EMC® Smarts® IP Performance Manager and Server Performance Manager

Version 7.0

User's Guide

P/N 300-004-089
REV A02

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Copyright ©1996–2007 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com

All other trademarks used herein are the property of their respective owners.

Contents

Preface vii

Chapter 1 Introduction

Important terminology 1-2
What do system and device mean? 1-2
What does modeled topology mean? 1-2
What does object mean? 1-2
About IP Performance Manager 1-3
Performance monitoring 1-3
Performance analysis 1-3
Performance notifications 1-4

Chapter 2 Viewing Analysis Results and Network Topology

Before you start 2-2
Attaching the Global Console to the Global Manager 2-3
Network notifications 2-5
Viewing network notifications 2-5
Opening a Notification Properties dialog box 2-5
Viewing impacts 2-9
Viewing details 2-9
Network topology 2-12
Viewing network topology in maps 2-13
Opening a network topology map 2-13
Network topology map pop-up menus 2-14
Network topology map graphical representations 2-14
Network topology map types 2-17
Physical Connectivity map 2-17
IP Network Connectivity map 2-18
IP Network Membership map 2-18
VLAN Connectivity map 2-18
VLAN Membership map 2-18
Group maps 2-19
Example 1: Displaying a Physical Connectivity map 2-20
Example 2: Displaying a Group IPNetwork Connectivity map 2-21
Network containment 2-22
Opening a network containment dialog box 2-22
Viewing network containment 2-23
Network containment tab pages 2-23

Chapter 3 Network Objects and Their Failures

Summary of exceptions, faults, and events 3-2
Exceptions and faults summary 3-2
Events summary 3-4
Network objects, attributes, exceptions, faults, and events 3-5
System 3-6
Attributes for system 3-7
Exceptions for system 3-9
Events for system 3-10
Chassis 3-11
Attributes for Chassis 3-11
Exceptions for Chassis 3-12
Faults for Chassis 3-12
VLAN 3-13
Attributes for VLAN 3-13
Exceptions for VLAN 3-14
Network adapter 3-15
Attributes for network adapter 3-16
Faults for network adapter 3-19
Duplex-mode discovery for network adapters 3-22
Processor 3-25
Attributes for Processor 3-25
Faults for Processor 3-25
Memory 3-26
Attributes for Memory 3-26
Faults for Memory 3-27
Disk 3-28
Attributes for Disk 3-28
Faults for Disk 3-29
FileSystem 3-30
Attributes for FileSystem 3-30
Faults for FileSystem 3-31
PowerSupply 3-32
Attributes for PowerSupply 3-32
Faults for PowerSupply 3-33
VoltageSensor 3-34
Attributes for VoltageSensor 3-34
Faults for VoltageSensor 3-35
TemperatureSensor 3-36
Attributes for TemperatureSensor 3-36
Faults for TemperatureSensor 3-37
Fan 3-38
Attributes for Fan 3-38
Faults for Fan 3-38
DuplicateIP 3-39
Attributes for DuplicateIP 3-39
Events for DuplicateIP 3-42

Appendix A MIBs Polled and SNMP Traps Processed

Standard SNMP MIBs polled A-2
Enterprise MIBs polled A-3
SNMP traps processed A-5
SNMP traps processed for discovery A-5
SNMP traps processed for analysis A-6

Appendix B Network Topology Naming Conventions

DisplayName and Name attributes B-2
Naming convention for network objects B-3

Appendix C Exception, Fault, Event, and Notification Summary

Exceptions C-2
Faults and events C-3
Notifications C-4

Index i-1

Preface

This document provides detailed information about EMC Smarts IP Performance Manager (IP Performance Manager) and the EMC Smarts IP Server Performance Manager (IP Server Performance Manager). Both applications monitor the performance of network objects, analyze the performance data, and send the results of their analysis to the EMC Smarts Service Assurance Manager (Global Manager). In addition to the standard capabilities of IP Performance Manager, IP Server Performance Manager can also discover and monitor host disks, host filesystems, and additional information about host processors and memory.

Throughout this document, the term "IP Performance Manager" applies to both IP Performance Manager and IP Server Performance Manager. Features or procedures that are unique to IP Server Performance Manager are indicated as such.

Audience for this guide

This document is intended for IT managers seeking to better understand the value of IP Performance Manager, for system administrators configuring and using IP Performance Manager, and for operators receiving and acting upon notifications.

Prerequisites

Before you perform the procedures in this document, the following software must be installed:

- EMC Smarts IP Performance Manager
- EMC Smarts Service Assurance Manager (Global Manager)
- EMC Smarts Global Console

The *EMC Smarts IP Management Suite Installation Guide* and the *EMC Smarts Service Assurance Management Suite Installation Guide* provide information about these products.

It is also assumed that IP Performance Manager has been configured in accordance with the *EMC Smarts IP Management Suite Configuration Guide* and that discovery has been initiated in accordance with the *EMC Smarts IP Management Suite Discovery Guide*.

EMC Smarts IP Management Suite installation directory

In this document, the term BASEDIR represents the location where EMC Smarts software is installed.

- For UNIX, this location is: /opt/InCharge*<n>*/*<productsuite>*.
- For Windows, this location is: C:\InCharge*<n>**<productsuite>*.

The <n> represents the EMC Smarts software platform version number. The <productsuite> represents the EMC Smarts product suite to which the product belongs. For example, on UNIX operating systems, EMC Smarts IP Availability Manager is, by default, installed to: /opt/InCharge7/IP/smarts. On Windows operating systems, this product is, by default, installed to: C:\InCharge7\IP\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 <productsuite> location under the root directory.

For more information about the directory structure of EMC Smarts software, refer to the *EMC Smarts System Administration Guide*.

EMC Smarts IP Management Suite products

The EMC Smarts IP Management Suite includes the following products:

- EMC Smarts IP Availability Manager
- EMC Smarts IP Discovery Manager
- EMC Smarts IP Performance Manager
- EMC Smarts IP Server Performance Manager
- EMC Smarts Adapter for HP OpenView NNM
- EMC Smarts Adapter for IBM/Tivoli NetView

Related documentation

In addition to this document, EMC Corporation provides a Help system for command line programs as well as product documentation.

Help for command line programs

Descriptions of command line programs are available as HTML pages. The index.html file, which provides an index to the various commands, is located in the BASEDIR/smarts/doc/html/usage directory.

EMC Smarts documentation

Readers of this guide may find the following related documentation helpful. It can be found in the BASEDIR/smarts/doc/pdf directory.

Note: These documents are updated periodically. Electronic versions of the updated manuals are available on the Powerlink website: **http://Powerlink.EMC.com**.

- *EMC Smarts Documentation Catalog*
- *EMC Smarts System Administration Guide*
- *EMC Smarts ICIM Reference*
- *EMC Smarts Common Information Model Infrastructure Models Chart*
- *EMC Smarts Common Information Model Application/Business Models Chart*

- *EMC Smarts ASL Reference Guide*
- *EMC Smarts Perl Reference Guide*
- *EMC Smarts Dynamic Modeling Tutorial*
- *EMC Smarts MODEL Reference Guide*

EMC Smarts IP Management Suite documentation

The following EMC Smarts documents are relevant to users of the IP Management product suite:

- *EMC Smarts IP Management Suite Installation Guide*
- *EMC Smarts IP Management Suite Deployment Guide*
- *EMC Smarts IP Management Suite Configuration Guide*
- *EMC Smarts IP Management Suite Discovery Guide*
- *EMC Smarts IP Availability Manager User's Guide*
- *EMC Smarts IP Performance Manager and Server Performance Manager User's Guide*
- *EMC Smarts IP Adapters User's Guide*
- *EMC Smarts IP Availability Manager Extension for IPv6 User's Guide*
- *EMC Smarts IP Availability Manager Extension for NAS User's Guide*
- *EMC Smarts Quick Start Guide*

Refer to the *EMC Smarts Documentation Catalog* for documentation resources provided with other EMC Smarts product suites.

Suggestions for searching PDF files

You may search across multiple PDF files using the Adobe Acrobat Reader software.

1. If the documentation is not accessible to all users of the EMC Smarts product suite, copy the contents of the *BASEDIR/smarts/doc/pdf d*irectory to a central location, such as a shared drive on your LAN, that operators and others may view.
2. To search throughout the documentation library, open the Acrobat Reader software.
   1. Choose **Edit** > **Search**, and enter a word or phrase.
   2. In the **Where would you like to search** option, select **All PDF Documents in** and type the pathname of the location where the PDF documents reside.

If you have more than one EMC Smarts product suite installed, you can set up cross-product document searches by copying files from the BASEDIR/smarts/doc/pdf directory for each product suite into this common documentation directory path.

Conventions used in this guide

EMC uses the following conventions for notes and cautions.

Note: A note presents information that is important, but not hazard-related.

IMPORTANT

An important notice contains information essential to the operation of the software.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

Typographical conventions

EMC uses the following conventions in this guide:

Normal font	In running text: • Interface elements (for example, button names, dialog box names) outside of procedures • Items that the user selects outside of procedures • Java classes and interface names • Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, filenames, functions, menu names, utilities • Pathnames, URLs, filenames, directory names, computer names, links, groups, service keys, file systems, environment variables (for example, command line and text), notifications
Bold	In procedures: • Names of dialog boxes, buttons, icons, menus, fields, and maps • Selections from the user interface, including menu items, and field entries • Key names • Window names • Code examples • Commands • User interface tabs
Italic	Used for: • Full publications titles referenced in text In procedures: • Directory paths • Filenames • Scripts • Important/unique words • URLs • Utilities • Variables
`Courier`	Used for: • System output • User entry
< >	Angle brackets used to enclose parameter or variable values supplied by the user.
[ ]	Square brackets used to indicate optional values.
|	Vertical bar used to indicate alternate selections. The bar means “or”.

{ }	Braces used to indicate content that you must specify (that is, x or y or z).
...	Ellipses used to indicate nonessential information omitted from the example.
%	Used to indicate a C shell prompt.
#	Used to indicate a C shell superuser prompt.
▼▲	Used to indicate a command is wrapped over one or more lines. The command must be typed as one line.

Pathname conventions

Directory pathnames are shown with forward slashes (/). Users of the Windows operating systems should substitute back slashes (\) for forward slashes.

Graphical conventions

If there are figures illustrating consoles in this document, they represent the consoles as they appear in Windows. Under UNIX, the consoles appear with slight differences. For example, in views that display items in a tree hierarchy such as the Topology Browser, a plus sign displays for Windows and an open circle displays for UNIX.

Smarts Manager

Unless otherwise specified, the term Smarts Manager is used to refer to EMC Smarts programs such as Domain Managers, Global Managers, and adapters.

Where to get help

EMC support, product, and licensing information can be obtained as follows.

Product information — For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Powerlink™ website (registration required) at:

http://Powerlink.EMC.com

Technical support — For technical support, go to EMC Customer Service on Powerlink. To open a service request through Powerlink, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Sales and customer service contacts — For the list of EMC sales locations, please access the EMC home page at:

http://EMC.com/contact

1

Introduction

This chapter describes the concepts of managing network performance using EMC® Smarts® IP Performance Manager. It consists of the following sections:

- Important terminology 1-2
- About IP Performance Manager 1-3
- Performance monitoring 1-3
- Performance analysis 1-3
- Performance notifications 1-4

Important terminology

EMC Smarts IP Performance Manager (IP Performance Manager) is an EMC Smarts Domain Manager, where a Domain Manager is a service-assurance application associated with a particular type of information-technology domain (networks, systems, applications, application services). For IP Performance Manager, the domain is IP network transport performance. Each Domain Manager is autonomous in the sense that it maintains its own data models, repository, and problem signatures, and monitors and analyzes the discovered objects in its own domain.

EMC Smarts IP Server Performance Manager (IP Server Performance Manager) is an enhanced version of IP Performance Manager and is available through a feature license. In addition to the standard capabilities of IP Performance Manager, IP Server Performance Manager can also discover and monitor host disks, host filesystems, and additional information about host processors and memory.

Throughout this document, the term "IP Performance Manager" applies to both IP Performance Manager and IP Server Performance Manager. Features or procedures that are unique to IP Server Performance Manager are indicated as such.

What do system and device mean?

The term "system," as used in this document, is a generic term representing a computer-based network entity, such as a switch, router, hub, bridge, or host. The term "device," as used in this document, has essentially the same meaning as system except that "device" also conveys a sense of specific model, such as a specific model of switch, router, hub, bridge, or host.

What does modeled topology mean?

IP Performance Manager uses EMC Smarts ICIM class models to create (within its repository) instances of the managed network systems (switches, routers, hubs, bridges, hosts), their dependencies, their internal components, and their connections. The "modeled topology" mirrors the real topology in the managed network.

What does object mean?

The term "object," as used in this document, is intended to have a dual meaning: To simultaneously represent both an instance (ICIM object) in the modeled topology and an instance (network entity) in the real topology. The ICIM object corresponds to the network entity.

About IP Performance Manager

Knowing the health of the network objects in your network is crucial to ensuring optimum network performance. Constant monitoring, especially of critical ports in the network, is necessary to detect when faults are occurring so that you can take appropriate corrective action.

IP Performance Manager monitors the performance of Layer 2 and Layer 3 network objects in switched and routed networks, and automates the analysis of faults using performance thresholds. Faults can occur in systems (switches, routers, hubs, bridges, hosts) and in network adapters (ports, interfaces). When a performance threshold is exceeded, IP Performance Manager generates a system-level exception notification.

For example, when a particular network adapter exceeds the ErrorThreshold, IP Performance Manager detects a HighErrorRate fault and generates an ErrorException for the system that contains the network adapter. In addition, if the network adapter is a member of a Virtual Local Area Network (VLAN), IP Performance Manager also generates the exception notification at the VLAN level.

Performance monitoring

After the initial discovery and modeling of the network, IP Performance Manager continuously monitors the status of the discovered systems using:

- Internet Control Message Protocol (ICMP) polling
- Simple Network Management Protocol (SNMP) polling

IP Performance Manager also processes SNMP trap messages received from the network to obtain status information for the discovered systems.

Appendix A, “MIBs Polled and SNMP Traps Processed,” provides information about the MIBs polled and SNMP traps processed by IP Performance Manager.

Performance analysis

IP Performance Manager retrieves fault-related, intra-system information from each network object and uses that information to conduct performance analysis.

Performance notifications

IP Performance Manager exports the results of its network performance analysis to the Global Manager in the form of notifications, which are displayed in the Notification Log Console view of the Global Console. The notifications identify IP Performance Manager by its domain name in the Source attribute. Users can double-click a notification to view detailed information about the notification.

IP Performance Manager creates three types of notifications: faults, events, and exceptions. Exceptions are also referred to as aggregate events.

- A fault indicates a performance problem detected by IP Performance Manager. Examples of faults are:
  - High error rate for a network adapter
  - High utilization of a switch's backplane
  - High buffer miss rate on a system's memory component
- An event indicates an abnormal condition detected by IP Performance Manager.
- An exception indicates that one or more faults are occurring in a particular system or VLAN.

Chapter 2, "Viewing Analysis Results and Network Topology," provides information about viewing the notifications, and Chapter 3, "Network Objects and Their Failures," provides descriptions and examples of the types of faults detected by IP Performance Manager.

2

Viewing Analysis Results and Network Topology

This chapter describes how to use the Global Console to view network notifications, topology maps, and containment information for IP Performance Manager. It consists of the following sections:

- Before you start 2-2
- Attaching the Global Console to the Global Manager 2-3
- Network notifications 2-5
- Network topology 2-12
- Network containment 2-22

Before you start

Chapter 3, "Network Objects and Their Failures," identifies the topology objects discovered and the events notified by IP Performance Manager.

Also, be aware that the console operations described in this chapter are controlled by certain console operation options such as Notification Properties, Expand Map Node, and Show Containment. The *EMC Smarts Service Assurance Manager Configuration Guide* provides instructions on changing the console operations.

Attaching the Global Console to the Global Manager

To attach the Global Console to the EMC Smarts Service Assurance Manager (Global Manager):

1. Start the Global Console.
   - On a Windows system, select **Start > Programs > InCharge 7> EMC Smarts Global Console**.
   - On a UNIX system, go to the *BASEDIR/smarts/bin* directory in the EMC Smarts Service Assurance Manager (Global Manager) installation area and enter **sm_gui**.

   The **Attach Manager** dialog box opens, an example of which is shown in Figure 2-1.

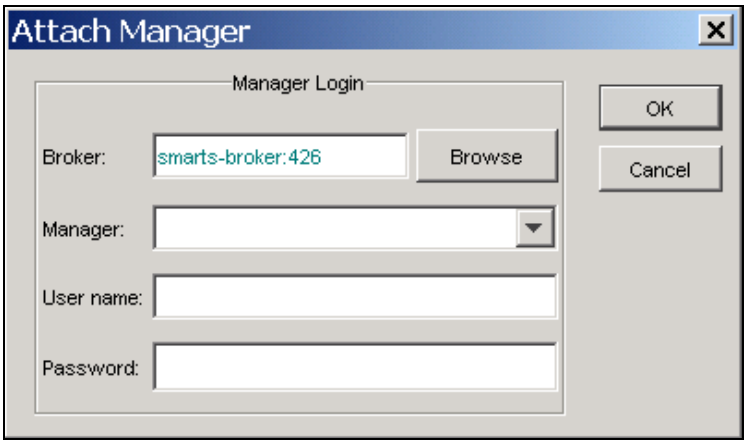

Figure 2-1 Attach Manager dialog box

2. In the dialog box,
   - Ensure that the EMC Smarts Broker for your deployment appears in the **Broker** text box.
   - Click the **Manager** drop-down list or the **Browse** button to display a list of active (running) Smarts Managers, and from that list select the Global Manager application (for example, INCHARGE-SA) in your deployment as the Smarts Manager to which you want to connect.
   - Enter your login username and password. (The default operator account is user name *oper* and password *oper*, and the default administration account is user name *admin* and password *changeme*.)
   - Click **OK**.

The **Notification Log Console** view of the Global Console opens, an example of which is shown in Figure 2-2. In the example display, the **Notification Log Console** is attached to a Global Manager application named INCHARGE-SA.

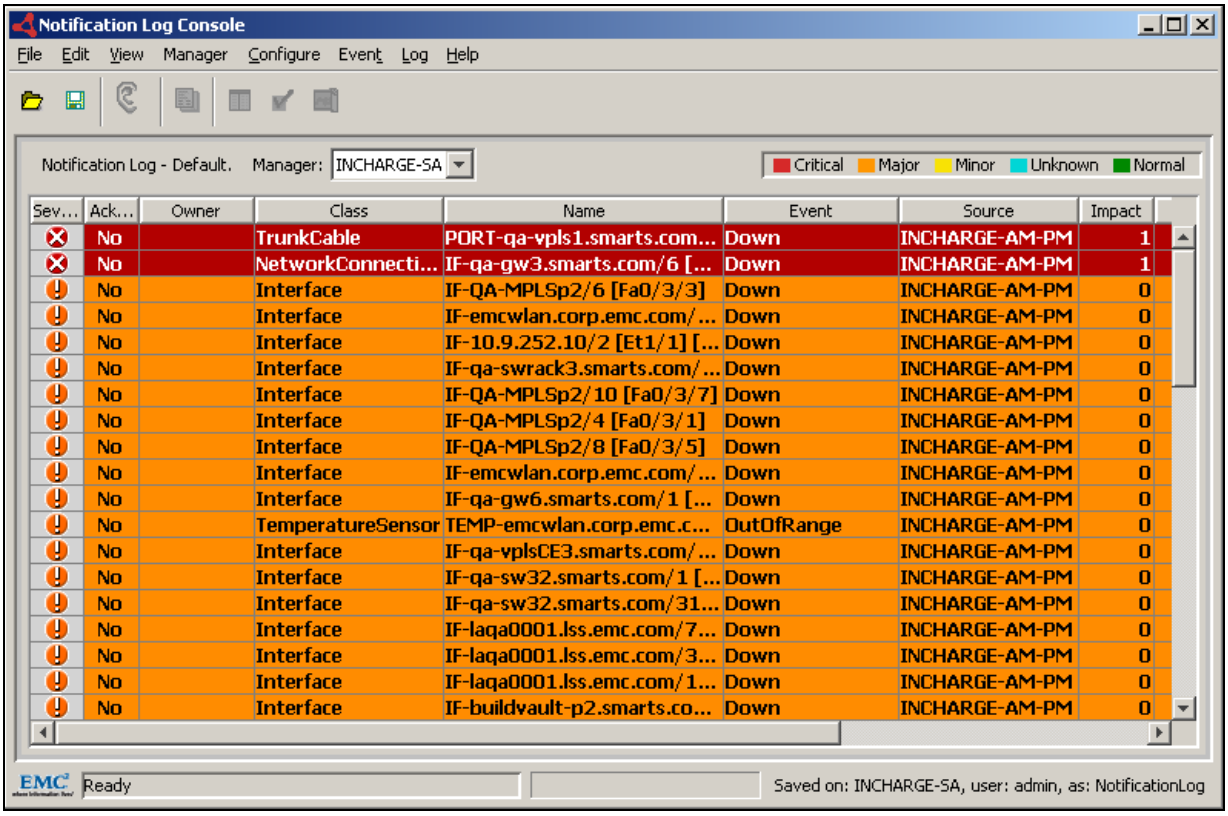

Figure 2-2 Notification Log Console—example

The Notification Log Console shown in Figure 2-2 is one of many console views composing the Global Console. One other console view of particular interest to the discussions that follow is the Map Console, which graphically represents topology in a map format.

