following Facility–Mnemonic name combinations:

- OSPF & ADJCHG
- SYS & CONFIG_I

Table 34  Syslog messages processed and actions taken

<table>
<thead>
<tr>
<th>Facility name</th>
<th>Mnemonic name</th>
<th>Action</th>
</tr>
</thead>
</table>
| OSPF         | ADJCHG       | • Extracts the OSPF configuration, change, and adjacency status information from the message and updates the appropriate router attributes.  
• If the message contains at least one OSPF endpoint that is not currently in the topology database, Network Protocol Manager for OSPF sends SNMP polls to the appropriate device to rediscover the device's OSPF-related objects. |
| SYS          | CONFIG_I     | • Does not extract any status information from the message.  
• Sends SNMP polls to the appropriate device to rediscover the device’s OSPF-related objects. |

In addition, Network Protocol Manager for OSPF responds to Mismatch Authentication Key syslog messages for Cisco devices in the same way that it responds to syslog messages that contain the OSPF & ADJCHG Facility–Mnemonic name combinations.
This appendix identifies the CLI commands that are invoked by Network Protocol Manager to monitor the discovered routing topology. It consists of the following sections:

- CLI commands for EIGRP monitoring .......................................................... 166
- CLI commands for IS-IS monitoring ........................................................... 166
- CLI commands for BGP IPv6 discovery and monitoring of Cisco devices ... 167
- CLI commands for BGP IPv6 discovery and monitoring of Juniper devices .. 168
CLI commands for EIGRP monitoring

Because the enterprise EIGRP MIB is typically not used by Cisco devices, Network Protocol Manager for EIGRP uses CLI discovery and CLI polling to discover and monitor EIGRP topology. The CLI commands that are invoked for EIGRP discovery are identified in the *EMC Smarts Network Protocol Manager Discovery Guide*, and the CLI commands that are invoked for EIGRP monitoring are identified in this section.

Network Protocol Manager for EIGRP establishes Telnet, SSH1, or SSH2 sessions to the Cisco devices and invokes the following CLI command:

```
show ip eigrp neighbors
and
sh ip eigrp vrf * neighbors
```

The command provides the IP address of the target device’s EIGRP neighbor (remote) and the local interface by which the neighbor can be reached.

CLI commands for IS-IS monitoring

Because the standards-based IS-IS MIB is used by Juniper devices but not by Cisco devices, Network Protocol Manager for IS-IS uses:

- SNMP discovery and SNMP polling to discover and monitor the IS-IS topology for Juniper devices.
- CLI discovery and CLI polling to discover and monitor the IS-IS topology for Cisco devices.

The CLI commands that are invoked for IS-IS discovery are identified in the *EMC Smarts Network Protocol Manager Discovery Guide*, and the CLI commands that are invoked for IS-IS monitoring are described in this section.

Network Protocol Manager for IS-IS establishes Telnet, SSH1, or SSH2 sessions to the Cisco devices and invokes the following CLI command:

```
show clns neighbors detail
```

The command provides the target device’s CLNS neighbor interface connections (neighbor IP addresses).
CLI commands for BGP IPv6 discovery and monitoring of Cisco devices

**Command**

`show bgp ipv6 unicast summary`

**NOTICE**

Ensure correct configuration of the BGP connection in order to get a response to this command.

When the router configuration is modified so that changes can be made to the IPv6 configuration, then the router does not return a result for this command. As a result, any information pertaining to IPv6 configuration change cannot be obtained.

- If the configuration change affects the status of the connection and the CLI response can be retrieved, then the status of the Cisco IPv6 BGP configuration can updated.
- If the configuration change does not return any response to the CLI command, then the BGP session will be shown as disconnected (with either BGPSession::Down or BGPService::Down as appropriate) and no further processing of notifications take place.