The *EMC Smarts Service Assurance Manager Operator's Guide* provides detailed information on using the Global Console.

Network notifications

IP Performance Manager passes the results of its analysis in the form of notifications to the Global Manager. The Global Manager, in turn, passes the notifications to the Global Console, where they are presented in a tabular form in the Notification Log Console.

Each notification consists of a set of attributes that describe properties of the notification, such as Class, Name, Event, Source, and Impact. The value in the Name attribute is the display name of the notification; Appendix B, "Network Topology Naming Conventions," describes the naming formats used to create network object names. The numeric value for the Impact attribute indicates the effect of this notification on other objects in the managed network; the larger the numeric value, the larger the effect.

The severity of a notification is reflected by its color, where red indicates the highest severity level.

Viewing network notifications

You can view the notifications through the Global Console in two basic ways:

- As tabular entries in a Notification Log Console view

  Included with the Notification Log Console view (or any other view where you can see notifications) is a Notification Properties dialog box for viewing detailed information about an individual notification.

- As color-coded severity bar icons in a Map Console view

  In a map, a color-coded severity bar icon appears underneath nodes (graphical representations of topology objects) that are affected by abnormal conditions denoted in notifications.

Opening a Notification Properties dialog box

To obtain detailed information about an individual network notification, you can use any of the following common methods to open the Notification Properties dialog box:

- Double-click a network notification in the Notification Log Console.
- Select a network notification in the Notification Log Console and then click the Show Notification Properties toolbar button.
- Right-click a selected network notification and then select Properties in the pop-up menu.
- Double-click an IP Performance Manager map icon (in the Map Console) affected by active events.

Figure 2-3 is an example of a Notification Properties dialog box showing detailed information for a Processor HighUtilization fault event.

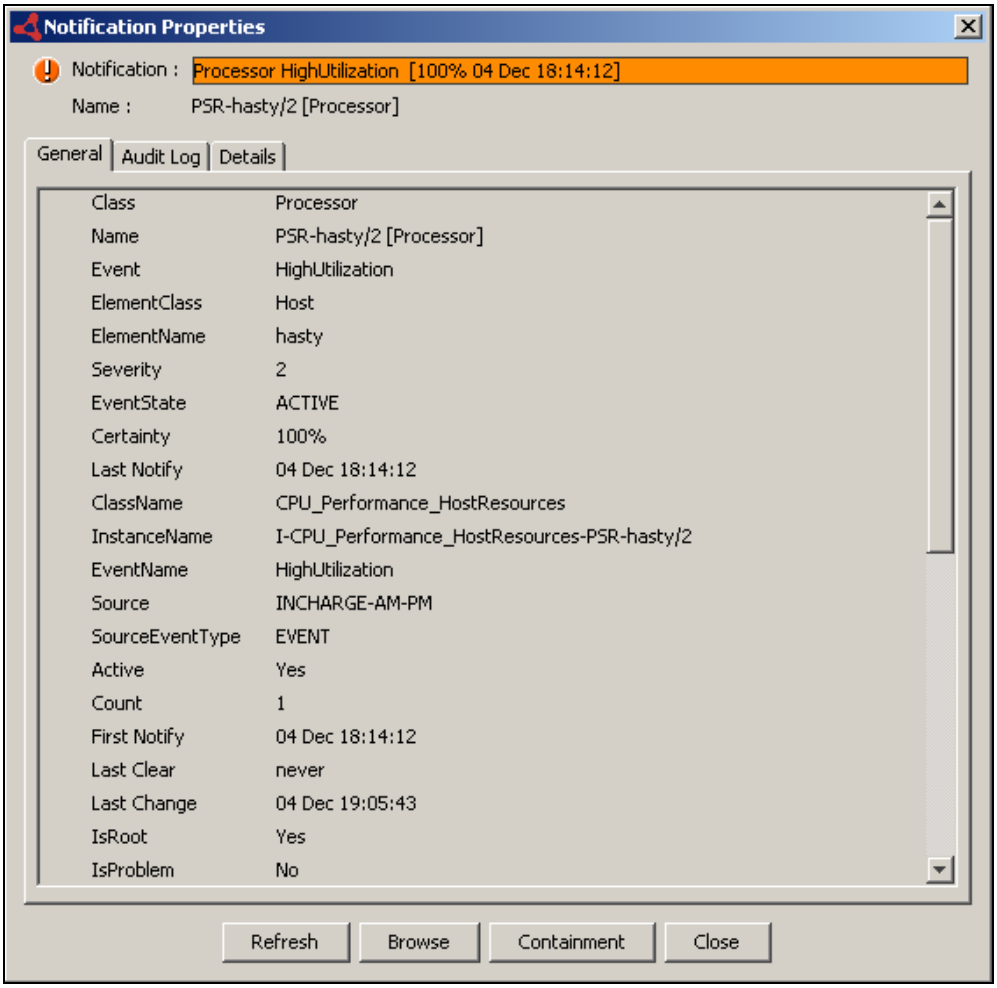

Figure 2-3 Notification Properties dialog box showing a Processor HighUtilization fault

Figure 2-4 is an example of a Notification Properties dialog box showing detailed information for a Memory InsufficientFreeMemory fault event.

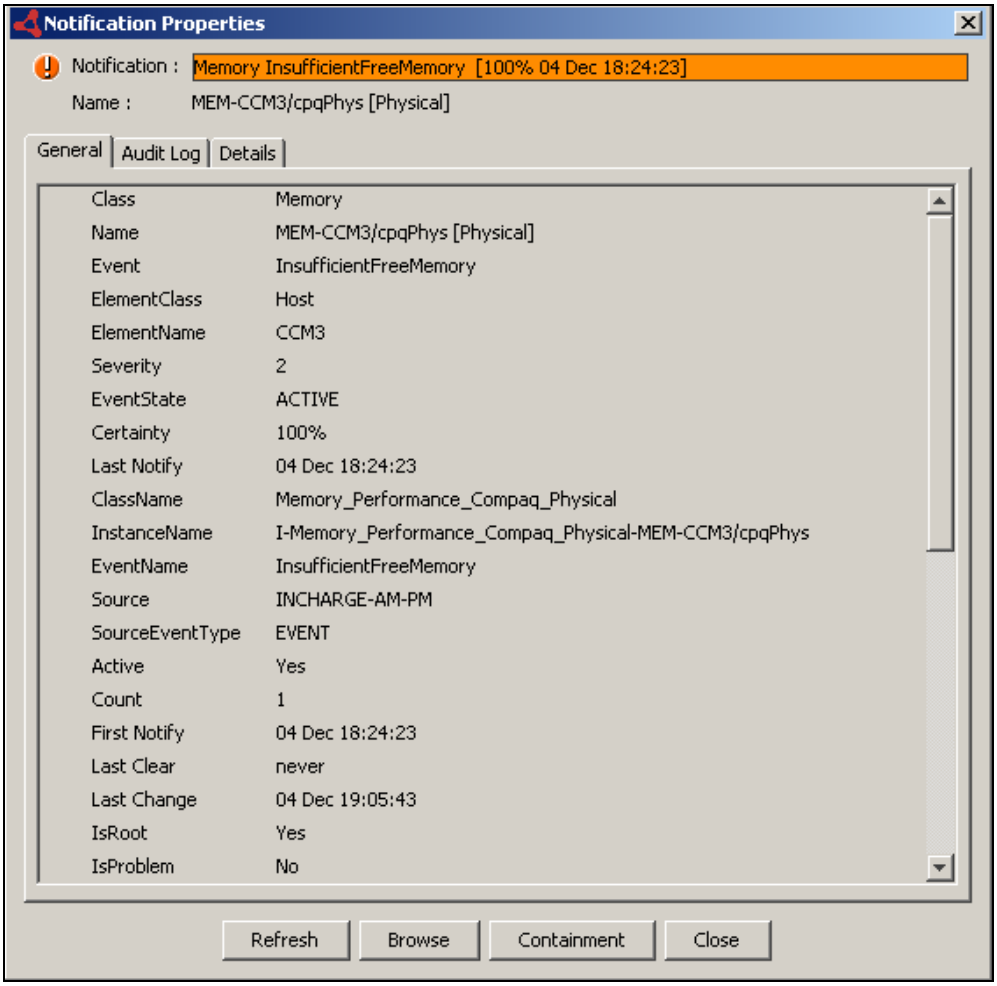

Figure 2-4 Notification Properties dialog box showing a Memory InsufficientFreeMemory fault

Figure 2-5 is an example of a Notification Properties dialog box showing detailed information for a TemperatureSensor OutOfRange fault event.

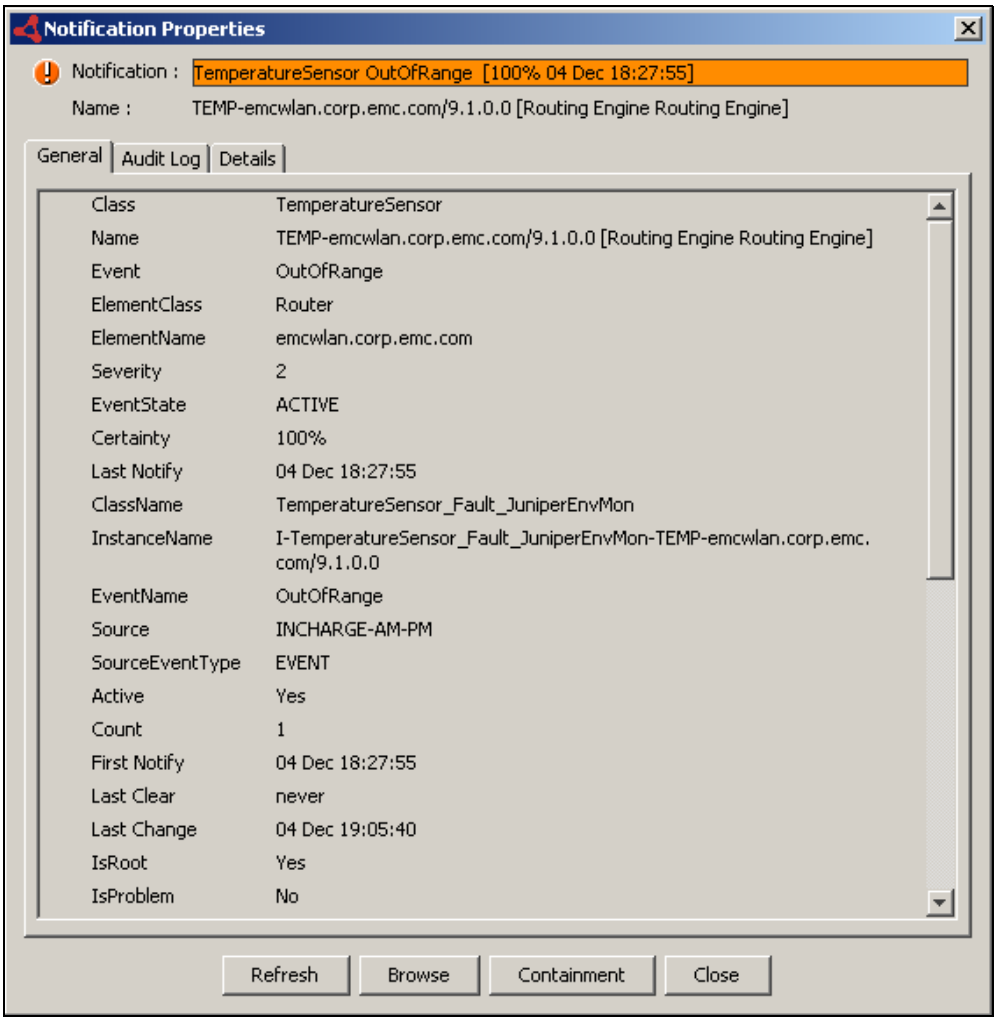

Figure 2-5 Notification Properties dialog box showing a TemperatureSensor OutOfRange fault

in Figure 2-3, Figure 2-4, and Figure 2-5, attribute IsRoot set to Yes indicates that the faults are root causes, and attribute IsProblem set to No indicates that the root causes were not diagnosed by IP Performance Manager using event-correlation analysis. Table 2-1 shows the three possible value combinations for these two attributes and what the combinations mean.

Table 2-1 **Possible value combinations for IsProblem and IsRoot attributes**

IsProblem Value	IsRoot Value	Meaning
Yes	Yes	Indicates that this notification is a root-cause problem diagnosed by an underlying Domain Manager using event-correlation analysis. **Note:** Does not apply to IP Performance Manager.
No	Yes	Indicates that this notification is an event computed by an underlying Domain Manager when a certain polled metric equals or exceeds a threshold. The event is a root cause unto itself.
No	No	Indicates that this notification is either an impact event generated by an underlying Domain Manager or an informational event originating from the managed network and forwarded by the underlying Domain Manager to the Global Manager. **Note:** Does not apply to IP Performance Manager.

By default, the IsProblem and IsRoot attributes columns do not display in the Notification Log Console. To add the IsProblem attribute column, right-click an attribute column heading (for example, Class) in the Notification Log Console, select Insert Column in the pop-up menu, and then select IsProblem in the submenu; the IsProblem column is inserted to the left of the selected column. Repeat this procedure to add the IsRoot attribute column.

Viewing impacts

You view the impacts for a network problem notification by clicking the Impact tab in the Notification Properties dialog box. The Impact tab lists all of the affected objects for the notification.

Because IP Performance Manager does not diagnose root-cause problems, it does not diagnose impacts. Therefore, the Notification Properties dialog box for notifications generated by IP Performance Manager does not contain the Impact tab.

Viewing details

You view the details for a network notification by clicking the Details tab in the Notification Properties dialog box. The Details tab identifies the Domain Manager source of the notification and the notification's attributes and corresponding values. If a notification has multiple sources, one Details tab appears for each source.

Figure 2-6 lists the details for a Host DiscoveryError notification.

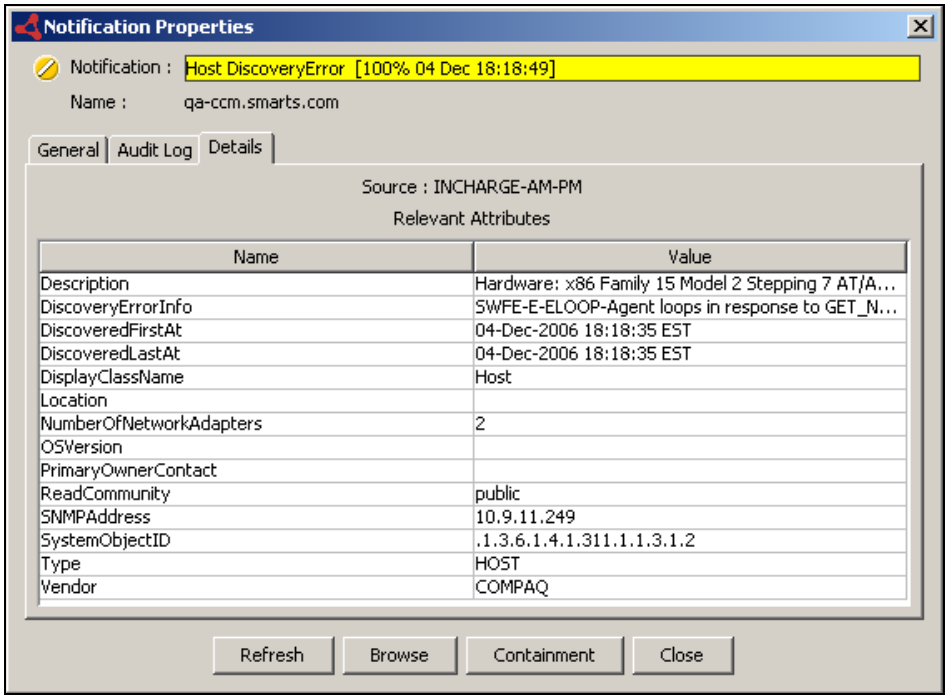

Figure 2-6 Notification Properties dialog box showing the details for a Host DiscoveryError event

The Details tab presents information as a table of attributes and values, or as a table of thresholds and their related attributes and values, or as a sum or total value with a table of other attributes compared against a threshold value. For system notifications (Figure 2-6, for example), the Details tab presents the information as a table of attributes and values.

Procedure to hide the read community string in the Details tab

For a system notification, the SM_HIDEREADCOMM environment variable controls whether to hide or show the read community string in the Details tab of the Notification Properties dialog box.

- A value of TRUE or 1 hides the read community string.
- A value of FALSE or 0 shows the read community string.

Note: Values TRUE and FALSE are not case-sensitive.

By default, SM_HIDEREADCOMM is not set—is undefined. In Figure 2-6, for example, the appearance of the ReadCommunity attribute and its value indicates that SM_HIDEREADCOMM either is not set or is set to FALSE or 0.

To hide the read community string in the Details tab of the Notification Properties dialog box:

1. Go to the *BASEDIR/smarts/bin* directory in the Service Assurance Management Suite (Global Manager) installation area and issue the following command to open the *runcmd_env.sh* file:

   ```
   sm_edit conf/runcmd_env.sh
   ```

2. Add the following line to the file:

   ```
   SM_HIDEREADCOMM=TRUE
   ```

3. Save the *runcmd_env.sh* file. The modified version of the file is saved to the *BASEDIR/smarts/local/conf* directory.
4. If the Global Manager was running before you edited the *runcmd_env.sh* file, restart the Global Manager.

The runcmd_env.sh file automatically sets the SM_HIDEREADCOMM environment variable (and any other environment variables that the file contains) for each newly started Global Manager application.

Network topology

The Global Manager imports instances of the following topology object types from IP Performance Manager. The imported topology includes systems, device connections, logical links, redundancy groups, and duplicate IPs (DuplicateIP objects)—the duplicate IPs are not shown in the list that follows.

Note: Bullet list items beginning with a dash indicate class hierarchy; for example, Firewall is a subclass of Router.

- Systems
  - Bridge
  - Host
  - Hub
  - LoadBalancer
  - Node
  - Probe
  - Router
    - Firewall
    - Multilayer Switch Feature Card (MSFC)
    - Router Switch Feature Card (RSFC)
    - Router Switch Module (RSM)
  - Switch
  - TerminalServer
- Device connections
  - NetworkConnection
    - Cable
    - TrunkCable
- Logical links
  - IPNetwork
  - VLAN
- Redundancy groups
  - SystemRedundancyGroup
  - NetworkAdapterRedundancyGroup
  - NetworkConnectionRedundancyGroup

Chapter 3, “Network Objects and Their Failures,” describes most of these topology object types, and Appendix A, "ICIM Network Concepts," in the *EMC Smarts IP Management Suite Discovery Guide* describes them all.

The Global Manager combines this topology with the topologies received from the other Domain Managers connected to the Global Manager.

Viewing network topology in maps

The Global Console presents the topology information in a variety of dynamically updated formats that show the status of the network objects and their many relationships. One of those formats is the topology map, which is a graphical representation of the topology.

Viewing topology maps is an easy and quick way to learn more about the source, impact, and cause of network notifications. You view the network topology maps, such as the one shown in Figure 2-7, using the Map Console view.

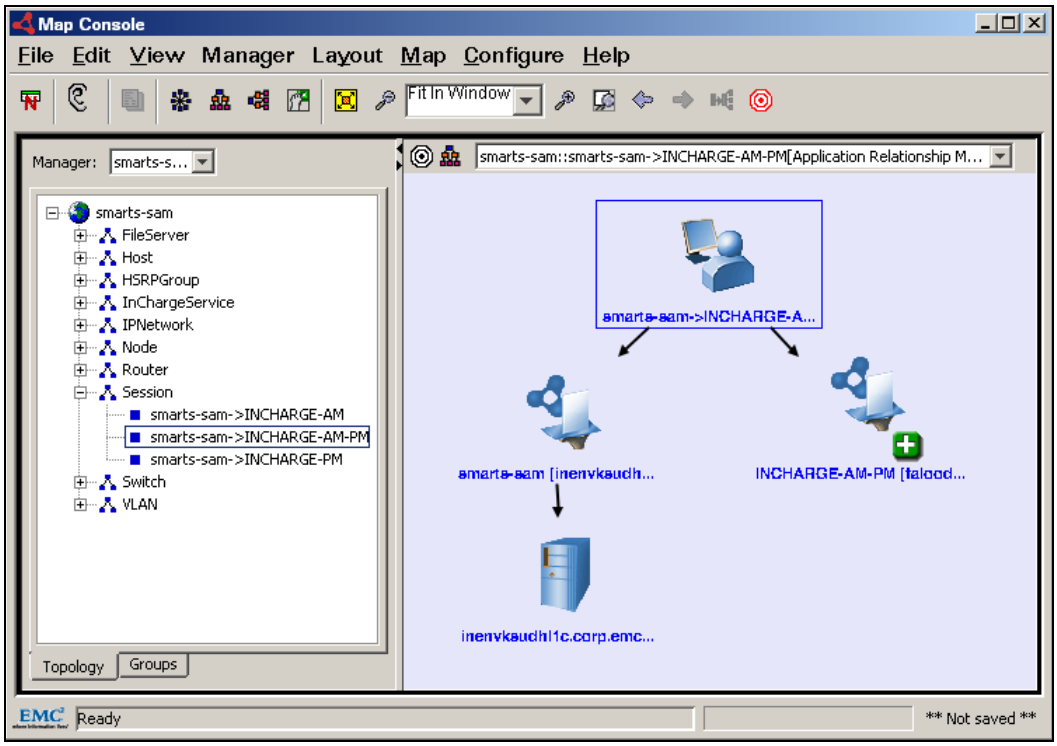

Figure 2-7 **Network topology map—example**

For information about the Map Console and general map concepts such as hops and color-coding in maps, see the *EMC Smarts Service Assurance Manager Operator's Guide*.

Opening a network topology map

You can use any of the following common methods to open a network topology map:

- Open the Map Console by selecting the Show Map menu option from any opened console attached to the Global Manager. For example, in the Notification Log Console, click a network notification and then select **Event > Show Map**, or right-click the notification and then select Show Map in the pop-up menu. In the Topology Browser Console, right-click a network object and then select Show Map in the pop-up menu.

- Open the Map Console from the Global Console by selecting **File > New > Map Console**. In the topology tree of the Map Console, click a network object to display a map for the object, or right-click a network object and then select a network map type (for example, Physical Connectivity) from the pop-up menu.
- In an opened topology map, right-click a network map icon and then select a network map type from the pop-up menu.

Network topology map pop-up menus

Two types of pop-up menus are available in a network topology map:

- Right-click a selected node in a map

  Opens a pop-up menu that enables you to select any of the map types available to the selected node (for example, Physical Connectivity, VLAN Connectivity, Group Membership), to display notification properties (if any) for the selected node, and so on. For a node marked with a + (plus) sign, the Expand Node menu option allows you to expand the node to see all nodes that are physically or logically connected to the node.

- Right-click an open space in a map

  Opens a pop-up menu that enables you to display a circular layout of the map, to manually position nodes in the map, and so on. The Reset map menu option enables you to reset changes made to the map or to return to the saved map display.

In the topology tree of a Map Console, a pop-up menu is also available when you right-click an object. This menu enables you to select any of the map types available to the selected object, to display notification properties (if any) for the selected object, and so on.

The *EMC Smarts Service Assurance Manager Operator's Guide* provides detailed descriptions of map menus and pop-up menus available for the Map Console.

Network topology map graphical representations

Network topology maps contain objects that may include IP networks, VLANs, routers, switches, hosts, and various types of connections such as cables and trunk cables. In a map display, a node is a graphical representation of a topology object, and an edge is a graphical representation of a relationship or connection between objects.

Table 2-2 identifies and describes the default nodes and edges that may appear in a network topology map. In the Map Console, you can also select **Map > Map Legend** to see a similar list.

Note that your system administrator may replace the standard map icons with other map icons that are preferred by your organization. In that case, use **Map > Map Legend** to see the definitions of your map icons.

Table 2-2 Default nodes, edges, and other indicators for network topology maps

Icon / Visual Indicator	Description
	Icon can represent a bridge, host, probe, terminal server, node, or unsupported device.
	Icon represents a hub.
	Icon represents a routing device. The routing device may be a physical router, a virtual router implemented within a physical router or a switch, or one of the following router cards installed in a physical switch: • Multilayer Switch Feature Card (MSFC) • Router Switch Feature Card (RSFC) • Router Switch Module (RSM)
	Icon represents a switch.
	Icon represents an IP network.
	Icon represents a VLAN.
	Icon represents a firewall.

Table 2-2 Default nodes, edges, and other indicators for network topology maps (continued)

Icon / Visual Indicator	Description
	Icon represents a redundancy group.
	Icon represents a network connection or a Permanent Virtual Circuit (PVC).
	Solid line can represent a physical connection, a logical IP connection, a logical VLAN connection, a membership, or a group relationship. A green line indicates a normal connection.
	Jagged line represents a network connection. A green line indicates a normal connection.
	Solid down arrow represents a dependency. A green arrow indicates a normal dependency.
	Dotted down arrow represents composition. A green arrow indicates a normal composition.
Light blue background	Light blue background appears in Physical Connectivity and Group Physical Connectivity maps.
Light yellow background	Light yellow background appears in IP Connectivity and Group IP Connectivity maps.
Light green background	Light green background appears in VLAN Connectivity and Group VLAN Connectivity maps.
Beige background	Beige background appears in IP Membership, VLAN Membership, and Group Membership maps.

Note: Additional icons may appear, depending on the underlying EMC Smarts products and certified devices.

Network topology map types

The following map types are available for viewing the network topology:

- Group Membership Map
- Physical Connectivity
- IP Network Connectivity
- IP Network Membership
- VLAN Connectivity
- VLAN Membership
- Group Maps

Table 2-3 summarizes the types of maps available for each type of object.

Table 2-3 Available network topology maps for topology objects

Object type	Available map types
Bridge Host Hub MSFC Probe Router RSM RSFC Switch TerminalServer Node	Physical Connectivity IP Network Connectivity VLAN Connectivity
IP Network	Physical Connectivity IP Network Membership IP Network Connectivity
VLAN	Physical Connectivity VLAN Membership VLAN Connectivity
Group	Group Physical Connectivity Group IP Network Connectivity Group VLAN Connectivity Group Membership

Physical Connectivity map

The Physical Connectivity map is the default map that appears when you select a system object (switch, router, hub, bridge, host) in the Topology tab of the Map Console. This map displays Layer 2 physical connectivity between system objects, including cables and network connections. A Physical Connectivity map is available for a selected system object, for all system objects in a selected IP network, and for all system objects in a selected VLAN.

For a Physical Connectivity map, the edges display as:

- Solid lines for direct connections such as cables.
- Jagged lines for network connections.

If you display a Physical Connectivity map for a selected IP network or VLAN, the map displays the physical connectivity of the system objects inside the IP network or VLAN. An icon representing the IP network or VLAN does not display.

In a Physical Connectivity map, a hop is the distance between two system objects that are physically connected.

IP Network Connectivity map

The IP Network Connectivity map is the default map that appears when you select an IP network in the Topology tab of the Map Console. It displays Layer 3 connectivity between routers and IP networks. An IP Network Connectivity map is available for a selected switch, router, RSM, hub, host, or IP network.

For an IP Network Connectivity map, the edges display as:

- Solid lines for IP addresses for objects on the connected IP network.
- Jagged lines for network connections.

In an IP Network Connectivity map, a hop is a logical hop. It represents the distance between a device and the IP network.

IP Network Membership map

The IP Network Membership map displays all objects having an IP address on a selected IP network. The edges display as solid lines for participation in the logical group and do not change color.

For an IP Network Membership map, the concept of a hop is not applicable.

VLAN Connectivity map

The VLAN Connectivity map is the default map that appears when you select a VLAN object in the Topology tab of the Map Console. It displays VLANs, the switches that participate in the VLAN, and the routers that enable connections between VLANs. A VLAN Connectivity map is available for a selected switch, router, RSM, hub, host, or VLAN.

For a VLAN Connectivity map, the edges display as:

- Solid lines for devices connected to ports on a VLAN or switch.
- Jagged lines for network connections.

In a VLAN Connectivity map, a hop is a logical hop. It represents the distance between an object (router or switch) and the VLAN. If a switch appears in a VLAN Connectivity map and no edge connects the switch to the VLAN, the switch is not capable of recognizing the VLAN even though the switch has another port that participates in the VLAN.

VLAN Membership map

The VLAN Membership map displays all devices that are members of a selected VLAN. The edges display as solid lines for participation in a selected VLAN and do not change color.

For a VLAN Membership map, the concept of a hop is not applicable.

Group maps

A group consists of one or more infrastructure devices, IP networks, VLANs, or subgroups. Groups are created by your administrator and might not be available for your session. For information about creating groups and importing data for groups, see the *EMC Smarts Service Assurance Manager Configuration Guide*.

Four types of group maps exist:

- Group Physical Connectivity map. This map displays physical connectivity between group objects. The solid line edges between groups represent one or more physical connections between objects of different groups. The edges do not change color to reflect their state. The number of hops cannot be changed.
- Group IP Network Connectivity map. In this map, an edge between two groups indicates that there are one or more IP networks common to the two groups. The group icon containing the IP network is displayed; no IP network icon is displayed. The number of hops cannot be changed.
- Group VLAN Connectivity map. In this map, an edge between two groups indicates that there are one or more VLANs common to the two groups. The group icon containing the VLAN is displayed; no VLAN icon is displayed. The number of hops cannot be changed.
- Group Membership. This map displays all the objects of a selected group or a subgroup. The edges do not display. The concept of a hop is not applicable.

Example 1: Displaying a Physical Connectivity map

To display a Physical Connectivity map:

1. Open the Map Console.
2. Select a system object in the Topology tab of the Map Console to display a Physical Connectivity map for the selected object.

Figure 2-8 shows an example of a Physical Connectivity map for a router named moto-gw.smarts.com. Note that the status of the switch named tetrahedron.smarts.com indicates that a major event is active. In addition, the icons representing the router and switches have a plus sign to indicate that their connectivity can be expanded by double-clicking their icons.

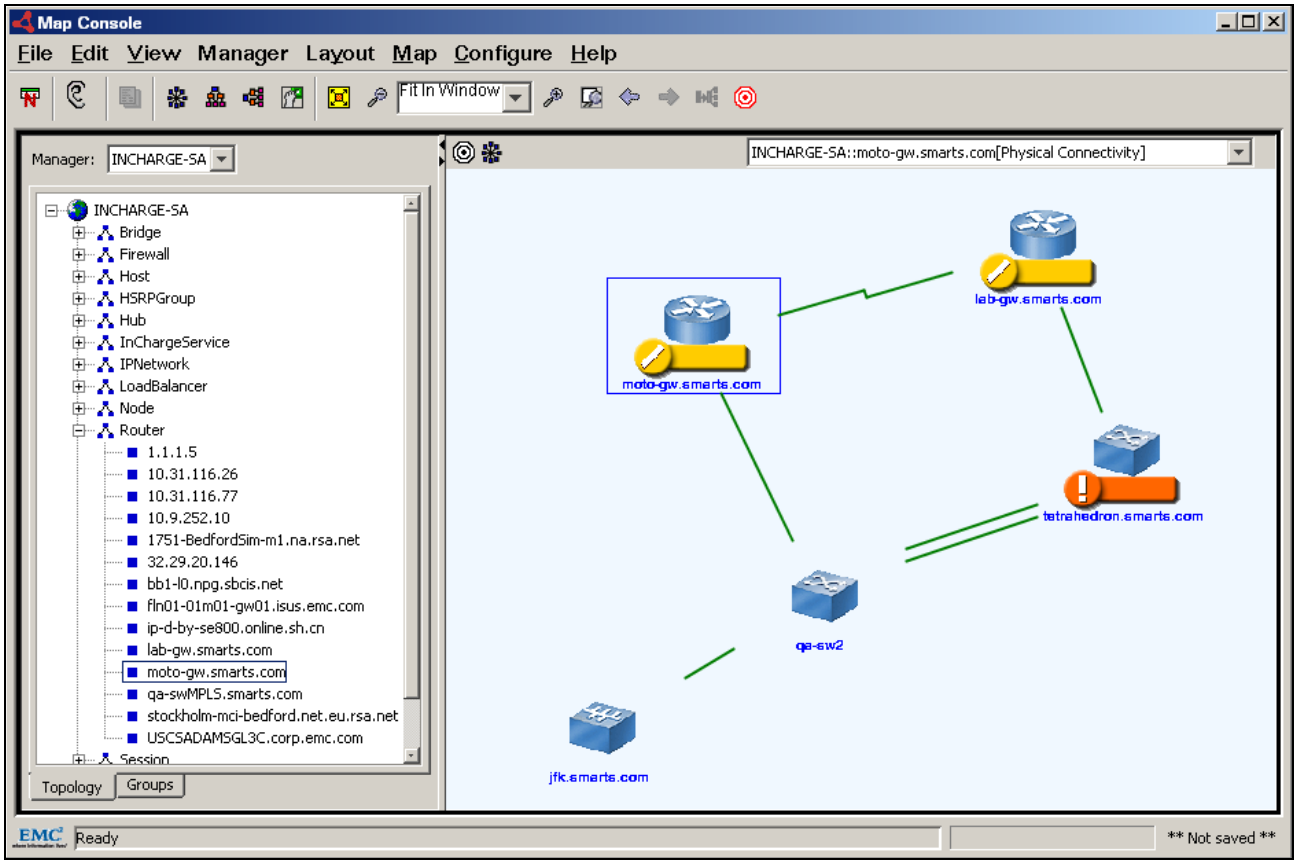

Figure 2-8 Physical Connectivity map

Example 2: Displaying a Group IPNetwork Connectivity map

To display a Group IPNetwork Connectivity map:

1. Open the Map Console.
2. Select an object in the Topology tab of the Map Console to display a map for the selected object.
3. Right-click the object and select Group IPNetwork Connectivity in the pop-up menu. The Group IPNetwork Connectivity map displays.

Figure 2-9 shows a Group IPNetwork Connectivity map for a subgroup named Second-Floor in the EMC group.

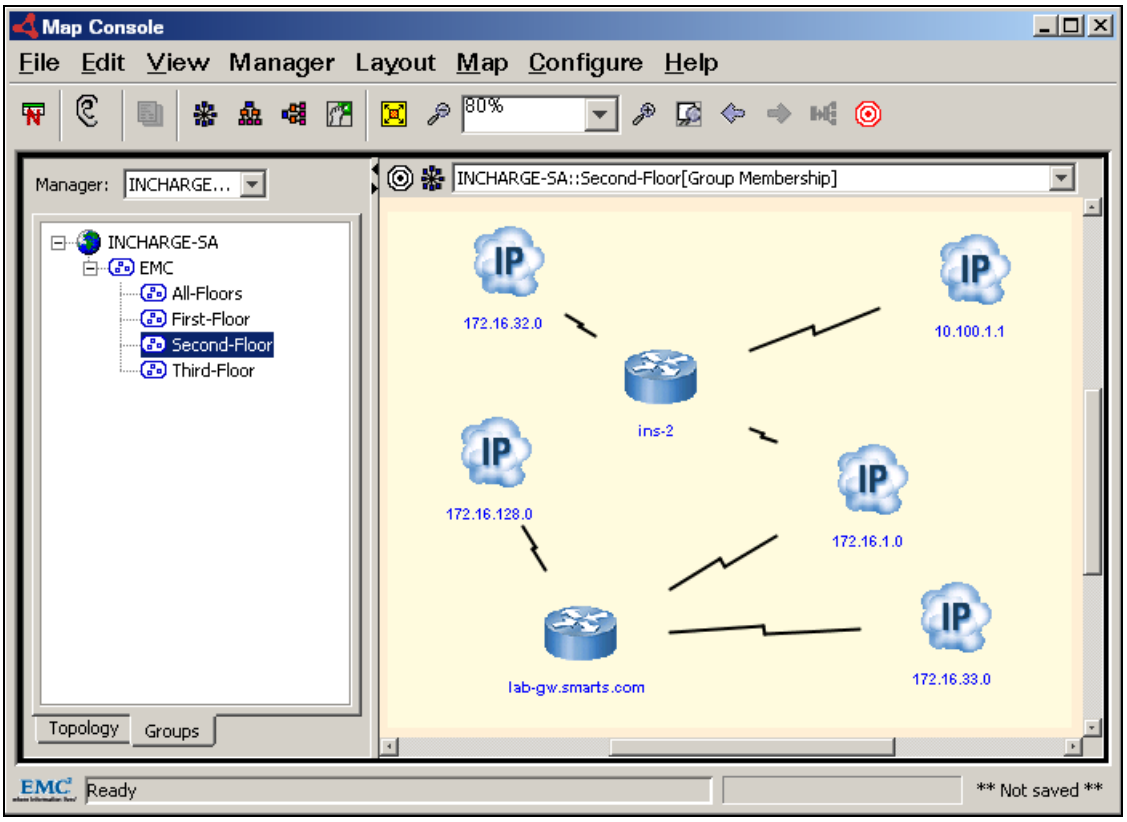

Figure 2-9 Group IP Network Connectivity map

Network containment

An object's Containment view appears in a dialog box that organizes the information for the object into tab pages and tables.

The intent of the Containment view is to allow users to examine detailed component topology of an individual object. The Global Console retrieves the topology information from the Global Manager and from the underlying Domain Managers. If an underlying Domain Manager is not attached to the console, the console automatically establishes a connection to the Domain Manager using the user's login ID.

In an IP Manager deployment, the Global Console retrieves the Containment topology information from the Global Manager, from IP Availability Manager and IP Performance Manager (typically running together as a single process), and from any other Domain Manager that attaches to the Global Manager. As an example, if you want to examine the network interfaces of a router, you can do so by opening a Containment dialog box for the router object. The console will retrieve the interface topology information from the underlying IP Availability Manager and IP Performance Manager.

Opening a network containment dialog box

To obtain containment information about an individual network object, you can use any of the following common methods to open a Containment dialog box for the object:

- In a network map tree, right-click the object and then select Containment in the pop-up menu.
- In a network map display, right-click the object and then select Containment in the pop-up menu.
- In a Topology Browser Console, right-click the object and then select Containment in the pop-up menu.
- In a Notification Log Console, double-click a notification for the object and click the Containment button in the Notification Properties dialog box.

Viewing network containment

Figure 2-10 shows a Containment dialog box for a switch object.

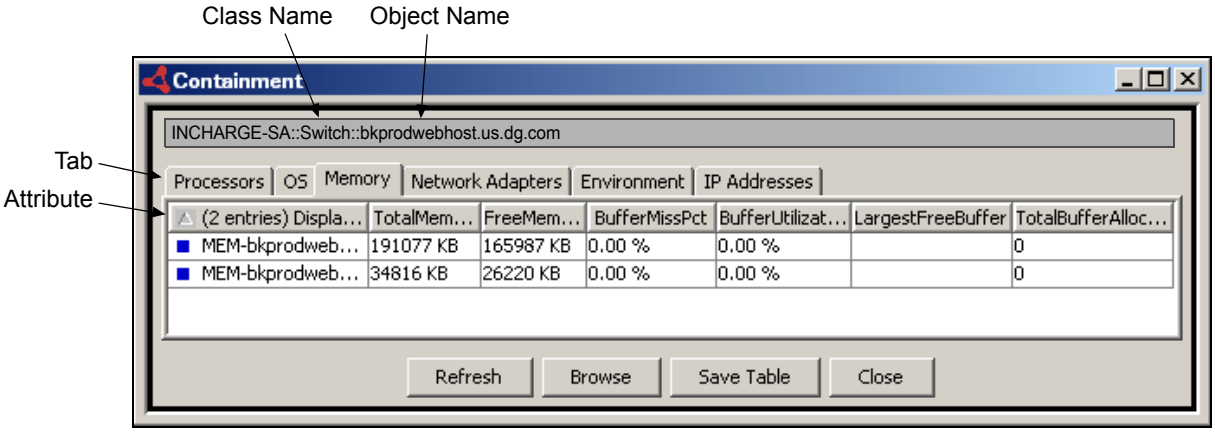

Figure 2-10 Switch Containment dialog box—example

In an object's Containment view, what tabs appear depends on which IP Managers are deployed, which feature licenses are installed, and which components are discovered.