**Sample output**

```
dev-7604_lwggw016#show bgp ipv6 unicast summary
BGP router identifier 192.168.216.240, local AS number 1097
BGP table version is 13, main routing table version 13
2 network entries using 336 bytes of memory
2 path entries using 208 bytes of memory
2/2 BGP path/bestpath attribute entries using 272 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 816 total bytes of memory
BGP activity 12/8 prefixes, 19/14 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ    Up/Down  State/PfxRcd
2001::2         4           1097 3180 3183       13    0    0   2d00h
```

dev-7604_lwggw016#exit
CLI commands for BGP IPv6 discovery and monitoring of Juniper devices

**Command**

show bgp summary

**Sample output**

<table>
<thead>
<tr>
<th>Table</th>
<th>Tot Paths</th>
<th>Act Paths</th>
<th>Suppressed</th>
<th>History</th>
<th>Damp</th>
<th>State</th>
<th>Pending</th>
</tr>
</thead>
<tbody>
<tr>
<td>inet.0</td>
<td>79</td>
<td>39</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>bgp.13vpn.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>inet6.0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>bgp.12vpn.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>inet.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Peer</th>
<th>AS</th>
<th>InPkt</th>
<th>OutPkt</th>
<th>OutQ</th>
<th>Flaps</th>
<th>Last Up/Dwn</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.4.1</td>
<td>1097</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7w6d9h Active</td>
</tr>
<tr>
<td>192.168.7.1</td>
<td>1097</td>
<td>131344</td>
<td>146791</td>
<td>0</td>
<td>1</td>
<td>6w4d16h Establ</td>
</tr>
<tr>
<td>192.168.8.1</td>
<td>1971</td>
<td>2197</td>
<td>0</td>
<td>5</td>
<td>16:44:53 Establ</td>
<td></td>
</tr>
<tr>
<td>192.168.10.1</td>
<td>8888</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7w6d9h Active</td>
</tr>
<tr>
<td>192.168.18.1</td>
<td>175922</td>
<td>174285</td>
<td>0</td>
<td>0</td>
<td>7w6d8h Establ</td>
<td></td>
</tr>
<tr>
<td>192.168.77.8</td>
<td>8888</td>
<td>175385</td>
<td>174287</td>
<td>0</td>
<td>0</td>
<td>7w6d9h Establ</td>
</tr>
<tr>
<td>192.168.77.18</td>
<td>8888</td>
<td>159555</td>
<td>174292</td>
<td>0</td>
<td>0</td>
<td>7w6d9h Establ</td>
</tr>
<tr>
<td>192.168.167.1</td>
<td>1097</td>
<td>131376</td>
<td>146792</td>
<td>0</td>
<td>1</td>
<td>6w4d16h Establ</td>
</tr>
<tr>
<td>2000::2</td>
<td>8888</td>
<td>175538</td>
<td>174078</td>
<td>0</td>
<td>0</td>
<td>7w6d9h Establ</td>
</tr>
<tr>
<td>inet6.0</td>
<td>0/1/1/0</td>
<td>0/1/1/0</td>
<td>0/1/1/0</td>
<td>0/1/1/0</td>
<td>0/1/1/0</td>
<td>0/1/1/0</td>
</tr>
</tbody>
</table>

**Groups:** 3  
**Peers:** 9  
**Down peers:** 2
This appendix describes the SNMP poller used by Network Protocol Manager to obtain status updates for its correlation analysis. It consists of the following sections:

- SNMP polling overview ................................................................. 170
- SNMP poller operation ................................................................. 170
SNMP polling overview

After the initial discovery and modeling of the topology objects for a specific routing protocol, Network Protocol Manager updates the status of the objects by continuously monitoring the devices through either SNMP or CLI polling. The results of the polling, in addition to the status updates extracted from SNMP traps and syslog messages (optional and applicable only to BGP and OSPF) and the status updates received from IP Availability Manager, serve as input to the Network Protocol Manager correlation analysis.

For SNMP polling, Network Protocol Manager uses an IPv4 SNMP poller, which sends SNMPv1, v2c, or v3 messages for use with IP version 4. Table 35 on page 170 identifies the Network Protocol Manager authentication and privacy protocol support for SNMPv3.