Note: Containment is not available for user-defined groups and services.

Network containment tab pages

The network tab pages that appear in a Containment view for a network object contain the topology information listed in Table 2-4.

Table 2-4 Network classes and their containment tab pages and associated attributes

Class name	Network tab name	Attributes in tab page
Bridge	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus

Table 2-4 Network classes and their containment tab pages and associated attributes (continued)

Class name	Network tab name	Attributes in tab page
Host	File Systems (Available only if IP Server Performance Manager is in the deployment)	Root StorageSize AvailableSpace UtilizationPct
	Disks (Available only if IP Server Performance Manager is in the deployment)	DisplayName AvgDataRate AvgQueueDepth
	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
	Memory (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName TotalMemory FreeMemory BufferMissPct BufferUtilizationPct LargestFreeBuffer TotalBufferAllocationFailures
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	Processors (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName CurrentUtilization

Table 2-4 Network classes and their containment tab pages and associated attributes (continued)

Class name	Network tab name	Attributes in tab page
FileServer	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
Hub	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName

Table 2-4 Network classes and their containment tab pages and associated attributes (continued)

Class name	Network tab name	Attributes in tab page
LoadBalancer	Processors (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName CurrentUtilization
	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
Node	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus

Table 2-4 Network classes and their containment tab pages and associated attributes (continued)

Class name	Network tab name	Attributes in tab page
Probe	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus

Table 2-4 Network classes and their containment tab pages and associated attributes (continued)

Class name	Network tab name	Attributes in tab page
Router	Processors (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName CurrentUtilization
	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
	Memory (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName TotalMemory FreeMemory BufferMissPct BufferUtilizationPct LargestFreeBuffer TotalBufferAllocationFailures
	Cards	DisplayName Status
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	Environment (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName CreationClassName Status
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	IPv6 Addresses	Address PrefixLength IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	IPv6 Networks	NetworkNumber PrefixLength

Table 2-4 Network classes and their containment tab pages and associated attributes (continued)

Class name	Network tab name	Attributes in tab page
Firewall	Processors (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName CurrentUtilization
	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus

Table 2-4 Network classes and their containment tab pages and associated attributes (continued)

Class name	Network tab name	Attributes in tab page
Multilayer Switch Feature Card (MSFC) Router Switch Feature Card (RSFC) Router Switch Module (RSM)	VPN Peers	VRFName SystemName DIsplayName RouteDistinguisher OperStatus NumberOfRoutes
	LSP Hops	DisplayName LSPId Label IsHavingProblems
	VRF Interfaces	CreationClassName Type DisplayName AdminStatus
	CEs attached	DisplayName Description Vendor Model Type Location
	VPN PEs	DisplayName Description Vendor Model Type Location
	All VRFs	SystemName DIsplayName RouteDistinguisher OperStatus NumberOfRoutes
	Hub VRFs	SystemName DIsplayName RouteDistinguisher OperStatus NumberOfRoutes
	Spoke VRFs	SystemName DIsplayName RouteDistinguisher OperStatus NumberOfRoutes

Table 2-4 Network classes and their containment tab pages and associated attributes (continued)

Class name	Network tab name	Attributes in tab page
Switch	Processors (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName CurrentUtilization
	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
	Memory (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName TotalMemory FreeMemory BufferMissPct BufferUtilizationPct LargestFreeBuffer TotalBufferAllocationFailures
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	Environment (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName CreationClassName Status
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus

Table 2-4 Network classes and their containment tab pages and associated attributes (continued)

Class name	Network tab name	Attributes in tab page
TerminalServer	File Systems (Available only if IP Server Performance Manager is in the deployment)	Root StorageSize AvailableSpace UtilizationPct
	Disks (Available only if IP Server Performance Manager is in the deployment)	DisplayName AvgDataRate AvgQueueDepth
	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
	Memory (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName TotalMemory FreeMemory BufferMissPct BufferUtilizationPct LargestFreeBuffer TotalBufferAllocationFailures
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	Processors (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName CurrentUtilization
Card Chassis NASChassis	Hosts	DisplayName Vendor Model Description IsUnresponsive Location PrimaryOwnerName PrimaryOwnerContact

Table 2-4 Network classes and their containment tab pages and associated attributes (continued)

Class name	Network tab name	Attributes in tab page
NetworkConnection Cable TrunkCable	Connected Systems	DisplayName Vendor Model Description IsUnresponsive Location PrimaryOwnerName PrimaryOwnerContact
	Connected Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
IP DuplicateIP VPNIP DuplicateVPNIP	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	Cards	DisplayName Status

Table 2-4 Network classes and their containment tab pages and associated attributes (continued)

Class name	Network tab name	Attributes in tab page
IPv6 DuplicateIPv6	IPv6 Addresses	Address PrefixLength IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	Cards	DisplayName Status
	IPv6 Networks	NetworkNumber PrefixLength
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory
IPNetwork VPNIPNetwork	Connected Systems	DisplayName Vendor Model Description IsUnresponsive Location PrimaryOwnerName PrimaryOwnerContact
IPv6Network	Connected Systems	DisplayName Vendor Model Description IsUnresponsive Location PrimaryOwnerName PrimaryOwnerContact

Table 2-4 Network classes and their containment tab pages and associated attributes (continued)

Class name	Network tab name	Attributes in tab page
VLAN	Connected Systems	DisplayName Vendor Model Description IsUnresponsive Location PrimaryOwnerName PrimaryOwnerContact
SystemRedundancyGroup NetworkAdapterRedundancyGroup NetworkConnectionRedundancyGroup HSRPGroup	HSRP Systems	DisplayName Vendor Model Description IsUnresponsive Location PrimaryOwnerName PrimaryOwnerContact
	HSRP Interfaces	DisplayName Priority State InterfaceName InterfaceNumber InterfaceAdminStatus InterfaceOperStatus SystemName

3

Network Objects and Their Failures

This chapter describes the network objects managed by IP Performance Manager and identifies the faults, events, and exceptions for each object type. It consists of the following sections:

- Summary of exceptions, faults, and events 3-2
- Network objects, attributes, exceptions, faults, and events 3-5
- System 3-6
- Chassis 3-11
- VLAN 3-13
- Network adapter 3-15
- Processor 3-25
- Memory 3-26
- Disk 3-28
- FileSystem 3-30
- PowerSupply 3-32
- VoltageSensor 3-34
- TemperatureSensor 3-36
- Fan 3-38
- DuplicateIP 3-39

Summary of exceptions, faults, and events

IP Performance Manager generates exceptions, detects performance faults, and detects events. It uses the performance faults to generate exceptions.

A performance fault is an abnormal condition that occurs when a component of a managed system, Chassis, or VLAN exceeds a threshold. An exception, or aggregate event, is a collection of performance faults associated with a particular managed system, Chassis, or VLAN. IP Performance Manager generates an exception whenever any of the composite faults for the managed system, Chassis, or VLAN occur. For example, IP Performance Manager will generate a ResourceException whenever a router has exhausted most of its processor or memory resources.

The Global Manager imports all faults and events detected by IP Performance Manager. (It does not import IP Performance Manager exceptions.) The fault notifications (one fault per notification) and the event notifications (one event per notification) are displayed in the Global Console.

Exceptions and faults summary

Table 3-1 lists the performance exceptions, the faults that trigger them, and the performance thresholds associated with each fault. The table also identifies the managed objects (systems, Chassis, VLANs) for which the exceptions are generated as well as the components of the managed objects that can be at fault.

Table 3-1 Exceptions generated by IP Performance Manager

Managed object	Exception	Component	Fault *	Threshold (setting)
System	Performance	Network adapter (Port or Interface)	HighBroadcastRate	BroadcastThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
			HighDiscardRate	DiscardThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
			HighQueueDropRate	QueueDropThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
			HighCollisionRate	CollisionThreshold (Ethernet Interface/Port Performance)
			HighUtilization	UtilizationThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
	Error	Network adapter (Port or Interface)	HighErrorRate	ErrorThreshold ErrorTrafficThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)

* Imported by the Global Manager.
** Available through IP Server Performance Manager only.

Table 3-1 Exceptions generated by IP Performance Manager (continued)

Managed object	Exception	Component	Fault *	Threshold (setting)
System (continued)	Resource	Memory	ExcessiveFragmentation	MemoryFragmentationThreshold (Processor and Memory)
			HighBufferMissRate	MemoryBufferMissThreshold (Processor and Memory)
			HighBufferUtilization	MemoryBufferUtilizationThreshold (Processor and Memory)
			InsufficientFreeMemory	FreeMemoryThreshold (Processor and Memory)
			InsufficientFreeMemory_MemoryPool	FreeMemoryThreshold
		Processor	HighUtilization	ProcessorUtilizationThreshold (Processor and Memory)
			HighUtilization_avgBusy5	ProcessorUtilizationThreshold
			HighUtilization_cpmCPUTotal5min	ProcessorUtilizationThreshold
		FileSystem (Host only) **	HighUtilization	MaxUtilizationPct (FileSystem)
	Operational	Disk (Host only) **	OperationallyDown	None
	PowerSupply	PowerSupply	StateNotNormal	None
		VoltageSensor	OutOfRange	RelativeVoltageThreshold (Environment)
			StateNotNormal	None
	Temperature	TemperatureSensor	OutOfRange	RelativeTemperatureThreshold (Environment)
			StateNotNormal	None
		Fan	StateNotNormal	None
Chassis	BackplaneUtilization	Chassis	HighBackplaneUtilization	BackplaneUtilizationThreshold (Processor and Memory)

* Imported by the Global Manager.
** Available through IP Server Performance Manager only.

Table 3-1 Exceptions generated by IP Performance Manager (continued)

Managed object	Exception	Component	Fault *	Threshold (setting)
VLAN	Performance	Network adapter (Port)	HighBroadcastRate	BroadcastThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
			HighDiscardRate	DiscardThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
			HighQueueDropRate	QueueDropThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
			HighCollisionRate	CollisionThreshold (Ethernet Interface/Port Performance)
			HighUtilization	UtilizationThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
	Error	Network adapter (Port)	HighErrorRate	ErrorThreshold ErrorTrafficThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)

* Imported by the Global Manager.
** Available through IP Server Performance Manager only.

Events summary

Table 3-2 lists the events detected by IP Performance Manager.

Table 3-2 Events detected by IP Performance Manager

Managed object	Event *	Threshold (setting)
System	DiscoveryError	None
DuplicateIP	Duplicate	None

* Imported by the Global Manager.

Note: Appendix C, "Exception, Fault, Event, and Notification Summary," provides a summary of the exceptions generated by IP Performance Manager, the faults detected by IP Performance Manager to generate the exceptions, the events detected by IP Performance Manager, and the notifications imported by the Global Manager from IP Performance Manager.

Network objects, attributes, exceptions, faults, and events

The sections that follow describe key attributes, exceptions, faults, and events for the following categories of network object types in the IP Performance Manager data model:

- Systems

  Represent computer-based entities. Examples of systems are Switch, Router, Hub, Bridge, and Host.

- Physical packages

  Represent physical objects that contain or host other components. An example of a physical package is Chassis.

- Network adapters

  A network adapter represents a Layer 2 connection point. Network adapters include Port and Interface.

- Service access points

  A service access point describes a logical endpoint that can be used to gain access to some network service. Examples of protocol endpoints are IP, DuplicateIP, and MAC.

  Note: Service access points are often described as protocol endpoints.

- Logical links

  A logical link models the path that connects service access points to each other. Examples of logical links are IPNetwork and VLAN.

- Logical devices

  A logical device is an emulation of a hardware entity that might or might not be realized in physical hardware. Logical devices include:

  - Processor
  - Memory
  - Disk
  - FileSystem
  - PowerSupply
  - VoltageSensor
  - TemperatureSensor
  - Fan

IP Performance Manager also instantiates device connection, collection, management agent, and redundancy group object types, but because IP Performance Manager does no analysis for these object types, they are not discussed here. Appendix A, "ICIM Network Concepts," in the *EMC Smarts IP Management Suite Discovery Guide* describes all of the object types instantiated by IP Performance Manager.

All of the object types instantiated by IP Performance Manager are available to a Global Console attached to IP Performance Manager, and a subset are available to a Global Console attached to the Global Manager. "Network topology" on page 2-12 provides a list of the object types imported by the Global Manager.

System

A system is a logically complete group of objects that provide services to users or other systems. Such objects may include processors, memory, disks, filesystems, network adapters, and cards.

- Bridge—A protocol-independent system that connects two LAN segments.
- FileServer—A system that hosts file shares.
- Firewall—A system that controls the flow of traffic between networks.
- Host—A general purpose computer, such as a workstation or server.
- Hub—A system that connects multiple physical segments. Active hubs are multi-port repeaters, which means that they repeat signals received on any port to all the other ports.
- LoadBalancer—A system that distributes client traffic across multiple web servers.
- Multilayer Switch Feature Card (MSFC)—A card in a switch that performs routing between VLANs.
- Node—A system that is monitored using generic network management instrumentation. Nodes are probed for standard MIB-II information but not for enterprise-specific information such as system resources.
- Probe—A system that monitors networks or other systems. An example is a Remote Monitoring (RMON) probe.
- Router—A system or, in some cases, software in a computer that determines the next network point to which a packet should be forwarded as it travels toward its destination. A router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks to which the router is connected.

  A router might also be a virtual router, which is a software emulation of a router implemented within a physical router or switch. Each virtual router has its own independent IP routing and forwarding tables, which permit the same routing and forwarding of packets as with a standard router. Virtual routers are often used with VPNs to allow a greater separation of VPN traffic while using the same equipment.
- Router Switch Feature Card (RSFC)—A card in a Catalyst switch that runs Cisco IOS router software and is used to perform routing between VLANs.
- Router Switch Module (RSM)—A card in a switch that performs routing between VLANs.
- Switch—A system that switches packets, typically at wire speeds, between physically separate network segments.
- TerminalServer—A specialized system that connects terminals to a network.
- Uncertified—An uncertified object identifies a system that has yet to be certified by EMC Corporation.

Attributes for system

Table 3-3 lists some key attributes for system.

Table 3-3 Attributes for system

Attribute	Description	Allowed values
AccessMode	Mode to access this system.	Enum: • ICMPONLY • ICMPSNMP • SNMPONLY
Certification	Defines the level of certification that this system has in the discovery process. • GENERIC indicates that the OID for this system is not recognized; this system is classified as GENERIC and is added to the Node class. • TEMPLATE indicates that this system is recognized but no information about the MIBs that this system supports is known. • CERTIFIED indicates that this system has the highest level of certification and is discovered using enterprise MIBs and standard MIB-II data. • UNDISCOVERED indicates that this system is undiscovered.	Enum: • GENERIC • TEMPLATE • CERTIFIED • UNDISCOVERED
DiscoveryErrorInfo	Message describing the last discovery error for this system; for example: No response from Ping	String
DisplayName	Name, as shown in the Global Console, of this system; for example: qa-switch.smarts.com	String
IsAddressable	TRUE if this system is IP addressable.	Boolean: true or false
IsDiscoveryInProgress	TRUE if discovery is in progress for this system.	Boolean: true or false
IsSeed	TRUE if this system is added as a seed system.	Boolean: true or false
IsUnresponsive	TRUE if this system is not responding to ICMP pings or SNMP polls. (FALSE if this system is responding to ICMP pings and/or SNMP polls.)	Boolean: true or false
Model	Name by which this system is generally known; for example: WS-C3550-24	String
Name	Name, as known in the modeled topology, of this system; for example: qa-switch.smarts.com	String
NumberOfInterfaces	Number of interfaces discovered for this system; for example: 4	Integer

Table 3-3 Attributes for system (continued)

Attribute	Description	Allowed values
NumberOfIPs	Number of IP addresses discovered for this system; for example: 13	Integer
NumberOfNetworkAdapters	Number of network adapters (ports and interfaces) discovered for this system; for example: 28	Integer
NumberOfPorts	Number of ports discovered for this system; for example: 24	Integer
OSVersion	Software version of this system's operating system.	String
ReadCommunity	SNMP read community string for this system; for example: public	String
SNMPAddress	Primary address used to contact the SNMP agent running on this system. **Note:** This system hosts more than one network address, another address might be currently being used to contact the SNMP agent.	String
SupportsSNMP	TRUE if this system is manageable via SNMP.	Boolean: true or false
SystemObjectID	System object identifier associated with the vendor of this system; for example: .1.3.6.1.4.1.9.1.366	String
Type	Type of this system; for example: SWITCH	Enum: • HOST • ROUTER • SWITCH • HUB • SERVER • BRIDGE • REPEATER • PROBE • OTHER • TERMINALSERVER
Vendor	Name of this system's supplier.	String

Exceptions for system

IP Performance Manager generates an exception for a system when it detects a performance fault for one or more of its components. The components of a system include network adapters (ports or interfaces), processors, memory, disks, filesystems, power supplies, voltage sensors, temperature sensors, and fans.

System PerformanceException

A system PerformanceException indicates that at least one of a system's network adapters is misconfigured or is exhibiting utilization conditions that affect an adapter's ability to receive or process packets.

Network adapter faults that result in a system PerformanceException are described in "Network adapter" on page 3-15.

System ErrorException

A system ErrorException indicates that a network adapter is experiencing transmission or functional problems, resulting in an abnormal number of errors.

The network adapter fault (HighErrorRate) that results in a system ErrorException is described in "Network adapter" on page 3-15.

System ResourceException

A system ResourceException indicates that processor or memory faults are occurring because a system does not have enough processor or memory resources to process the current traffic load. For a host system, a ResourceException might also indicate that the utilization of the host's filesystem is higher than normal. Filesystem monitoring and analysis is available through IP Server Performance Manager only.

Processor, memory, and filesystem faults that result in a system ResourceException are described in "Processor" on page 3-25, "Memory" on page 3-26, and "FileSystem" on page 3-30.

System OperationalException

A system OperationalException indicates that a disk on a host system is experiencing faults possibly because the disk is not operational. Disk monitoring and analysis is available through IP Server Performance Manager only.

Disk faults that result in a system OperationalException are described in "Disk" on page 3-28.

System PowerSupplyException

A system PowerSupplyException indicates that power supply or voltage conditions around a system present a potential hazard.

Power supply and voltage faults that result in a system PowerSupplyException are described in "PowerSupply" on page 3-32 and "VoltageSensor" on page 3-34.

System TemperatureException

A system TemperatureException indicates that the temperature conditions around the system present a potential hazard.

Temperature and fan faults that result in a system TemperatureException are described in "TemperatureSensor" on page 3-36 and "Fan" on page 3-38.

Events for system

The only event detected for system is DiscoveryError, which is exported to the Global Manager. A DiscoveryError indicates that the discovery process did not rediscover a system.

A DiscoveryError is detected under the following conditions:

- SNMP request times out
- SNMPAgent encounters a loop
- System Down
- Qualified access address not found
- A previously discovered system fails authentication

The condition is listed in the DiscoveryErrorInfo attribute of a DiscoveryError notification. Chapter 8, "Understanding Discovery Results," in the *EMC Smarts IP Management Suite Discovery Guide* provides information about resolving DiscoveryErrors.

Note: The Out of License event may also occur during discovery. This event stops the discovery process if more systems are discovered than are permitted with your EMC Smarts volume licenses. Chapter 8, "Understanding Discovery Results," in the *EMC Smarts IP Management Suite Discovery Guide* provides information about the effects of this event.

Chassis

A chassis is a physical package that encloses other objects and provides definable functionality, such as a desktop, processing node, uninterruptible power supply (UPS), disk or tape storage, or a combination of these.

Attributes for Chassis

Table 3-4 lists some key attributes for Chassis.

Table 3-4 Attributes for Chassis

Attribute	Description	Allowed values
BackplaneUtilization	Percentage of bandwidth utilization for the Chassis backplane as reported by the instrumentation; for example: 3.0	Numeric (float)
DisplayName	Name, as shown in the Global Console, of this Chassis; for example: CHASSIS-10.9.1.108	String
IsAnySystemResponsive	TRUE if any system packaged by this Chassis is responding to ICMP pings and/or SNMP polls.	Boolean: true or false
Location	Specifies the position and address of this Chassis.	String
Name	Name, as known in the modeled topology, of this Chassis; for example: CHASSIS-10.9.1.108	String
SerialNumber	Indicates the version of this Chassis.	String

Table 3-4 Attributes for Chassis (continued)

Attribute	Description	Allowed values
Status	Reflects the current state of the Chassis as reported by the instrumentation. • OK indicates that this Chassis is operating normally. • MARGINAL indicates that this Chassis is partially operational. • CRITICAL indicates that this Chassis is not operational. • OTHER indicates that the status of this Chassis is other than OK, MARGINAL, or CRITICAL, or is an unrecognized SNMP error. • NOTPRESENT indicates that the MIB Status value for this Chassis is missing. IP Availability Manager sets a Chassis' Status value to NOTPRESENT when receiving one of the following SNMP errors: SNMP_EXP_NOSUCHOBJECT SNMP_ERR_NOSUCHNAME SNMP_EXP_NOSUCHINSTANCE SNMP_EXP_ENDOFMIB • UNKNOWN is the default Status value before sending SNMP polls to this Chassis.	Enum: • OK • MARGINAL • CRITICAL • OTHER • NOTPRESENT • UNKNOWN
SystemName	Name of the system containing this Chassis.	String
Tag	Uniquely identifies this Chassis and serves as the Chassis' key. The Tag property can contain information such as asset tag or serial number data.	String

Exceptions for Chassis

IP Performance Manager generates the following exception for Chassis.

BackplaneUtilizationException: Indicates that excessive data is being transmitted over a chassis' backplane.

Faults for Chassis

IP Performance Manager detects the following fault for Chassis.

HighBackplaneUtilization fault: The data being transmitted over the chassis' backplane has exceeded the BackplaneUtilizationThreshold. This threshold is contained in the Processor and Memory setting, described in Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide*.

When IP Performance Manager detects a HighBackplaneUtilization fault for a chassis, it generates a BackplaneUtilizationException for the chassis.

VLAN

A VLAN groups user stations and network devices into a single logical network regardless of the physical LAN segment to which the stations or devices are attached. A VLAN allows traffic to flow within populations of mutual interest.

Attributes for VLAN

Table 3-5 lists some key attributes for VLAN.

Table 3-5 Attributes for VLAN

Attribute	Description	Allowed values
DisplayName	Name, as shown in the Global Console, of this VLAN; for example: VLAN-2 [VLAN0002]	String
isImpactPropOver-VLANEnabled	TRUE if impact propagation over VLANs is allowed; FALSE if impact propagation over VLANs is prevented. The value of this attribute is controlled by the "Problem Impact propagation policy over VLANs" setting, which is described in Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide*.	Boolean: true or false (Default: true)
MembershipCriteria	Membership criteria for participation in this VLAN. (PORT membership criteria is assumed here.)	Enum: • MACADDRESS • PORT • INTERFACE • PROTOCOL • OTHER • UNKNOWN
Name	Name, as known in the modeled topology, of this VLAN; naming scheme is VLAN-<VLANKey>; for example: VLAN-2	String
VLANKey	Value that distinguishes this VLAN from all other VLANs in the managed topology and consists of any combination of the following identifiers: <management domain name> <user-defined VLAN tag> <VLANNumber> Example of a VLANKey value consisting of just a management domain name: VLAN #66 Example of a VLANKey value consisting of a user-specified VLAN tag and a VLANNumber: Marketing-2 Example of a VLANKey value consisting of just a VLANNumber: 2	String

Table 3-5 **Attributes for VLAN (continued)**

Attribute	Description	Allowed values
VLANNumber	Number, or VLAN ID, that uniquely defines this VLAN across all VLANs within a given VLAN domain; for example: 2 **Note:** This number is not guaranteed to be unique across all VLANs in the managed topology but is unique across all VLANs within a given VLAN domain.	Integer (The range of the VLAN number depends on the bridging protocol. For the 802.1Q protocol, the range is 1 to 4096.)

Exceptions for VLAN

IP Performance Manager generates an exception for a VLAN when it detects a fault for any of the network adapters (ports) that are members of the VLAN.

VLAN PerformanceException

A VLAN PerformanceException indicates that one or more of the ports that are members of the VLAN are misconfigured or are exhibiting utilization conditions that affect a port's ability to receive or process packets.

Network adapter faults that result in a VLAN PerformanceException are described in "Network adapter" on page 3-15.

VLAN ErrorException

A VLAN ErrorException indicates that one or more of the ports that are members of the VLAN are experiencing transmission or functional problems.

The network adapter fault (HighErrorRate) that results in a VLAN ErrorException is described in "Network adapter" on page 3-15.

Network adapter

A network adapter is a logical or physical component of a network system at which the system connects to a network. IP Performance Manager performs performance analysis on the following network adapter object types:

- Port—A point where the physical connection to a network segment is made. For example, an Ethernet segment is connected to an Ethernet switch at one of the switch's ports. A port may have a Media Access Control (MAC) address associated with it.

  IP Performance Manager separates ports into two groups: trunk ports and access ports. A trunk port is a switch port that is connected to a switch, router, hub, or bridge. An access port is connected to a host.

  Note: By default, IP Performance Manager monitors trunk ports but not access ports. However, if you so choose, you can enforce a management policy that manages access ports, as described in Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide*.

- Interface—A point where the physical connection to a network is made. An interface may have a MAC address, an IP address, or both. For example, a host uses an Ethernet interface to connect to an Ethernet segment.
- Subinterface—A logical division of a physical interface. A physical interface can be divided into one or more subinterfaces. For example, in a typical frame relay or ATM network, a physical interface is configured with multiple virtual circuits and each virtual circuit is associated with a subinterface.

  Note: Subinterface objects are instances of the Interface class.

Attributes for network adapter

Table 3-6 lists some key attributes for network adapter.

Table 3-6 Attributes for network adapter

Attribute	Description	Allowed values
AdminStatus	Reflects the current administrative status of this network adapter (port or interface) as reported by the instrumentation. • UP indicates that this network adapter is administratively enabled. • DOWN indicates that this network adapter is administratively disabled. • TESTING indicates that this network adapter is in testing mode. • OTHER indicates that this network adapter is in an unknown state. • NOTPRESENT indicates that the MIB AdminStatus value for this network adapter is missing. IP Availability Manager sets a network adapter's AdminStatus value to NOTPRESENT when receiving one of the following SNMP errors: SNMP_EXP_NOSUCHOBJECT SNMP_ERR_NOSUCHNAME SNMP_EXP_NOSUCHINSTANCE SNMP_EXP_ENDOFMIB • UNKNOWN indicates that this network adapter has yet to be polled. **Note:** IP Availability Manager uses the values of a network adapter's AdminStatus and OperStatus attributes to determine the state of the adapter. When the value of AdminStatus is UP, the value of OperStatus determines the state of the adapter. Otherwise, the value of AdminStatus determines the state of the adapter.	Enum: • UP • DOWN • TESTING • OTHER • NOTPRESENT • UNKNOWN
CurrentUtilization	Current utilization of this network adapter as reported by the instrumentation. The utilization is expressed as a percentage of the bandwidth; for example: 3.7179998E-4	Numeric (float)
DeviceID	Address or other identifying information to uniquely name this network adapter. DeviceID refers to the system to which this network adapter belongs.	String
DisplayName	Name, as shown in the Global Console, of this network adapter. Port example: PORT-10.9.252.2/1 [Gi1/1] Interface example: IF-10.9.1.253/1 [Ethernet] [10.9.1.253]	String

Table 3-6 Attributes for network adapter (continued)

Attribute	Description	Allowed values
DuplexMode	Indicates whether this network adapter is full-duplex or half-duplex. • FULLDUPLEX indicates that this network adapter is full-duplex. • HALFDUPLEX indicates that this network adapter is half-duplex. • UNSPECIFIED indicates that the duplex mode value is not available for this network adapter.	Enum: • FULLDUPLEX • HALFDUPLEX • UNSPECIFIED
DuplexSource	Indicates the source for setting this network adapter to full-duplex or half-duplex. • ENTERPRISE_MIB indicates that duplex mode for this network adapter is set by an enterprise specific MIB. • ETHERLIKE_MIB indicates that duplex mode for this network adapter is set by the value of dot3StatsDuplexStatus in the ETHERLIKE MIB. • NEIGHBOR_MIB indicates that duplex mode for this network adapter is set by the neighbor MIB (such as the Cisco CDP MIB). • USER_CHANGED indicates that duplex mode for this network adapter is set by the user. • ASSUMED indicates that duplex mode for this network adapter is set based on the type of network adapter. • NONE indicates that duplex mode for this network adapter is not set by any source. • OTHER_SOURCE value is a placeholder for future use.	Enum: • ENTERPRISE_MIB • ETHERLIKE_MIB • NEIGHBOR_MIB • USER_CHANGED • ASSUMED • NONE • OTHER_SOURCE
InterfaceAlias	An alias name for the network adapter as specified by a network manager; for example: • By VPNSC: Job Id# = 77 • By VPNSC: Job Id# = 82	String
IsFlapping	TRUE if this network adapter is flapping. (FALSE if this network adapter is not flapping.)	Boolean: true or false
MaximumUptime	Maximum length of time, in seconds, that a backup or dial-on-demand network adapter may be in the UP state before the event ExceededMaximumUptime is generated. If this attribute is set to 0, the event is disabled.	Integer
MaxSpeed	Maximum speed, in bits per second (bps), for this network adapter; for example: 10000000 bps	Integer

Table 3-6 Attributes for network adapter (continued)

Attribute	Description	Allowed values
MaxTransferUnit	Size of the largest datagram, in octets, that can be sent or received on this network adapter; for example: 1500 octets For a network adapter that is used for transmitting network datagrams, this value is the size of the largest network datagram that can be sent on the adapter.	Integer
Mode	Indicates the intended purpose of this network adapter: normal, backup, or dial-on-demand. The diagnostics applied to a particular network adapter varies based on its mode. For instance, an event is not generated when a backup or dial-on-demand adapter is down.	Enum: • NORMAL • BACKUP • ONDEMAND
Name	Name, as known in the modeled topology, of this network adapter. Port example: PORT-10.9.252.2/1 Interface example: IF-10.9.1.253/1	String
NumberOfNetworkAdapters	Total number of network adapters for the system containing this network adapter.	Integer
OperStatus	Reflects the current operational status of this network adapter as reported by the instrumentation. • UP indicates that this network adapter is operationally up. • DOWN indicates that this network adapter is operationally down. • TESTING indicates that this network adapter is in testing mode. • OTHER indicates that this network adapter is in an unknown state. • DORMANT indicates that this network adapter is waiting for an external action to occur before becoming active. • NOTPRESENT indicates that the MIB OperStatus value for this network adapter is missing. IP Availability Manager sets a network adapter's OperStatus value to NOTPRESENT when receiving one of the following SNMP errors: SNMP_EXP_NOSUCHOBJECT SNMP_ERR_NOSUCHNAME SNMP_EXP_NOSUCHINSTANCE SNMP_EXP_ENDOFMIB • UNKNOWN indicates that this network adapter has yet to be polled.	Enum: • UP • DOWN • TESTING • OTHER • DORMANT • NOTPRESENT • UNKNOWN
PortType	Applicable to Port only: Type of port represented by this Port.	Enum: • TRUNK • ACCESS (default)

Table 3-6 Attributes for network adapter (continued)

Attribute	Description	Allowed values
SystemName	Name of the system containing this network adapter; for example: 10.9.1.108	String
SystemObjectID	System object identifier associated with the vendor of the system containing this network adapter; for example: .1.3.6.1.4.1.311.1.1.3.1.1	String
SystemType	Type of system containing this network adapter; for example: SWITCH	Enum: • HOST • ROUTER • SWITCH • HUB • SERVER • BRIDGE • REPEATER • PROBE • OTHER • TERMINALSERVER
Type	Type of network adapter, distinguished according to the physical/link protocols immediately "below" the network layer in the protocol stack.	Enum: • ATMFUNI • ARCNET • SONET • HIPPI • MODEM • V36 • IEEE1394 • IFGSN • ATMVIRTUAL (and many more)

Faults for network adapter

IP Performance Manager detects the following faults for ports, interfaces, and subinterfaces:

- HighBroadcastRate
- HighDiscardRate
- HighQueueDropRate
- HighCollisionRate
- HighUtilization
- HighErrorRate

Note: To enable subinterface performance analysis, see the Generic Interface/Port Performance setting description or the Ethernet Interface/Port Performance setting description in Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide*.

When any of these faults occur, IP Performance Manager generates the appropriate system-level exception notification.

HighBroadcastRate fault

When a HighBroadcastRate fault occurs, IP Performance Manager generates a PerformanceException for the affected system or VLAN. IP Performance Manager detects a HighBroadcastRate fault when the input packet broadcast percentage exceeds the BroadcastThreshold. The input packet broadcast percentage calculates the percentage of total capacity that was used to receive broadcast packets.

The BroadcastThreshold is contained in both the Generic Interface/Port Performance setting and the Ethernet Interface/Port Performance setting. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* describes these settings.

HighDiscardRate fault

A HighDiscardRate fault results in a PerformanceException for the affected system or VLAN. IP Performance Manager detects a HighDiscardRate fault when one of the following conditions occurs:

- The percentage of discarded input packets is greater than the DiscardThreshold. The input packet discard percentage is derived by dividing the rate of input packets discarded by the rate of packets received.
- The percentage of discarded output packets is greater than the DiscardThreshold. The output packet discard percentage is derived by dividing the rate of output packets discarded by the rate of packets sent.

For either condition, the input or output packet queued rate must be greater than the minimum packet rate.

The DiscardThreshold is contained in both the Generic Interface/Port Performance setting and the Ethernet Interface/Port Performance setting. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* describes these settings.

HighQueueDropRate fault

A HighQueueDropRate fault results in a PerformanceException for the affected system or VLAN. IP Performance Manager detects a HighQueueDropRate fault when the number of packets discarded due to input or output queue overflow exceeds the QueueDropThreshold. The input (or output) queue overflow is derived by dividing the number of packets designated to be sent (or received) that were discarded due to queue overflow by the total number of packets in the queue.

This threshold is contained in both the Generic Interface/Port Performance setting and the Ethernet Interface/Port Performance setting. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* describes these settings.

HighCollisionRate fault

A HighCollisionRate fault results in a PerformanceException for the affected system or VLAN. IP Performance Manager detects a HighCollisionRate fault when the rate of collisions exceeds the CollisionThreshold.

This threshold is contained in the Ethernet Interface/Port Performance setting. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* describes this setting.

Note: This fault is detected only for Ethernet adapters.

HighUtilization fault

A HighUtilization fault for a network adapter results in a PerformanceException for the affected system or VLAN. IP Performance Manager detects a HighUtilization fault when the current utilization is greater than the UtilizationThreshold configured for this network adapter.

Port and Interface objects represent the connections between switches and routers, respectively, and the wires or other physical media that lead to other systems. Two fundamental properties that describe a Port or Interface are its speed and its duplex mode:

- The speed of a port or interface is the maximum rate at which it can transport information. Speed is usually expressed in bits per second (bps).
- The duplex mode for a port or interface controls whether data transmission is full-duplex or half-duplex. With full-duplex transmission, both ends of a network connection can send data simultaneously. With half-duplex transmission, only one end of a network connection can send data at a time. "Duplex-mode discovery for network adapters" on page 3-22 provides more information about how IP Performance Manager determines duplex mode for a port or interface.

The current utilization of a port or interface is the ratio, expressed as a percentage, of the total number of bits sent over some interval over the total number of bits that could have been sent in that same interval. A value of 100% means that, had more traffic arrived in that period, some would have been dropped due to lack of capacity.

As an example, suppose a port with a speed of 100,000 bps sent 450,000 bits and received 400,000 bits in the last 10 seconds. To compute the current utilization, IP Performance Manager first needs to know whether the system is full- or half-duplex:

- If the system is full-duplex, the limiting factor is the more heavily loaded (outgoing or incoming) wire. For a full-duplex, 100,000 bps system, each wire can carry 1,000,000 bits in 10 seconds. The outgoing wire carried 450,000 bits, or 45% of the theoretical capacity; the incoming wire carried 400,000 bits, or 40% of capacity. IP Performance Manager defines the current utilization as 45%, the higher percentage.
- If the system is half-duplex, the total traffic has to go over a single wire. In this case, a total of 850,000 bits moved over the wire, which could have carried 1,000,000. Hence, the current utilization is 85%.

IP Performance Manager reports the HighUtilization fault when the current utilization exceeds the UtilizationThreshold configured for the port or interface.

This threshold is contained in both the Generic Interface/Port Performance setting and the Ethernet Interface/Port Performance setting. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* describes these settings.

HighErrorRate fault

A HighErrorRate fault results in an ErrorException for the affected system or VLAN. IP Performance Manager detects a HighErrorRate fault when one of the following conditions occurs.

- The percentage of input packet errors is greater than the ErrorThreshold configured for this network adapter. The input packet error percentage is derived by dividing the number of input packets in error by the total number of input packets. The result of this calculation is expressed as a percentage and compared to the ErrorThreshold.

- The percentage of output packet errors is greater than the ErrorThreshold configured for this network adapter. The output packet error percentage is derived by dividing the number of output packets in error by the total number of output packets. The result of this calculation is expressed as a percentage and compared to the ErrorThreshold.

For either condition, the input or output packet rate must be greater than or equal to the minimum packet rate. The minimum packet rate is derived by dividing the speed of the network adapter by the value of its maximum transfer unit (MTU) and multiplying the result by the ErrorTrafficThreshold.

For more information regarding a HighErrorRate fault, select the Details tab in the Notification Properties dialog for the HighErrorRate notification to view the breakdown by type of error; for example, cyclic redundancy check (CRC) or frame alignment. The type of information available is dependent on the system's MIB.

The ErrorThreshold and the ErrorTrafficThreshold are contained in the Generic Interface/Port Performance setting and the Ethernet Interface/Port Performance setting. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* describes these settings.

Duplex-mode discovery for network adapters

The duplex mode setting for a network adapter determines whether IP Performance Manager monitors the adapter for HighUtilization faults:

- If duplex mode is full-duplex or half-duplex, IP Performance Manager calculates current utilization for the adapter and monitors the adapter for HighUtilization faults.
- If duplex mode is unspecified, IP Performance Manager neither calculates current utilization for the network nor monitors the adapter for HighUtilization faults.

A network adapter's duplex mode setting is specified in the DuplexMode attribute, and its duplex mode source setting—the means by which the duplex mode is determined for the adapter—is specified in the DuplexSource attribute. The default value for DuplexMode is UNSPECIFIED, and the default value for DuplexSource is NONE.

Determining duplex-mode

IP Performance Manager reads the following MIBs to determine the duplex mode value for a network adapter:

1. Checks for a duplex mode value in the enterprise-specific MIB.

   If found and the value is full-duplex or half-duplex, sets DuplexMode to FULLDUPLEX or HALFDUPLEX and sets DuplexSource to ENTERPRISE_MIB. If no value is found or the found value is not understood, IP Performance Manager continues to the next step.

2. Checks for a duplex mode value in the ETHERLIKE- MIB.

   If found and the value is full-duplex or half-duplex, sets DuplexMode to FULLDUPLEX or HALFDUPLEX and sets DuplexSource to ETHERLIKE_MIB. If no value is found or the found value is not understood, IP Performance Manager continues to the next step.

3. Checks for a duplex mode value in the neighbor MIB.

   If found and the value is full-duplex or half-duplex, sets DuplexMode to FULLDUPLEX or HALFDUPLEX for both local and remote ports and sets DuplexSource to NEIGHBOR_MIB. If no value is found or the found value is not understood, IP Performance Manager continues to the next step.

4. Checks the value of ICF_TopologyManager::ICF-TopologyManager::DuplexAssumed.

   The value of this attribute is the value of the DuplexAssumed parameter in the discovery.conf file. At this point in the search for a duplex mode setting, IP Performance Manager uses the DuplexAssumed value to determine the values for the network adapter's DuplexMode and DuplexSource attributes.

Understanding the DuplexAssumed parameter

The DuplexAssumed parameter in the discovery.conf file controls how to set the duplex mode for network adapters in the topology. Valid values are TRUE and FALSE. The default value is FALSE.

- A value of TRUE indicates that duplex mode is assumed for all network adapters regardless of whether duplex mode can be determined by checking the MIBs.
- A value of FALSE indicates that duplex mode is set only for the network adapters for which duplex mode can be determined by checking the MIBs.

A value of TRUE means that IP Performance Manager will monitor all network adapters in the topology for HighUtilization faults. For any network adapter whose duplex mode cannot be determined by checking the MIBs, IP Performance Manager sets the adapter's DuplexMode attribute to FULLDUPLEX and its DuplexSource attribute to ASSUMED. The one exception is the 10 megabit (Mb) Ethernet adapter, for which IP Performance Manager sets the adapter's DuplexMode attribute to HALFDUPLEX.

Note: Be aware that monitoring all network adapters in the topology requires considerable system resources. Ensure that your server is sized properly to accommodate the size of your environment, as described in the *EMC Smarts IP Management Suite Deployment Guide*.