<table>
<thead>
<tr>
<th>Operation</th>
<th>AuthProtocol</th>
<th>PrivProtocol</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AuthProtocol</td>
<td>PrivProtocol</td>
</tr>
<tr>
<td></td>
<td>MD5</td>
<td>SHA-1</td>
</tr>
<tr>
<td>Discovery/monitoring</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

SNMP poller operation

The SNMP poller is a synchronous, multithreaded poller that currently uses ten synchronous polling threads.

The SNMP poller fully supports the SNMPv1 and v2c protocols, and supports authentication and data encryption for the SNMPv3 protocol. With SNMPv1, the correlation model uses 32-bit counters in its correlation analysis. With SNMPv2c or v3, the correlation model uses high-capacity 64-bit counters in its correlation analysis. Using 64-bit counters is critical for performance analysis of high-speed data links because using 32-bit counters might result in wrapping (overflow) of the counters between polls.

Polling for devices with multiple IP addresses is supported because the SNMP poller supports multiple IP addresses for each SNMP agent. The SNMP poller automatically switches to an alternate IP address during failures, thereby ensuring the integrity of the Network Protocol Manager correlation analysis during an outage.

Just-in-time polling

The SNMP poller’s MIB variable poll list is driven by a Just-In-Time polling algorithm, which ensures that only those MIB variables needed for correlation are polled. For example, if a port monitored for performance data is disabled, or goes down, the SNMP poller automatically removes the relevant MIB variables from the poll list. If the port is reenabled, or comes back up, the variables are automatically put back onto the MIB poll list.
Request-consolidation polling

Issuing a single SNMP GET request that requests 10 variables is more efficient than issuing 10 GET requests each requesting a single variable. The SNMP poller consolidates as many variables as possible into a single SNMP GET request. The consolidation is not restricted to variables from the same SNMP table. Polling consolidation continually adapts to changes in the MIB variable poll list.

Upon encountering a non-fatal error during polling consolidation, the SNMP poller responds differently to an SNMPv1 agent than to an SNMPv2c or v3 agent for the following reason: Where an SNMPv1 agent stops processing a request upon encountering an error, an SNMPv2c or v3 agent continues processing a request upon encountering an error. An SNMPv2c or v3 agent handles errors on a per-OID basis.

If a non-fatal error is encountered by an SNMPv1 agent during a GET request that is seeking multiple variables, the SNMP poller suspends the polling of the affected variable because continuing to poll that variable would require the resending of the remainder of the request after receiving the error. An example of an affected variable is one that has become unavailable due to a configuration change. Of course, the SNMP poller continues to poll the unaffected variables. This behavior enables the SNMP poller to operate efficiently with an SNMPv1 agent during unexpected changes to a device's configuration.

In contrast, if a non-fatal error is encountered by an SNMPv2c or v3 agent during a GET request that is seeking multiple variables, the SNMP poller continues the polling of the affected variable as well as the unaffected variables.
APPENDIX F
NPM dump instrumentation utility

This appendix describes the Network Protocol Manager dump instrumentation utility used for troubleshooting. It consists of the following sections:

- Network Protocol Manager dump instrumentation utility ........................................ 174
- Invoking the NPM dump instrumentation utility .................................................... 174
Network Protocol Manager dump instrumentation utility

The Network Protocol Manager dump instrumentation utility is a tool that can provide useful event information for troubleshooting by EMC Support.

**NOTICE**

You must send both the output file plus the repository file (for example, bgp.rps) in order for EMC Support to troubleshoot the problem.

Table 36 on page 174 provides a list of scripts that write the instrumented values to an output file.

**Table 36 NPM dump instrumentation utility scripts**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ic_dumpinst_bgp.asl</td>
<td>Writes the instrumented attribute values for BGP objects to an output file.</td>
</tr>
<tr>
<td>ic_dumpinst_eigrp.asl</td>
<td>Writes the instrumented attribute values for EIGRP objects to an output file.</td>
</tr>
<tr>
<td>ic_dumpinst_isis.asl</td>
<td>Writes the instrumented attribute values for IS-IS objects to an output file.</td>
</tr>
<tr>
<td>ic_dumpinst_ospf.asl</td>
<td>Writes the instrumented attribute values for OSPF objects to an output file.</td>
</tr>
</tbody>
</table>

Invoking the NPM dump instrumentation utility

The following are sample commands to run the utility.