A value of FALSE means that IP Performance Manager will monitor *only* those network adapters that can be determined as full-duplex or half-duplex by reading the Enterprise MIB, ETHERLIKE-MIB, and Neighbor MIB. Any network adapter having an unspecified duplex mode setting will be ignored.

Chapter 2, "Setting Configuration Parameters," in the *EMC Smarts IP Management Suite Configuration Guide* provides information about the discovery.conf file.

Using the setDuplexMode command

You can use the setDuplexMode command to overwrite the DuplexMode attribute value for an individual network adapter. For example, if the value of the DuplexMode attribute for a network adapter is UNSPECIFIED and you know that the duplex mode is FULLDUPLEX or HALFDUPLEX, you can use the setDuplexMode command to set the duplex mode, thereby enabling the adapter for HighUtilization monitoring. You invoke the setDuplexMode command through the dmctl command line utility from the BASEDIR/smarts/bin directory.

The following command example sets the DuplexMode attribute value to HALFDUPLEX for a network adapter named Interface::IF-moto-gw/2:

```
dmctl -s INCHARGE-PM invoke Interface::IF-moto-gw/2
   setDuplexMode HALFDUPLEX
```

Note: The example command line assumes that the INCHARGE-PM instance is attached to the default Broker "localhost:426." If the INCHARGE-PM instance were attached to an alternate Broker, the option -b <broker> would be required in the command line to identify the host and port (<host:port>) location of the alternate Broker.

In addition, when you manually assign a value to the DuplexMode attribute for a network adapter, EMC Smarts software automatically assigns a value of USER_CHANGED to the DuplexSource attribute for the adapter.

The following command example verifies the DuplexMode attribute setting for Interface::IF-moto-gw/2:

```
dmctl -s INCHARGE-PM get Interface::IF-moto-gw/2::DuplexMode
```

In this series of examples, the returned value is HALFDUPLEX.

The following command example verifies the DuplexSource attribute setting for Interface::IF-moto-gw/2:

```
dmctl -s INCHARGE-PM get Interface::IF-moto-gw/2::DuplexSource
```

In this series of examples, the returned value is USER_CHANGED.

Any change that you make to the DuplexMode attribute of a network adapter is not overwritten when the associated system is rediscovered unless IP Performance Manager discovers a duplex mode value for the adapter when checking the MIBs during the rediscovery. A MIB-determined duplex mode value takes precedence over a manually set duplex mode value.

In addition to using the dmctl command line utility to invoke the setDuplexMode command, you can also use ASL scripts and C++, Java, and Perl API.

Other network adapters that are not monitored

In addition to an unspecified duplex mode setting, the following properties also determine whether a network adapter is monitored for utilization:

- If the network adapter is unmanaged, it is not monitored.
- If the network adapter uses the description of “*Vlan” for a Cisco device, it is not monitored.
- If the interface is a subinterface, it is not monitored unless subinterface performance analysis is enabled, which is explained in the Generic Interface/Port Performance setting or the Ethernet Interface/Port Performance setting. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* describes these settings.

Processor

A processor, or central processing unit (CPU), controls the operation of a system. A system can have one or more CPUs. IP Performance Manager monitors each CPU to measure its utilization whenever a system's CPU usage information is available.

IP Performance Manager performs performance analysis on the Processor object type.

Attributes for Processor

Table 3-7 lists some key attributes for Processor.

Table 3-7 Attributes for Processor

Attribute	Description	Allowed values
CurrentUtilization	Current utilization of this Processor as reported by the instrumentation. The utilization is expressed as a percentage of the overall capacity of the Processor; for example: 9	Integer
DeviceID	Address or other identifying information to uniquely name this Processor; for example: 1	String
DisplayName	Name, as shown in the Global Console, of this Processor; for example: PSR-10.9.1.108/1 [Intel]	String
Name	Name, as known in the modeled topology, of this Processor; for example: PSR-10.9.1.108/1	String
SystemName	Name of the system containing this Processor; for example: 10.9.1.108	String

Faults for Processor

IP Performance Manager detects the HighUtilization fault for Processor. When a HighUtilization fault occurs, IP Performance Manager generates a system ResourceException for the affected system.

A HighUtilization fault indicates that the processor utilization exceeds the ProcessorUtilizationThreshold. The threshold for processor utilization is contained in the Processor and Memory setting, described in Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide*.

Memory

Memory is the working space associated with a system's processor, used to run programs and process data (for example, the RAM on a PC). IP Performance Manager monitors a processor's memory as well as any other memory pools that the system supports (for example, a pool of I/O memory).

IP Performance Manager performs performance analysis on the Memory object type.

Attributes for Memory

Table 3-8 lists some key attributes for Memory.

Table 3-8 Attributes for Memory

Attribute	Description	Allowed values
BufferMissPct	Number of buffer misses for this Memory, expressed as a percentage of the total number of buffer requests; for example: 0.0	Numeric (float)
BufferMissPct	Number of buffer misses for this Memory, expressed as a percentage of the total number of buffer requests; for example: 0.0	Numeric (float)
BufferUtilizationPct	Number of buffers used for this Memory, expressed as a percentage of the total number of buffers; for example: 0.0	Numeric (float)
DeviceID	Address or other identifying information to uniquely name this Memory; for example: 3	String
DisplayName	Name, as shown in the Global Console, of this Memory; for example: MEM-10.9.1.108/3 [Virtual Memory]	String
FreeMemory	Amount of free memory in kilobytes available for this Memory; for example: 185024	Integer
LargestFreeBuffer	Largest number of contiguous kilobytes that are currently unused for this Memory; for example: 93656	Integer
Name	Name, as known in the modeled topology, of this Memory; for example: MEM-10.9.1.108/3	String

Table 3-8 **Attributes for Memory (continued)**

Attribute	Description	Allowed values
SystemName	Name of the system containing this Memory; for example: 10.9.1.108	String
TotalBufferAllocationFailures	Number of buffer allocation failures due to lack of memory experienced in the last polling cycle for this Memory; for example: 0	Integer
TotalMemory	Amount of memory present in this Memory as reported by the instrumentation; for example: 2521984	Integer

Faults for Memory

Table 3-9 lists the faults detected for Memory.

Table 3-9 **Faults and related thresholds for Memory**

Memory Fault	Description	Threshold
ExcessiveFragmentation	Indicates that the system memory is highly fragmented and exceeds the Memory Fragmentation Threshold.	MemoryFragmentationThreshold
HighBufferMissRate	Indicates that the rate of buffer misses exceeds the Memory Buffer Miss Threshold. Drill down on this event notification in the Notification Log to view the percentage breakdown of buffer misses into the types of misses (such as small, medium, big, large, and huge buffer misses).	MemoryBufferMissThreshold
HighBufferUtilization	Indicates that the number of buffers used exceeds the Memory Buffer Utilization Threshold. Drill down on this event notification in the Notification Log to view the percentage of small, medium, big, large, and huge buffers used.	MemoryBufferUtilizationThreshold
InsufficientFreeMemory	Indicates that the system is running out of memory resources and that the percentage of free memory falls below the Free Memory Threshold. This fault is also reported if there has been a failure to allocate a buffer due to lack of memory.	FreeMemoryThreshold

When a memory-related fault occurs, IP Performance Manager generates a system ResourceException for the affected system. The thresholds for memory faults are listed in the Processor and Memory setting, described in Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide*.

Disk

A disk represents a physical device, installed on a host system, that contains filesystems. The device could be a hard disk, a floppy disk, an optical disk, or other kind of disk. IP Server Performance Manager monitors each disk to verify that it is operational.

IP Server Performance Manager performs performance analysis on the Disk object type.

Note: Disk monitoring and analysis is available only through IP Server Performance Manager.

Attributes for Disk

Table 3-10 lists some key attributes for Disk.

Table 3-10 Attributes for Disk

Attribute	Description	Allowed values
Access	Indicates whether this Disk is readable and writable or only readable. • readWrite indicates that this Disk can be read and written. • readOnly indicates that this Disk can be read but not written.	Enum: • readOnly • readWrite
Capacity	Size in kilobytes for this Disk; for example: 3395069 If the media is removable and is currently removed, this value should be 0.	Integer
DeviceID	Address or other identifying information to uniquely name this Disk; for example: 5	String
DisplayName	Name, as shown in the Global Console, of this Disk; for example: DISK-10.9.1.108/5 [Fixed Disk]	String
Media	Indication of the type of media used in this Disk. • other indicates that the media used in this Disk is of type other. • unknown_media indicates that the media type used in this Disk is not known. • hardDisk indicates that the media used in this Disk is a hard disk. • floppyDisk indicates that the media used in this Disk is a floppy disk. • opticalDiskrom indicates that the media used in this Disk is an optical disk ROM. • opticalDiskworm indicates that the media used in this Disk is an optical disk WORM. • opticalDiskrw indicates that the media used in this Disk is an optical disk RW. • ramDisk indicates that the media used in this Disk is a RAM disk.	Enum: • other • unknown_media • hardDisk • floppyDisk • opticalDiskrom • opticalDiskworm • opticalDiskrw • ramDisk

Table 3-10 Attributes for Disk (continued)

Attribute	Description	Allowed values
Name	Name, as known in the modeled topology, of this Disk; for example: DISK-10.9.1.108/5	String
Removable	TRUE if this Disk can be removed; for example, a floppy disk. FALSE if this Disk cannot be removed; for example, a hard disk.	Boolean: true or false
Status	Current status of this Disk as reported by the instrumentation.	Enum: • running
SystemName	Name of the system containing this Disk; for example: 10.9.1.108	String

Faults for Disk

IP Server Performance Manager detects the OperationallyDown fault for Disk. When a OperationallyDown fault occurs, IP Server Performance Manager generates a system OperationalException for the affected host system.

An OperationallyDown fault indicates that the disk is not operational. Possibly the disk was removed from the host system, or an error occurred when the operating system attempted to access the disk. No threshold is associated with an OperationallyDown disk.

FileSystem

A filesystem is a logical representation of the data within a disk or across disks. FAT32, NTFS, and LinuxExt2 are examples of filesystems. IP Server Performance Manager monitors each filesystem to measure its utilization.

IP Server Performance Manager performs performance analysis on the FileSystem object type.

Note: Filesystem monitoring and analysis is available only through IP Server Performance Manager.

Attributes for FileSystem

Table 3-11 lists some key attributes for FileSystem.

Table 3-11 Attributes for FileSystem

Attribute	Description	Allowed values
AvailableSpace	Total free space in kilobytes on this FileSystem; for example: 22812526	Integer
DeviceID	Address or other identifying information to uniquely name this FileSystem; for example: 3	String
DisplayName	Name, as shown in the Global Console, of this FileSystem; for example: FS-10.9.130.119/2 [C:\ Label:W2K Serial Number 70be674b]	String
Mounted	TRUE if the FileSystem is mounted. (FALSE if the FileSystem is not mounted.)	Boolean: true or false
Name	Name, as known in the modeled topology, of this FileSystem; for example: FS-10.9.130.119/3	String
Root	Pathname defining the root of this FileSystem; for example: C:\ Label:W2K Serial Number 70be674b	String
StorageSize	Total size in kilobytes of this FileSystem; for example: 36981629	Integer
SystemName	Name of the system containing this FileSystem; for example: 10.9.130.119	String
UtilizationPct	Percentage of space currently being used by this FileSystem; for example: 38.313896	Numeric (float)

Faults for FileSystem

IP Server Performance Manager detects the HighUtilization fault for FileSystem. When a HighUtilization fault occurs, IP Server Performance Manager generates a system ResourceException for the affected host system.

A HighUtilization fault indicates that the filesystem utilization exceeds the MaxUtilizationPct threshold..

PowerSupply

A power supply provides power to a system. A system can have one or more power supplies. IP Performance Manager monitors the power supply's status to determine whether a system's power supply is functioning properly.

IP Performance Manager performs performance analysis on the PowerSupply object type.

Attributes for PowerSupply

Table 3-12 lists some key attributes for PowerSupply.

Table 3-12 Attributes for PowerSupply

Attribute	Description	Allowed values
DeviceID	Address or other identifying information to uniquely name this PowerSupply; for example: 1	String
DisplayName	Name, as shown in the Global Console, of this PowerSupply; for example: PWR-10.9.252.2/1 [Power Supply 1]	String
Name	Name, as known in the modeled topology, of this PowerSupply; for example: PWR-10.9.252.2/1	String
Status	Current state of this PowerSupply as reported by the instrumentation. • OK indicates that the observed power supply status is acceptable. • WARNING indicates that the observed power supply status is unacceptable but that the operation of the system can continue. • CRITICAL indicates that the observed power supply status is unacceptable and that operation of the system might cease as a result. • SHUTDOWN indicates that the power supply has been shut down. • OTHER indicates that the state of the power supply is not OK, WARNING, CRITICAL, or SHUTDOWN. • UNKNOWN indicates that the power supply has yet to be polled.	Enum: • OK • WARNING • CRITICAL • SHUTDOWN • OTHER • UNKNOWN
SystemName	Name of the system containing this PowerSupply; for example: 10.9.252.2	String

Faults for PowerSupply

IP Performance Manager detects the PowerSupply StateNotNormal fault for power supplies. When a power supply fault occurs, IP Performance Manager generates a system PowerSupplyException for the affected system.

A PowerSupply StateNotNormal fault indicates that the power supply is in the WARNING or CRITICAL state. The power supply state can be one of four states:

- NORMAL
- WARNING
- CRITICAL
- SHUTDOWN

VoltageSensor

A voltage sensor is a device that measures the voltage of the power supply. IP Performance Manager performs performance analysis on the VoltageSensor object type.

Attributes for VoltageSensor

Table 3-13 lists some key attributes for VoltageSensor.

Table 3-13 Attributes for VoltageSensor

Attribute	Description	Allowed values
CurrentValue	Current value in volts of this VoltageSensor as reported by the instrumentation; for example: 3.3 V	Numeric (float)
DeviceID	Address or other identifying information to uniquely name this VoltageSensor; for example: 1	String
DisplayName	Name, as shown in the Global Console, of this VoltageSensor; for example: VOLT-ca-hsiaoy.corp.emc.com/1 [Voltage 1]	String
HighThreshold	Current high threshold value in volts of this VoltageSensor as reported by the instrumentation; for example: 3.63 V	Numeric (float)
LowThreshold	Current low threshold value in volts of this VoltageSensor as reported by the instrumentation; for example: 2.97 V	Numeric (float)

Table 3-13 Attributes for VoltageSensor (continued)

Attribute	Description	Allowed values
Name	Name, as known in the modeled topology, of this VoltageSensor; for example: VOLT-ca-hsiaoy.corp.emc.com/1	String
Status	Current state of this VoltageSensor as reported by the instrumentation. • OK indicates that the observed voltage is acceptable. • WARNING indicates that the observed voltage is unacceptable but that the operation of the system can continue. • CRITICAL indicates that the observed voltage is unacceptable and that operation of the system might cease as a result. • SHUTDOWN indicates that the power supply has been shut down or that this VoltageSensor has been shut down. • OTHER indicates that the state of this VoltageSensor is not OK, WARNING, CRITICAL, or SHUTDOWN. • UNKNOWN indicates that this VoltageSensor has yet to be polled.	Enum: • OK • WARNING • CRITICAL • SHUTDOWN • OTHER • UNKNOWN
SystemName	Name of the system containing this VoltageSensor; for example: ca-hsiaoy.corp.emc.com	String

Faults for VoltageSensor

Table 3-14 lists the faults detected for VoltageSensor.

Table 3-14 Faults and related thresholds for VoltageSensor

Voltage Fault	Description	Threshold
OutOfRange	Indicates that the voltage for this system is outside the normal operating range and exceeds the RelativeVoltageThreshold.	RelativeVoltageThreshold
StateNotNormal	Indicates that the voltage sensor test point for this system is in the CRITICAL or WARNING state. The voltage sensor state can be one of four states: NORMAL, WARNING, CRITICAL, or SHUTDOWN.	N/A

When a voltage-related fault occurs, IP Performance Manager generates a system PowerSupplyException for the affected system.

TemperatureSensor

A temperature sensor is a physical package that describes the capabilities and management of temperature-related numeric devices. A temperature sensor is represented by the TemperatureSensor logical device class.

IP Performance Manager performs performance analysis on the TemperatureSensor object type.

Attributes for TemperatureSensor

Table 3-15 lists some key attributes for TemperatureSensor.

Table 3-15 Attributes for TemperatureSensor

Attribute	Description	Allowed values
CurrentValue	Current value in degrees centigrade (C) of this TemperatureSensor as reported by the instrumentation; for example: 45 C	Integer
DeviceID	Address or other identifying information to uniquely name this TemperatureSensor; for example: 1	String
DisplayName	Name, as shown in the Global Console, of this TemperatureSensor; for example: TEMP-10.9.252.2/1 [Chassis Temperature Sensor]	String
HighThreshold	Current high threshold value in degrees C of this TemperatureSensor as reported by the instrumentation; for example: 85.5 C	Numeric (float)

Table 3-15 Attributes for TemperatureSensor (continued)

Attribute	Description	Allowed values
Name	Name, as known in the modeled topology, of this TemperatureSensor; for example: TEMP-10.9.252.2/1	String
Status	Current state of this TemperatureSensor as reported by the instrumentation. • OK indicates that the observed temperature is acceptable. • WARNING indicates that the observed temperature is unacceptable but that the operation of the system can continue. • CRITICAL indicates that the observed temperature is unacceptable and that operation of the system might cease as a result. • SHUTDOWN indicates that the fan or chassis has been shut down or that this TemperatureSensor has been shut down. • OTHER indicates that the state of this TemperatureSensor is not OK, WARNING, CRITICAL, or SHUTDOWN. • UNKNOWN indicates that this TemperatureSensor has yet to be polled. • MARGINAL indicates that the observed temperature is unacceptable, but that the operation of the system can continue.	Enum: • OK • WARNING • CRITICAL • SHUTDOWN • OTHER • UNKNOWN • MARGINAL
SystemName	Name of the system containing this TemperatureSensor; for example: qa-gw3.smarts.com	String

Faults for TemperatureSensor

Table 3-16 lists the faults detected for TemperatureSensor.

Table 3-16 Faults and related thresholds for TemperatureSensor

Temperature Fault	Description	Threshold
OutOfRange	Indicates that the temperature for this system is outside the normal operating range and exceeds the RelativeTemperatureThreshold.	RelativeTemperatureThreshold
StateNotNormal	Indicates that the temperature sensor for this system is in the WARNING or CRITICAL states. The temperature sensor state can be NORMAL, WARNING, or CRITICAL.	N/A

When a temperature-related fault occurs, IP Performance Manager generates a system TemperatureException for the affected system.

Thresholds for temperature faults are contained in the Environment threshold setting. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* describes this setting.

Fan

A fan is a cooling device that blows air through the chassis of a system to cool its circuitry. A system can have one or more fans. IP Performance Manager monitors a fan's status to determine whether a fan is functioning properly.

IP Performance Manager performs performance analysis on the Fan object type.

Attributes for Fan

Table 3-17 lists some key attributes for Fan.

Table 3-17 Attributes for Fan

Attribute	Description	Allowed values
DeviceID	Address or other identifying information to uniquely name this Fan; for example: 1	String
DisplayName	Name, as shown in the Global Console, of this Fan; for example: FAN-10.9.252.2/1 [Chassis Fan Tray 1]	String
Name	Name, as known in the modeled topology, of this Fan; for example: FAN-10.9.252.2/1	String
Status	Current state of this Fan as reported by the instrumentation. • OK indicates that the fan is operating normally. • WARNING indicates that the fan is at warning status. • CRITICAL indicates that the fan is at critical status. • SHUTDOWN indicates that the fan has been shut down. • OTHER indicates that the state of the fan is not OK, WARNING, CRITICAL, or SHUTDOWN. • UNKNOWN indicates that the fan has yet to be polled.	Enum: • OK • WARNING • CRITICAL • SHUTDOWN • OTHER • UNKNOWN
SystemName	Name of the system containing this Fan; for example: 10.9.252.2	String

Faults for Fan

IP Performance Manager generates a StateNotNormal fault for Fan. When a fan fault occurs, IP Performance Manager generates a system TemperatureException for the affected system.

A Fan StateNotNormal fault indicates that the fan is in the WARNING or CRITICAL state. The fan state can be one of NORMAL, WARNING, or CRITICAL.

DuplicateIP

A DuplicateIP object represents two or more instances of the same IP address discovered in the managed network environment.

Attributes for DuplicateIP

Table 3-18 lists some key attributes for DuplicateIP.