The utility connects to the Network Protocol Manager and writes the instrumentation attribute values for objects to an output file that is created in the `<BASEDIR>/smarts/local/log` directory.

**BGP instrumentation utility command**

The command to write the instrumented values is:

```
sm_adapter --output=<LOG_FILE> --server=<BGP-DOMAIN-MANAGER> utils/ic_dumpinst_bgp.asl
```

where:

- `<BGP-DOMAIN-MANAGER>` is the name of the Network Protocol Manager for BGP.
- `<LOG_FILE>` is the name of log file.

**EIGRP instrumentation utility command**

The command to write the instrumented values is:

```
sm_adapter --output=<LOG_FILE> --server=<EIGRP-DOMAIN-MANAGER> utils/ic_dumpinst_eigrp.asl
```

where:

- `<EIGRP-DOMAIN-MANAGER>` is the name of the Network Protocol Manager for EIGRP.
◆  `<LOG_FILE>` is the name of log file.

IS-IS instrumentation utility command

The command to write the instrumented values is:

```bash
sm_adapter --output=<LOG_FILE> --server=<IS-IS-DOMAIN-MANAGER> utils/ic_dumpinst_isis.asl
```

where:

◆  `<IS-IS-DOMAIN-MANAGER>` is the name of the Network Protocol Manager for IS-IS.

◆  `<LOG_FILE>` is the name of log file.

OSPF instrumentation utility command

The command to write the instrumented values is:

```bash
sm_adapter --output=<LOG_FILE> --server=<OSPF-DOMAIN-MANAGER> utils/ic_dumpinst_ospf.asl
```

where:

◆  `<OSPF-DOMAIN-MANAGER>` is the name of the Network Protocol Manager for OSPF.

◆  `<LOG_FILE>` is the name of log file.
NPM dump instrumentation utility
INDEX

A
AccessProtocol 54
Adapter for Alcatel-Lucent 5620 SAM EMS 131, 133, 135
5620 polling groups 127
IsDisplayNameCustom 34
Adapter Platform
  Configuration tasks 20
  Overview 17
Adapters 34, 127, 131, 133, 135
Adding or removing matching criteria 118
AdminDownFlag parameter 28, 30, 31, 34
AllowedAuthentications option 109
AnalysisMode
  BGP External Setting 129
  BGP SNMP Setting 128
  EIGRP CLI Setting 130
  ISIS CISCO CLI Setting 132
  OSPF External Setting 135
  OSPF SNMP Setting 134
Architecture, Network Protocol Manager 13
Authentication
  Host-based 102
  Password 102
  Public-key 102

B
BGP External Setting 128
  AnalysisMode 129
  PeerState 129
BGP light discovery 29
BGP maps
  Enabling 75
BGP polling group 126, 127
BGP Protocol Endpoints threshold group 137
BGP Session Flapping threshold setting 137
  FLAP_Clear_Window 130
  Trap_Count_Threshold 130
  Trap_Time_Window 130
BGP SNMP Setting 127
  AnalysisMode 128
  PollingInterval 128
  Retries 128
  Timeout 128
bgp.conf file 23, 25, 27
  SyslogName 26
  TrapPort 26, 27
Broker
  Overview 18

C
Changing matching criteria 118
Changing priority of a group 117
Changing setting parameters 116
Cisco Devices polling group 126, 131
CLI
  Discovery 17
  Polls 17, 124, 170
CLI Access Setting
  AccessProtocol 54
  LoginID 54
  Password 54
  PrivilegedModePassword 54
  Timeout 54
CLI commands
  show clns neighbors detail 132, 166
  show ip eigrp neighbors 130, 166
CLI modules
  DASL CLI module 102
  Perl CLI module 102
Config parameter 27, 30, 31, 33
Configuration files
  bgp.conf 23, 27
  eigrp.conf 23, 30
  isis.conf 23, 31
  ospf.conf 23, 33
  trapd.conf 81, 85
Configuration roadmap 18
Configuring syslog message forwarding 97
Consoles
  Polling and Thresholds Console 112
Copying a group 119
Creating a group 119

D
DASL CLI module 102
Device
  Definition of 12
Device Access tab 113
Device support
  MSFCs 47
  Physical routers 47
  RSFCs 47
  RSMs 47
  Virtual routers 47
Discovery
  bgp.conf 27
  eigrp.conf 30
  isis.conf 31
  Light 29
  ospf.conf 33
  perl-cli.conf 104, 106
  Route Reflectors 28
Seed file
  Creating 88
  SNMP and CLI 17
Domain Manager
  Definition of 12
Index

E
EIGRP CLI Setting 130
  AnalysisMode 130
  PollingInterval 130
  Retries 130
  Timeout 131
EIGRP EXTERNAL Setting 131
  eigrpPeerAdminStatus 131
  PeerState 131
EIGRP maps
  Enabling 75
EIGRP polling group 126, 130
  eigrp.conf file 23, 25, 30
  eigrpPeerAdminStatus
    EIGRP EXTERNAL Setting 131
EnableAlertsOnDynamicOSPFLinks 34
EnablePeriodicLiteSynchronization 29
EnableRReconfigureLaunchedLiteSynchronization 29
EnableRReDiscovery parameter 28
Enabling maps 75
  Console Operations 75
  Global Manager Administration Console 75
  User Profiles 75

F
FLAP_Clear_Window 138
FORWARD entries 86, 87

G
Global Console
  Overview 18, 39
  Overview discussion 38
  Polling and Thresholds Console 113
  Polling, Thresholds, and Device Access 38
  Type of
    Domain Manager Administration 38
    Global Manager Administration 38
    Topology Browser Console 64
Global Manager 17
  Configuration tasks 19
  Enabling maps 75
  Overview 17
Global Manager Administration Console 58, 61, 62, 91
Group
  Changing priority 117
  Copying 119
  Creating 119
  Definition of 114
  Polling 126
    BGP 126, 127
    Cisco Devices 126, 131
    EIGRP 126, 130
    Juniper Devices 126, 133
    OSPF 126, 134
  Properties 115
  Threshold 137
    BGP Protocol Endpoints 137

H
Host-based authentication 102

I
ic_dumpinst_bgp.asl 174
ic_dumpinst_eigrp.asl 174
ic_dumpinst_isis.asl 174
ic_dumpinst_ospf.asl 174
Importing
  Topology information 10
  Topology objects 91
InitialAdminStatus
  OSPF External Setting 135
InitialIfState
  OSPF External Setting 135
InitialMulticastIfState
  OSPF External Setting 135
InitialNeighborState
  OSPF External Setting 136
InitialNonMulticastIfState
  OSPF External Setting 136
InitialVirtualNeighborState
  OSPF External Setting 136
InitialVirtualState
  OSPF External Setting 136
IP Availability Manager
  Configuration tasks 19
  Overview 16
IP tagging feature 49
IsDisplayNameCustom parameter 28, 34
ISIS CISCO CLI Setting 132
  AnalysisMode 132
  PollingInterval 132
  Retries 132
  Timeout 132
ISIS EXTERNAL Setting 133, 134
  NeighborState 133
ISIS JUNIPER SNMP Setting 133
IS-IS maps
  Enabling 75
  isis.conf file 23, 25, 31

J
Juniper Devices polling group 126, 133

L
LiteSynchronizationInterval 29
LoginID 54

M
Matching
  Pattern 140
Matching criteria
    Adding or removing 118
    Changing 118
N
Neighbor Down alarm
  Control 34
NeighborState
  ISIS EXTERNAL Setting 133
Network Protocol Manager
  Configuration tasks 18
  Overview 16
  Polling 170
  Repository file 25, 26
Network Protocol Manager architecture 13
NPM dump instrumentation utility 174

O
Object
  Definition of 12
  Tagged IP 48
Operator
  Wildcard 140
OSPF External Setting 135
  AnalysisMode 135
  InitialAdminStatus 135
  InitialIfState 135
  InitialMulticastIfState 135
  InitialNeighborState 136
  InitialNonMulticastIfState 136
  InitialVirtualNeighborState 136
  InitialVirtualState 136
OSPF maps
  Enabling 75
OSPF polling group 126, 134
OSPF SNMP Setting 134
  AnalysisMode 134
  PollingInterval 134
  Retries 134
  Timeout 135
ospf.conf file 23, 25, 33
  TrapPort 33