Table 3-18 Attributes for DuplicateIP

Attribute	Description	Allowed values
Address	IP address of this DuplicateIP; for example: 10.0.0.4	String
DisplayName	Name, as shown in the Global Console, of this DuplicateIP; for example: 10.0.0.4 [hagg-01-lo0-0.west.twtelecom.net]	String
DuplicatedBySystems	List of systems on which the IP address for this DuplicateIP is duplicated.; for example: hagg-01-lo0-0.west.twtelecom.net, cpe-66-66-65-1.rochester.res.rr.com, ...	String
InterfaceAdminStatus	Reflects the current administrative status of the interface underlying this DuplicateIP. • UP indicates that the interface is administratively enabled. • DOWN indicates that the interface is administratively disabled. • TESTING indicates that the interface is in testing mode. • OTHER indicates that the interface is in an unknown state. • NOTPRESENT indicates that the MIB AdminStatus value for the interface is missing. • UNKNOWN indicates that the interface has yet to be polled. When the value of the interface's InterfaceAdminStatus is UP, the value of InterfaceOperStatus determines the state of the interface. Otherwise, the value of InterfaceAdminStatus determines the state of the interface.	Enum: • UP • DOWN • TESTING • OTHER • NOTPRESENT • UNKNOWN
InterfaceMode	Indicates the intended purpose of the interface underlying this DuplicateIP: normal, backup, or dial-on-demand.	Enum: • NORMAL • BACKUP • ONDEMAND
InterfaceName	Name, as shown in the Global Console, of the interface underlying this DuplicateIP; for example: IF-hagg-01-lo0-0.west.twtelecom.net/14 [fxp1.0] [10.0.0.4]	String

Table 3-18 Attributes for DuplicateIP (continued)

Attribute	Description	Allowed values
InterfaceOperStatus	Reflects the current operational status of the interface underlying this DuplicateIP. • UP indicates that the interface is operationally up. • DOWN indicates that the interface is operationally down. • TESTING indicates that the interface is in testing mode. • OTHER indicates that the interface is in an unknown state. • DORMANT indicates that the interface is waiting for an external action to occur before becoming active. • NOTPRESENT indicates that the MIB OperStatus value for the interface is missing. • UNKNOWN indicates that the interface has yet to be polled.	Enum: • UP • DOWN • TESTING • OTHER • DORMANT • NOTPRESENT • UNKNOWN
InterfaceType	Type of interface underlying this DuplicateIP, distinguished according to the physical/link protocols immediately "below" the network layer in the protocol stack.	Enum: • ATMFUNI • ARCNET • SONET • HIPPI • MODEM • V36 • IEEE1394 • IFGSN • ATMVIRTUAL (and many more)

Table 3-18 Attributes for DuplicateIP (continued)

Attribute	Description	Allowed values
IPStatus	Reflects the current state of this DuplicateIP as reported by the instrumentation. **Note:** For a DuplicateIP, this attribute is set to UNKNOWN. • OK indicates that the IP interface is responding to ICMP pings. • NETUNREACHABLE indicates that the IP network is unreachable. • HOSTUNREACHABLE indicates that the host is unreachable. • PROTOCOLUNREACHABLE indicates that the ICMP protocol is unreachable. • PORTUNREACHABLE indicates that the port is unreachable. • NEEDFRAGUNREACHABLE indicates that the destination was unreachable because fragmentation was needed and do not fragment was set. • SRCFAILEDUNREACHABLE indicates that the source route failed. • DESTNETUNREACHABLE indicates that the destination network is unknown. • DESTHOSTUNREACHABLE indicates that the destination host is unknown. • ISOLATEDUNREACHABLE indicates that the source host is isolated. • AUTHNETUNREACHABLE indicates that communication with the destination network is administratively prohibited. • AUTHHOSTUNREACHABLE indicates that communication with the destination host is administratively prohibited. • NETSVCUNREACHABLE indicates that the destination network is unreachable for this type of service. • HOSTSVCUNREACHABLE indicates that the destination host is unreachable for this type of service. • TIMEXCEEDINTRANS indicates that the Time to Live (TTL) was exceeded in transit. • TIMEXCEEDREASS indicates that the fragment reassembly time was exceeded. • TIMEDOUT indicates that the last ICMP ping timed out. • OTHER indicates an unspecified error condition occurred. • UNKNOWN indicates an unspecified error condition occurred.	Enum: • OK • NETUNREACHABLE • HOSTUNREACHABLE • PROTOCOLUNREACHABLE • PORTUNREACHABLE • NEEDFRAGUNREACHABLE • SRCFAILEDUNREACHABLE • DESTNETUNREACHABLE • DESTHOSTUNREACHABLE • ISOLATEDUNREACHABLE • AUTHNETUNREACHABLE • AUTHHOSTUNREACHABLE • NETSVCUNREACHABLE • HOSTSVCUNREACHABLE • TIMEXCEEDINTRANS • TIMEXCEEDREASS • TIMEDOUT • OTHER • UNKNOWN
IsInterfaceInstrumented	TRUE if "IP LayeredOver Interface" is instrumented.	Boolean: true or false
Name	Name, as known in the modeled topology, of this DuplicateIP; for example: IP-10.0.0.4	String

Table 3-18 Attributes for DuplicateIP (continued)

Attribute	Description	Allowed values
Netmask	Network mask for this DuplicateIP; for example: 255.0.0.0	String
NetworkNumber	Network number (computed from the Address and Netmask values) for this endpoint; for example: 10.0.0.0	String
Responsive	TRUE if this DuplicateIP is responding to ICMP pings and/or SNMP polls. (FALSE if this DuplicateIP is not responding to ICMP pings and/or SNMP polls.) **Note:** For a DuplicateIP, this attribute is set to FALSE.	Boolean: true or false
SystemName	Name of the system hosting this DuplicateIP; for example: hagg-01-lo0-0.west.twtelecom.net	String
SystemType	Type of system hosting this DuplicateIP; for example: OTHER	Enum: • HOST • ROUTER • SWITCH • PROBE • OTHER

Events for DuplicateIP

IP Performance Manager generates a Duplicate event when it discovers two systems with the same IP address. When this event occurs, IP Performance Manager proceeds as follows:

- Classifies the IP address as a DuplicateIP
- Suspends IP-related analysis for the address
- Generates a Duplicate notification

Chapter 11, "Working with the Topology," in the *EMC Smarts IP Management Suite Discovery Guide* provides information about correcting Duplicate notifications.

A

MIBs Polled and SNMP Traps Processed

This appendix identifies the MIBs and SNMP traps used by IP Performance Manager to diagnose network performance problems. It consists of the following sections:

- Standard SNMP MIBs polled A-2
- Enterprise MIBs polled A-3
- SNMP traps processed A-5

Standard SNMP MIBs polled

IP Performance Manager polls the following standard MIBs:

- ATM-MIB (RFC 2515)
- BRIDGE-MIB (RFC 1493)
- ENTITY-MIB (RFC 2737)
- ETHERLIKE-MIB (RFC 1650)
- FRAME-RELAY-DTE-MIB (RFC 2115)
- HOST-RESOURCES-MIB (RFC 1514)
- IF-MIB (RFC 1573)
- IP-MIB (RFC 2011)
- ISDN-MIB (RFC 2127)
- SNMP MIB-II (RFC 1213)
- VPN-MIB (RFC 1212)

Enterprise MIBs polled

IP Performance Manager polls the following vendor-specific MIBs:

- AI194HUB-MIB
- AI198CLC-MIB
- ALTEON-CHEETAH-SWITCH-MIB
- ARROWPOINT-CHASSISMGREXT-MIB
- ATM-FORUM-TC-MIB
- CENTILLION-BRIDGE-MIB
- CENTILLION-IF-EXTENSIONS-MIB
- CENTILLION-FDB-MIB
- CISCO-2900XL-MIB
- CISCO-CPU-MIB
- CISCO-CDP-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENVMON-MIB
- CISCO-FRAME-RELAY-MIB
- CISCO-FRU-CONTROL-MIB
- CISCO-HSRP-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PAGP-MIB
- CISCO-PROCESS-MIB
- CISCO-RF-MIB
- CISCO-RHINO-MIB
- CISCO-STACK-MIB
- CISCO-SYSTEM-EXT-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- OLD-CISCO-CPU-MIB
- OLD-CISCO-ENV-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-MEMORY-MIB
- OLD-CISCO-SYSTEM-MIB
- CNT21-MIB
- CNT241-MIB
- COSINE-ORION-MIB
- CT-CONTAINER-MIB
- CTRON-CHASSIS-MIB
- EXTREME-EDP-MIB

- EXTREME-FDB-MIB
- EXTREME-SYSTEM-MIB
- EXTREME-VLAN-MIB
- Fore-Common-MIB
- Fore-Switch-MIB
- FOUNDRY-SN-AGENT-MIB
- FOUNDRY-SN-SWITCH-GROUP-MIB
- GDCSCM-MIB
- GENERIC-3COM-TRUNK-MIB (A3Com)
- HP-ICF-OID (Hewlett Packard)
- HUAWEI-3COM-OID-MIB
- HUAWEI-LswDEVM-MIB
- JUNIPER-MIB
- LANPLEX-SYSTEM-MIB-1-1-1
- MP-DETOUR-MIB (NEC Corporation)
- ONS15501-MIB (Cisco)
- RAPID CITY
- RBT-MIB (Riverbed)
- REPEATER-REV4-MIB (Cabletron)
- RND-MIB (RAD Network Devices)
- SSG-5000-CHASSIS-MIB (Shasta)
- STRATACOM-MIB
- SW-MIB (BCSI)
- SYNOPTICS-LS-ETHERNET-MIB
- TapeAlert-MIB (Hewlett Packard)
- UNISPHERE-DATA-ERX-SYSTEM-MIB
- Wellfleet-CCT-NAME-MIB
- Wellfleet-GAME-STATS-MIB
- Wellfleet-HARDWARE-MIB
- Wellfleet-IP-MIB
- XYLAN-BASE-MIB

SNMP traps processed

IP Performance Manager processes data found in the following fields of each SNMP trap message:

- Enterprise (the sysObjectID of the agent/object)
- Generic Trap Identifier
- Specific Trap Identifier
- Variable-Bindings
- IP address of the SNMP agent

IP Performance Manager uses trap messages for two purposes:

- Discovery
- Analysis

SNMP traps processed for discovery

A trap message processed for discovery purposes conveys one of the following conditions for a device in the managed network:

- A device, not yet in the modeled topology, was started.
- A device, already in the modeled topology, was equipped with an additional field replaceable unit (FRU) or had an FRU removed; for example, a card was inserted into the device.
- A device, already in the modeled topology, had a TCP connection closed by a remote application; for example, a Telnet session to the device was terminated.

Table A-1 lists the SNMP traps processed by IP Performance Manager for discovery purposes.

Table A-1 SNMP traps processed by IP Performance Manager for discovery

Trap type	Trap name	MIB module
Generic traps	coldStart*	Standard SNMP (RFC 1215 MIB)
	warmStart*	
Enterprise-specific traps for 3Com Corporation	a3ComSysModuleCardInsertEvent**	CB9000-MIB
Enterprise-specific traps for Cisco	cefcFRUInserted**	CISCO-ENTITY-FRU-CONTROL-MIB
	cefcFRURemoved**	
	tcpConnectionClose*	CISCO-GENERAL-TRAPS

* IP Performance Manager processes this trap but takes no action.

** IP Performance Manager places the associated device for this trap on the Pending Devices list.

As indicated in the table, only for a trap message indicating the insertion or removal of a component does IP Performance Manager place the associated device (which is already in the modeled topology) on the Pending Devices list. During the next pending discovery, IP Performance Manager will send SNMP polls to the device to rediscover the device and its components.

SNMP traps processed for analysis

A trap message processed for analysis purposes pertains to a device that has been discovered and therefore is already in the modeled topology. IP Performance Manager extracts the information from the trap message and updates the appropriate device attributes.

Note: IP Performance Manager uses trap messages and the results obtained from periodic SNMP polling to detect network degradations that adversely affect network performance.

Table A-2 lists the SNMP traps processed by IP Performance Manager for analysis purposes.

Table A-2 SNMP traps processed by IP Performance Manager for analysis

Trap type	Trap name	MIB module
Enterprise-specific traps for Cisco	ciscoEnvMonVoltageNotification	CISCO-ENVMON-MIB
	ciscoEnvMonTemperatureNotification	
	ciscoEnvMonFanNotification	
	ciscoEnvMonRedundantSupplyNotification	
	cefcPowerStatusChange	CISCO-ENTITY-FRU-CONTROL-MIB
Enterprise-specific traps for Riverstone Networks	rsEnvirTempExceeded	RIVERSTONE-NOTIFICATIONS-MIB
	rsEnvirTempNormal	
	rsEnvirFanFailed	
	rsEnvirFanRecovered	
	rsEnvirPowerSupplyFailed	
	rsEnvirPowerSupplyRecovered	

B

Network Topology Naming Conventions

This appendix describes the naming conventions used by IP Performance Manager to name the discovered network objects.

- DisplayName and Name attributes B-2
- Naming convention for network objects B-3

DisplayName and Name attributes

Each network object has a unique name, which is defined by the DisplayName and Name attributes for the object (Figure B-1).

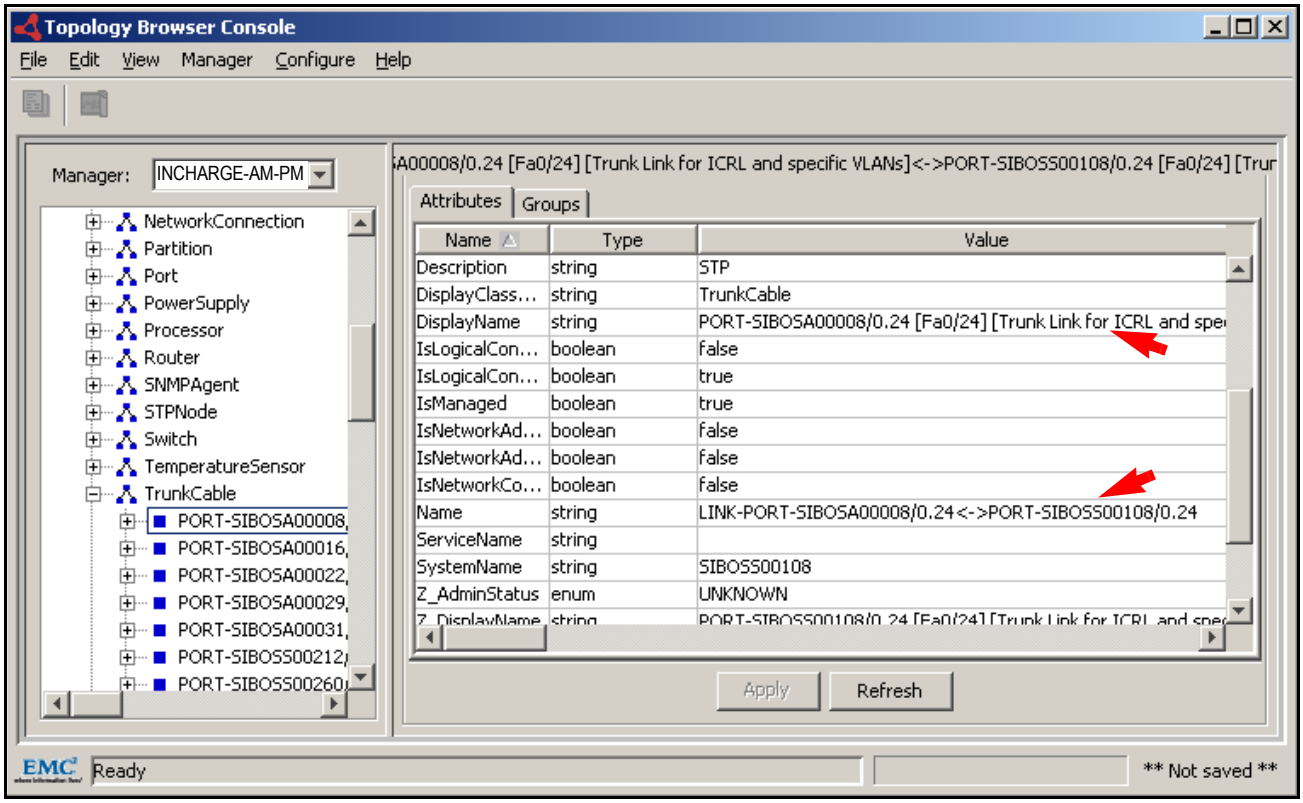

Figure B-1 **DisplayName and Name attributes for a network object**

The name specified in the DisplayName attribute is the name of the object displayed in the Global Console, while the name specified in the Name attribute is the name of the object as known in the Domain Manager's repository. If an object's DisplayName attribute is empty, the display name of the object defaults to the name specified in the object's Name attribute.

The DisplayName and Name attributes of a network object are viewable through a Topology Browser Console attached to the Global Manager or to IP Performance Manager.

Note: To launch a Topology Browser Console from the Global Console, select File > New > Topology Browser Console.

Note: The name specified in an object's DisplayName attribute also appears in the Name attribute of a notification involving that object. Notifications are imported by the Global Manager and displayed in the Notification Log Console.

Naming convention for network objects

For a discovered system, IP Performance Manager uses a consistent naming convention to assign the system and each of its components a unique name. The name assigned to a system is determined by the setting of the NameFormat parameter in the name-resolver.conf file, which is located in the BASEDIR/smarts/conf/discovery directory. The assigned name becomes the value of the system's Name attribute. (Chapter 3, "Name Resolution," in the *EMC Smarts IP Management Suite Discovery Guide* provides information about the name resolution process used to name a system.)

Note: The values of a system's Name attribute and DisplayName attribute may be different, depending on the setting of the DisplayNameFormat parameter in the discovery.conf file. Chapter 2, "Setting Configuration Parameters," in the *EMC Smarts IP Management Suite Configuration Guide* describes the configuration parameters in the discovery.conf file and provides instructions on modifying the parameters.

To name a discovered network object, IP Performance Manager uses the appropriate naming format defined in Table B-1 to name the object. The naming formats shown in the table are the default naming conventions. If no naming format is listed for Display Name, the naming format is the same as the one listed for Name.

Table B-1 Naming formats for discovered network objects

Class Name	Naming Format
Systems	
Bridge	Name: *<IP Address/FQDN>*
	Display Name: Name or *<MIBIISysName>*
FileServer	Name: *<IP Address/FQDN>*
	Display Name: Name or *<MIBIISysName>*
Firewall	Name: *<IP Address/FQDN>*
	Display Name: Name or *<MIBIISysName>*
Host	Name: *<IP Address/FQDN>*
	Display Name: Name or *<MIBIISysName>*
Hub	Name: *<IP Address/FQDN>*
	Display Name: Name or *<MIBIISysName>*
LoadBalancer	Name: *<IP Address/FQDN>*
	Display Name: Name or *<MIBIISysName>*

Table B-1 Naming formats for discovered network objects (continued)

Class Name	Naming Format
MSFC (Multilayer Switch Feature Card)	Name: <*IP Address/FQDN*>
	Display Name: Name or <*MIBIISysName*>
Node	Name: <*IP Address/FQDN*>
	Display Name: Name or <*MIBIISysName*>
Probe	Name: <*IP Address/FQDN*>
	Display Name: Name or <*MIBIISysName*>
Router	Name: <*IP Address/FQDN*>
	Display Name: Name or <*MIBIISysName*>
RSFC (Router Switch Feature Card)	Name: <*IP Address/FQDN*>
	Display Name: Name or <*MIBIISysName*>
RSM (Router Switch Module)	Name: <*IP Address/FQDN*>
	Display Name: Name or <*MIBIISysName*>
Switch	Name: <*IP Address/FQDN*>
	Display Name: Name or <*MIBIISysName*>
TerminalServer	Name: <*IP Address/FQDN*>
	Display Name: Name or <*MIBIISysName*>
Uncertified	Name: <*IP Address/FQDN*>
	Display Name: Name or <*MIBIISysName*>

Table B-1 Naming formats for discovered network objects (continued)

Class Name	Naming Format
Physical packages	
Card	Name: CARD-<*IP Address/FQDN*>/INDEX
	Display Name: NAME [SLOT] [CARDTYPE]
Chassis	Name: CHASSIS-<*IP Address/FQDN*>
	Display Name: CHASSIS-<*IP Address/FQDN*>
Rack	Name: RACK-<*IP Address/FQDN*>
	Display Name: RACK-<*IP Address/FQDN*>
Network adapters	
Interface	Name: IF-<*IP Address/FQDN*>/<*INDEX*>
	Display Name: NAME [SLOT/PORT] [IPLIST] [Interface Description]
Port	Name: PORT-<*IP Address/FQDN/INDEX*>
	Display Name: NAME [SLOT/PORT] [IPLIST] [Port Description]
Device connections	
Cable	Name: LINK-IF-<*IP Address/FQDN*>/<*INDEX*><->PORT-<*IP Address/FQDN*>
	Display Name: NAME [SLOT/PORT] [IPLIST] [Connectivity Description]
NetworkConnection	Name: LINK-IF<*IP Address/FQDN*>
	Display Name: NAME
TrunkCable	Name: LINK-PORT-<*IP Address/FQDN/INDEX*>
	Display Name: NAME [SLOT/PORT] [Link Description]
Service access points	
DLCI	Name: IF-<*IP Address/FQDN*>/<*INDEX*>
	Display Name: NAME [SLOT/PORT] [IPLIST] [Interface Description]
DuplicateIP	Name: IP-<*IP Address*>
	Display Name: NAME-<*IP Address/FQDN*>
DuplicateIPv6	Name: IPv6-<*IPv6 Address*>
	Display Name: <*IPv6 Address*> [*IP Address*]

Table B-1 Naming formats for discovered network objects (continued)

Class Name	Naming Format
DuplicateVPNIP	Name: IP-<*IP Address*>
	Display Name: NAME-<*IP Address/FQDN*>
HSRPEndpoint	Name: HSRP-<*IP Address/FQDN*>/<*HSRPEndpointKey*>
	Display Name: NAME [Group <*GroupNumber*>] [Interface NAME]
IP	Name: IP-<*IP Address*>
	Display Name: IP-<*IP Address*> [SystemName]
IPv6	Name: IPv6-<*IPv6 Address*>
	Display Name: <*IPv6 Address*> [*IP Address*]
MAC	Name: MAC-<*MAC Address*>
	Display Name: <*IP Address/FQDN*> [<*MAC Address*>]
STPNode	Name: STPNODE-<*IP Address/FQDN*>/<*DesignatedPortNumber*>/<*STPNodeKey*>
	Display Name: NAME
VirtualTCP	Name: VIRT-TCP-<*IP Address/FQDN*>:<*PortNumber*>
	Display Name: <*IP Address/FQDN*>:<*PortNumber*>
VPNIP	Name: VPN-IP-<*IP Address/FQDN*>
	Display Name: <*IP Address/FQDN*>
Logical links	
IPNetwork	Name: IPNET-<*IP Address/FQDN*>
	Display Name: <*IP Address/FQDN*>
IPv6Network	Name: IPv6NET-<*IPv6 Address*>
	Display Name: <*IPv6 Address*> [*IP Address*]/<*PrefixLength*>
VLAN	Name: VLAN-<*VLANKey*>
	Display Name: NAME-[VLAN Description]

Table B-1 Naming formats for discovered network objects (continued)

Class Name	Naming Format
VPNIPNetwork	Name: IP-<*IP Address*>
	Display Name: IP-<*IP Address*> [SystemName]
Collections	
Partition	Name: Partition-<*PartitionKey*>
	Display Name: NAME
Management agents	
SNMPAgent	Name: SNMPAgent-<*IP Address/FQDN*>
	Display Name: SNMPAgent-<*IP Address/FQDN*>
Logical devices	
Disk (IP Server Performance Manager only)	Name: DISK-<*IP Address/FQDN/INDEX*>/<*Disk Index*>
	Display Name: NAME [Description]
Fan	Name: FAN-<*IP Address/FQDN*>/<*Device ID*>
	Display Name: NAME [Description]
FileSystem (IP Server Performance Manager only)	Name: FS-<*IP Address/FQDN*>/<*Device ID*>
	Display Name: NAME [Root]
Memory	Name: MEM-<*IP Address/FQDN*>/<*Device ID*>
	Display Name: NAME [Description]
PowerSupply	Name: PWR-<*IP Address/FQDN*>/<*Device ID*>
	Display Name: NAME [Description]
Processor	Name: PSR-<*IP Address/FQDN*>/<*Device ID*>
	Display Name: NAME [Description]
TemperatureSensor	Name: TEMP-<*IP Address/FQDN*>/<*Device ID*>
	Display Name: NAME [Description]
VoltageSensor	Name: VOLT-<*IP Address/FQDN*>/<*Index*>
	Display Name: NAME [VoltageSensor description]

Table B-1 Naming formats for discovered network objects (continued)

Class Name	Naming Format
Redundancy groups	
CardRedundancyGroup	Name: CardRedundancyGroup-<*IP Address/FQDN*>/<*moduleType*>
	Display Name: NAME [Description]
HSRPGroup	Name: HSRP-GROUP-<*IP Address/FQDN*>
	Display Name: NAME [Group <*GroupNumber*>]
NetworkAdapterRedundancyGroup	Name: NetworkAdapterRedundancyGroup-<*IP Address/FQDN*>/<*moduleType*>
	Display Name: NAME [Description]
SystemRedundancyGroup	Name: SystemRedundancyGroup-<*IP Address/FQDN*>/<*moduleType*>
	Display Name: NAME [Description]
KEY FQDN = Fully Qualified Domain Name	

C

Exception, Fault, Event, and Notification Summary

This appendix summarizes the exceptions generated by IP Performance Manager, the faults detected by IP Performance Manager to generate the exceptions, the events detected by IP Performance Manager, and the notifications imported by the Global Manager. It consists of the following sections:

- Exceptions C-2
- Faults and events C-3
- Notifications C-4

Exceptions

Table C-1 lists, on a managed object basis, the exceptions generated by IP Performance Manager.

Table C-1 Exceptions generated by IP Performance Manager

Managed object	Exception	Class of origin
System	Performance	UnitaryComputerSystem
	Error	
	Resource	
	Operational	
	PowerSupply	
	Temperature	
Chassis	BackplaneUtilization	Chassis
VLAN	Performance	VLAN
	Error	

Faults and events

Table C-2 lists, on a managed object basis, the faults (f) detected by IP Performance Manager and the events (e) detected by IP Performance Manager.

Table C-2 Faults and events detected by IP Performance Manager

Managed object	Fault or event	Class of origin
System	DiscoveryError (e)	UnitaryComputerSystem
Chassis	HighBackplaneUtilization (f)	Chassis_Performance
Network adapter (Interface, Port)	HighBroadcastRate (f)	NetworkAdapter_Performance
	HighDiscardRate (f)	
	HighQueueDropRate (f)	
	HighCollisionRate (f)	EthernetAdapter_Performance
	HighUtilization (f)	NetworkAdapter_Performance
	HighErrorRate (f)	
Memory	ExcessiveFragmentation (f)	Memory_Performance
	HighBufferMissRate (f)	
	HighBufferUtilization (f)	
	InsufficientFreeMemory (f)	
	InsufficientFreeMemory_MemoryPool (f)	
Processor	HighUtilization (f)	Processor_Performance
	HighUtilization_avgBusy5 (f)	
	HighUtilization_cpmCPUTotal5min (f)	
Disk (Host only and IP Server Performance Manager only)	OperationallyDown (f)	Disk_Fault
FileSystem (Host only and IP Server Performance Manager only)	HighUtilization (f)	FileSystem_Performance
PowerSupply	StateNotNormal (f)	PowerSupply_Fault
VoltageSensor	OutOfRange (f)	VoltageSensor_Fault
	StateNotNormal (f)	
Temperature	OutOfRange (f)	TemperatureSensor_Fault
	StateNotNormal (f)	
Fan	StateNotNormal (f)	Fan_Fault
DuplicateIP	Duplicate (e)	DuplicateIP
KEY (f) = Fault (e) = Event		

Notifications

All of the faults and events listed in Table C-2 are imported by the Global Manager.

At the Global Manager, all IP Performance Manager faults and errors are known as events (e).

Index

A

AdminStatus attribute 3-16
Analysis 1-3
Attribute
    AdminStatus 3-16
    Certification 3-7
    Chassis
        BackplaneUtilization 3-11
        Status 3-12
    DiscoveryErrorInfo 3-10
    DisplayName B-3
    IPStatus 3-41
    IsFlapping 3-17
    IsUnresponsive 3-7
    Name B-3
    OperStatus 3-18
Attributes
    DisplayName B-2
    Name B-2

B

Backplane utilization exception 3-3, 3-12, C-2
Backplane utilization threshold 3-3, 3-12
BackplaneUtilization attribute 3-11
Bridge 3-6
Broadcast input packets 3-20

C

Calculating current utilization 3-21
Certification attribute 3-7
Chassis 3-3, 3-11
    Backplane utilization exception 3-3, 3-12, C-2
    High backplane utilization 3-3, 3-12
Containment 2-22
Containment dialog box 2-22
    Opening 2-22

D

Device support
    MSFCs 2-15
    Physical routers 2-15
    RSFCs 2-15
    RSMs 2-15
    Virtual routers 2-15
Discarded input packets 3-20
Discarded output packets 3-20
Discovery error 3-10
discovery.conf
    DuplexAssumed 3-23
    MinimumDemandGet 2-11
DiscoveryErrorInfo attribute 3-10
Disk 3-28
    Operationally down 3-29
DisplayName attribute B-2, B-3
dmctl 3-23
    setDuplexMode command 3-23
Domain Manager
    Containment 2-22
Duplex mode setting
    Full 3-21, 3-22
    Half 3-21, 3-22
DuplexAssumed 3-23
Duplicate event 3-42
Duplicate IP
    Duplicate 3-4

E

Edges
    Table of 2-14, 2-15
Environment
    Relative temperature threshold 3-37
    Relative voltage threshold 3-35
Error exception
    System 3-2, 3-9, 3-21, C-2
    VLAN 3-4, 3-14, C-2
Ethernet interface/port performance
    Broadcast threshold 3-20
    Collision threshold 3-20
    Discard threshold 3-20
    Error threshold 3-22
    Error traffic threshold 3-22
    Queue drop threshold 3-20
Event 1-4
    Definition of 1-4
    Duplicate 3-42

Duplicate IP
Duplicate 3-4
Summary table 3-4
System
Discovery error 3-4
Event notification
See Notification
Exception 1-4
Chassis
Backplane utilization 3-3, 3-12, C-2
Definition of 1-4
Summary table 3-2
System
Error 3-2, C-2
Operational 3-3, C-2
Power supply 3-3, C-2
Resource 3-3, C-2
Temperature 3-3, C-2
Excessive memory fragmentation 3-3, 3-27, C-3

F

Fan 3-38
State not normal 3-38
Fault 1-4
Definition of 1-4
Faults
Chassis
High backplane utilization 3-3, 3-12
Disk
Operationally down 3-29
Operationally down (IP Server Performance Manager only) 3-3
Fan
State not normal 3-38
Filesystem
High utilization 3-3, 3-31
Memory
Excessive fragmentation 3-3, 3-27, C-3
High buffer miss rate 3-27
High buffer utilization 3-27
Insufficient free memory 3-3, 3-27, C-3
Memory pool 3-3, C-3
Network adapter
High broadcast rate 3-2, 3-19, 3-20
High buffer miss rate 3-3, C-3
High buffer utilization 3-3, C-3
High collision rate 3-2, 3-19, 3-20
High discard rate 3-2, 3-19, 3-20
High error rate 3-2, 3-19, 3-21
High queue drop rate 3-2, 3-19, 3-20
High utilization 3-2, 3-19, 3-21, 3-22
Port
High broadcast rate 3-4
High collision rate 3-4
High discard rate 3-4
High queue drop rate 3-4
High Utilization 3-4
Power supply
Power supply state not normal 3-33
State not normal 3-3
Processor
High utilization 3-3, 3-25, C-3
Summary table 3-2
Temperature sensor
Out of range 3-3, 3-37
State not normal 3-3, 3-37
Voltage sensor
Out of range 3-3, 3-35
State not normal 3-3, 3-35
File server 3-6
Filesystem 3-30
High utilization 3-31
Maximum utilization percentage threshold 3-3, 3-31
Firewall 3-6
Free memory threshold 3-27

G

Generic interface/port performance
Broadcast threshold 3-20
Discard threshold 3-20
Error threshold 3-22
Error traffic threshold 3-22
Queue drop threshold 3-20
Utilization threshold 3-21
Global Console 1-4, 2-1
Containment dialog box 2-22
Notification Properties dialog box 2-5, 2-22
Overview 2-4
Type of
Map Console 2-4, 2-5, 2-13
Notification Log Console 1-4, 2-5
Topology Browser Console B-2
Global Manager 1-4, 2-5

H

High backplane utilization 3-3, 3-12
High broadcast rate
Network adapter 3-2, 3-19, 3-20
Port 3-4
High buffer miss rate 3-3, 3-27, C-3
High buffer utilization 3-3, C-3
High collision rate
Network adapter 3-2, 3-19, 3-20
Port 3-4
High discard rate
Network adapter 3-2, 3-19, 3-20
Port 3-4
High error rate
Network adapter 3-2, 3-4, 3-19, 3-21
Port 3-4
High queue drop rate
Network adapter 3-2, 3-19, 3-20
Port 3-4
High utilization
Filesystem 3-31
Filesystem (IP Server Performance Manager only) 3-3
Network adapter 3-2, 3-19, 3-21, 3-22
Port 3-4
Processor 3-3, 3-25, C-3

Host 3-6
Hub 3-6

I

ICMP polls 1-3
Infrastructure
    Containment 2-22
Input packet
    Broadcast 3-20
    Discarded 3-20
    Errors 3-21
Input queue overflow 3-20
Insufficient free memory 3-3, 3-27, C-3
    Memory pool 3-3, C-3
Interface 3-15
    Duplex mode setting 3-21, 3-22
IP
    Duplicate event 3-42
IP network 2-17
    Connectivity map 2-18
    Membership map 2-18
IP Performance Manager
    Analysis 1-3
IP Server Performance Manager 1-2
IPStatus attribute 3-41
IsFlapping attribute 3-17
IsUnresponsive attribute 3-7

L

Load balancer 3-6

M

Map
    Background 2-16
    Type of 2-17
        IP network connectivity 2-18
        IP network membership 2-18
        Physical connectivity 2-17, 2-19
        VLAN connectivity 2-18
        VLAN membership 2-18
Map Console 2-4
    Icons and indicators 2-14, 2-15
    Type of map 2-17
        IP network connectivity 2-18
        IP network membership 2-18
        Physical connectivity 2-17, 2-19
        VLAN connectivity 2-18
        VLAN membership 2-18
    Type of maps 2-17
Maps
    IS-IS topology 2-13
    Opening 2-13
Memory 3-26
    Excessive fragmentation 3-27
    High buffer miss rate 3-27
    High buffer utilization 3-27
    Insufficient free memory 3-27
Memory buffer miss threshold 3-3, 3-27
Memory buffer utilization threshold 3-3, 3-27
Memory fragmentation threshold 3-3, 3-27
MIBs polled
    List of A-2
Minimum packet rate 3-20, 3-22
MinimumDemandGet 2-11
Multilayer switch feature card (MSFC) 3-6

N

Name attribute B-2, B-3
Naming convention B-2
Network adapter
    Current utilization 3-21
    High broadcast rate 3-20
    High collision rate 3-20
    High discard rate 3-20
    High error rate 3-4, 3-21
    High queue drop rate 3-20
    High utilization 3-21, 3-22
    Interface 3-15
    Port 3-15
    Subinterface 3-15
Node 3-6
Nodes
    Table of 2-14, 2-15
Notification 2-5
    Attributes 2-5
    Display of 1-4
    Naming convention B-2
    Types 1-4
    Unique name B-2
    Aggregate events
        see Exception
    Events
        see Event
    Exception
        see Exception
Notification Log Console 1-4, 2-5
Notification Properties dialog box 2-5, 2-22
    Opening 2-5
Notifications
    Event 3-2
    Fault 3-2

O

Object
    Naming convention B-2
    Unique name B-2
Opening a Containment dialog box 2-22
Opening a Map 2-13
Opening a Notification Properties dialog box 2-5
Operational exception 3-9, 3-29
    System 3-3, C-2
Operationally down
    Disk 3-3, 3-29
OperStatus attribute 3-18
Out of range
    Temperature sensor 3-3, 3-37
    Voltage sensor 3-3
Output packet

Discarded 3-20
Errors 3-22
Output queue overflow 3-20

P

Packet errors
Input 3-21
Output 3-22
Performance exception
System 3-9, 3-20, 3-21
VLAN 3-4, 3-14, C-2
Performance Manager
Purpose 1-3
Permanent Virtual Circuit (PVC) 2-16
Physical connectivity map 2-17, 2-19
Polling
ICMP 1-3
SNMP 1-3
Port 3-15
Duplex mode setting 3-21, 3-22
High broadcast rate 3-4
High collision rate 3-4
High discard rate 3-4
High queue drop rate 3-4
High Utilization 3-4
Power supply
Exception 3-9, 3-33, 3-35
Power supply not normal 3-33
State not normal 3-33
Probe 3-6
Processing
SNMP traps 1-3
Processor 3-25
CurrentUtilization attribute 3-25
High utilization 3-25
Processor and memory
Backplane utilization threshold 3-3, 3-12
Processor utilization threshold 3-3, 3-25

Q

Queue drop threshold 3-2, 3-4, 3-20
Queue overflow
Input 3-20
Output 3-20

R

Redundancy group 2-16
Relative temperature threshold 3-3, 3-37
Relative voltage threshold 3-3, 3-35
Resource exception 3-3, 3-9, 3-25, 3-27, 3-31, C-2
Router 3-6
Router switch feature card (RSFC) 3-6
Router switch module (RSM) 3-6

S

setDuplexMode command 3-23
Setting
Environment 3-37
Relative temperature threshold 3-37
Relative voltage threshold 3-35
Ethernet interface/port performance
Broadcast threshold 3-20
Collision threshold 3-20
Error threshold 3-22
Error traffic threshold 3-22
Generic interface/port performance
Broadcast threshold 3-20
Discard threshold 3-20
Error threshold 3-22
Error traffic threshold 3-22
Queue drop threshold 3-20
Utilization threshold 3-21
Processor and memory 3-27
Backplane utilization threshold 3-3, 3-12
Processor utilization threshold 3-25
SNMP
Polls 1-3
Traps 1-3
List of A-5
Traps for analysis purposes
List of A-6
Traps for discovery purposes
List of A-5
SNMP trap message processing 1-3
State not normal
Fan 3-38
Power supply 3-3
Temperature sensor 3-3, 3-37
Voltage sensor 3-3
Status attribute 3-12
Subinterface 3-15
Switch 3-6
System 3-6
Bridge 3-6
Discovery error 3-4, 3-10
DisplayName attribute B-3
Exception
Error 3-9, 3-21
Operational 3-9, 3-29
Performance 3-9, 3-20, 3-21
Power supply 3-9, 3-33, 3-35
Resource 3-9, 3-25, 3-27, 3-31
Temperature 3-9, 3-37, 3-38
Exceptions and faults 3-2
File server 3-6
Firewall 3-6
Host 3-6
Hub 3-6
Load balancer 3-6
Multilayer switch feature card 3-6
Name attribute B-3
Node 3-6
Probe 3-6
Router 3-6
Router switch feature card 3-6
Router switch module 3-6
Switch 3-6
Terminal server 3-6

Uncertified 3-6

T

Temperature
Exception 3-3, 3-9, 3-37, 3-38, C-2
Sensor
Out of range 3-37
State not normal 3-37
Temperature sensor 3-36
Terminal server 3-6
Threshold
Backplane utilization 3-3, 3-12
Broadcast 3-2, 3-4, 3-20
Collision 3-2, 3-4, 3-20
Discard 3-2, 3-4, 3-20
Error 3-2, 3-21, 3-22
Error traffic 3-2, 3-4, 3-22
Free memory 3-27
Maximum utilization percentage 3-3, 3-31
Memory buffer miss 3-3, 3-27
Memory buffer utilization 3-3, 3-27
Memory fragmentation 3-27
Memory management 3-3
Processor utilization 3-3, 3-25
Queue drop 3-2, 3-4, 3-20
Relative temperature 3-3, 3-37
Relative voltage 3-3, 3-35
Utilization 3-2, 3-4, 3-21
Topology
Containment 2-22
Topology Browser B-2
Topology Maps
See Maps 2-17
Topology object
Naming convention B-2
Unique name B-2

U

Uncertified 3-6
Utilization threshold 3-2, 3-4, 3-21

V

VLAN 2-17, 3-4, 3-13
Connectivity map 2-18
Exception
Error 3-4, 3-14, C-2
Performance 3-4, 3-14, C-2
Membership map 2-18
Voltage sensor 3-34
Out of range 3-35
State not normal 3-35

Z

Aggregate event
see Exception