P
Parameter
  Override 25
Password 54
  Password authentication 102
  PasswordAuthentication option 109
Pattern 140
  Pattern matching 140
PeerState
  BGP External Setting 129
  EIGRP EXTERNAL Setting 131
Perl CLI module 102
perl-cli.conf 104, 106
Polling
  CLI 124, 170
  Groups 127, 130, 131, 134
  SNMP 124, 170
  SNMP and CLI 17
Polling and Thresholds Console 112
  Device Access tab 113
  Layout 113
  Polling tab 112
  Tagging tab 113
  Thresholds tab 113
  Toolbar buttons 113
Priority
  Changing 117
PrivilegedModePassword 54
  PrivLevel parameter 30, 32
  ProhibitPrivLevelCLILogon parameter 30, 31
  Public-key authentication 102

R
Removing or adding matching criteria 118
Repository
  Location 25, 26
  Restoring default values of a setting 117
Retries
  BGP SNMP Setting 128
  EIGRP CLI Setting 130
  ISIS CISCO CLI Setting 132
  OSPF SNMP Setting 134

S
Security 36
  clientConnect.conf 36
  Secure communications 36
  serverConnect.conf 36
  SSH security 99
Seed file 88
  Creating 88
Service Assurance Manager
  See Global Manager
Setting
  Changing parameters 116
  Definition of 114
  Restoring default values 117
show clns neighbors detail 132, 166
show ip eigrp neighbors 130, 166
sm_service install command 92
sm_service start command 93
SNMP
  BGP traps
    List of 146
  Cisco configuration traps
    List of 147, 154
  Discovery 17
  Instrumentation BGP4 MIB objects
    List of 144
  Instrumentation IS-IS MIB objects
    List of 155, 156, 157
  Instrumentation OSPF MIB objects
    List of 147, 148
OSPF traps
  List of 153
Polling 170
Polls 17, 124, 170
Trap
  bgpEstablished 137
Trap messages 79
TrapPort 26, 27, 33
SNMP Trap Adapter 79
  Editing the trapd.conf File 85
SNMP trap and syslog processing 147, 155
SSH options
  AllowedAuthentications 109
  PasswordAuthentication 109
Starting syslog message forwarding 97
Syslog
  Message format 160
  Sample messages 160
  Syslog messages 97
  SyslogName 26
Syslog adapter, built-in 97
Syslog message forwarding
  Configuring 97
  Starting 97
SyslogName 26
SyslogName parameter 27, 33
System
  Definition of 12

T
Tagged IP objects 40
Tagging tab 113
Threshold
  Groups 137
Thresholds tab 113
Timeout 54
  BGP SNMP Setting 128
  EIGRP CLI Setting 131
  ISIS CISCO CLI Setting 132
  OSPF SNMP Setting 135
Topology
  File location 25, 26
Topology Browser 64
Topology Browser Console 40
Topology Importer 18
TraceSyslog parameter 27, 33
TraceTraps parameter 27, 33
Trap
  Authentication 80
  Decryption 80
  PORT parameter 81
  Processing 79
  SNMP messages 79
  SNMP Trap Adapter 79
  Translation of incoming 80
  Versions 80
Trap exploder 79
  Creating a service for 92
  Starting a service for 93
Trap receiver 81

Trap receiver, built-in 79
  Trap_Count_Threshold 138
  Trap_Time_Window 138
  trapd.conf file 85
    FORWARD entries 86, 87
  TrapPort 26, 27, 33
  Traps required for IP Availability Manager 87
  Traps required for Network Protocol Manager for BGP 86
  Traps required for Network Protocol Manager for OSPF 87
  Traps selected for the trap receiver 88
Troubleshooting
  NPM dump instrumentation 174

U
User Profiles
  Configure 75

W
Wildcard 140
  Chart of operators 140