EMC® Smarts®
IP Availability Manager

Version 7.0

User's Guide

300-004-088
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 Availability Manager 1-3
Availability monitoring 1-3
Availability analysis 1-3
Availability 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 2-7
Viewing details 2-8
Network topology 2-10
Viewing network topology in maps 2-11
Opening a network topology map 2-12
Network topology map pop-up menus 2-12
Network topology map graphical representations 2-13
Network topology map types 2-15
Physical Connectivity map 2-15
IP Network Connectivity map 2-16
IP Network Membership map 2-16
VLAN Connectivity map 2-16
VLAN Membership map 2-16
Group maps 2-17
Example 1: Displaying a Physical Connectivity map 2-18
Example 2: Displaying a Group IPNetwork Connectivity map 2-19
Network containment 2-20
Opening a network containment dialog box 2-20
Viewing network containment 2-21
Network containment tab pages 2-21

Chapter 3 Network Objects and Their Failures

Summary of root-cause problems, exceptions, and events 3-2
Root-Cause problems summary 3-2
Exceptions summary 3-4
Events summary 3-4
Network objects, attributes, problems, exceptions, and events 3-7
System 3-8
Attributes for system 3-9
Root-cause problems for system 3-11
Exceptions for system 3-11
Events for system 3-12
Chassis 3-14
Attributes for Chassis 3-14
Root-cause problems for Chassis 3-15
Events for Chassis 3-15
Card 3-16
Attributes for Card 3-16
Root-cause problems for Card 3-17
Events for Card 3-18
Network adapter 3-19
Attributes for network adapter 3-20
Root-cause problems for network adapter 3-23
Events for network adapter 3-25
Device connection 3-27
Attributes for device connection 3-27
Root-cause problems for device connection 3-31
Events for device connection 3-32
Service access point 3-33
IP 3-33
IPv6 3-39
HSRPEndpoint 3-43
Logical link 3-47
IPv6Network 3-47
VLAN 3-48
Partition 3-50
Attributes for Partition 3-50
Root-cause problems for Partition 3-51
Events for Partition 3-51
Management agent 3-52
Attributes for management agent 3-52
Root-cause problems for management agent 3-55
Events for management agent 3-55
Redundancy group 3-56
Attributes for redundancy group 3-56
Root-cause problems for redundancy group 3-57
Events for redundancy group 3-57
Attributes for HSRPGroup 3-58
Root-cause problems for HSRPGroup 3-59
Events for HSRPGroup 3-59
Monitoring and analysis of a redundancy group 3-59

Chapter 4 Diagnosis of Unstable Objects

Overview of trap analysis 4-2
Thresholds associated with unstable analysis 4-3
Example of unstable analysis 4-4
Unstable notifications for backup or dial-on-demand interfaces 4-5

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 Problem, Event, and Notification Summary

Problems and events C-2
Notifications C-4

Appendix D Redundancy Group Creation

Creation of card redundancy groups D-2
Creation of system redundancy groups D-3
Creation of network adapter redundancy groups D-4
Creation of HSRPGroups D-6

Index i-1

Preface

This document provides detailed information about EMC Smarts IP Availability Manager (IP Availability Manager). IP Availability Manager automatically diagnoses connectivity failures in IP networks and sends the results of its analysis to the EMC Smarts Service Assurance Manager (Global Manager).

Audience for this guide

This document is intended for IT managers seeking to better understand the value of IP Availability Manager, for system administrators configuring and using IP Availability 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 Availability 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 Availability 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 connectivity using EMC® Smarts® IP Availability Manager. It consists of the following sections:

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

Important terminology

IP Availability 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 Availability Manager, the domain is IP network transport connectivity. 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.

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 Availability 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 Availability Manager

In a typical managed network, a management station monitors the network's availability by frequently probing the systems in the network. One failed system or connection in the network will break the connectivity between the management station and all other network systems reached through the failed system or connection. As a result of this failure, the management station will generate an alarm for each unreachable system, making it difficult to determine which system or connection has failed. The challenge of managing network connectivity is to determine which alarms are real problems and which alarms are symptoms of real problems.

IP Availability Manager correlates the alarms that are generated as a result of a failure to pinpoint the failed object—the problem origin. It also identifies all managed objects affected by the failed object. With IP Availability Manager, you can focus on addressing the failed object and can consider all other alarms as symptoms of that failure.

IP Availability Manager diagnoses connectivity failures in multi-vendor, switched, and routed networks by discovering and monitoring Layer 2 (data-link) and Layer 3 (network) systems. Layer 2 systems transmit packets from network node to network node based on station address, and Layer 3 systems route data to different Local Area Networks (LANs) and Wide Area Networks (WANs) based on network address.

Availability monitoring

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

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

IP Availability 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 Availability Manager.

Availability analysis

The polling results and received traps serve as input to the data model maintained by IP Availability Manager. The data model involves a codebook created by EMC engineering as a result of its knowledge of storage resources. The codebook identifies network problems and their symptoms, and presents a causality mapping between each problem and its set of symptoms.

As IP Availability Manager monitors the network and applies the received status changes to the appropriate systems in its repository, it diagnoses root-cause availability problems by finding the problems in the codebook that can best explain the observed symptoms. It also uses the codebook to compute the impact of a root-cause problem on the network objects that are either inaccessible or impaired as a result of the root-cause problem.

Availability notifications

IP Availability Manager exports the results of its root-cause 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 Availability Manager by its domain name in the Source attribute. Users can double-click a notification to view detailed information about the notification.

IP Availability Manager creates three types of notifications: root-cause failures, events, and exceptions. Exceptions are also referred to as aggregate events.

- Root-cause notifications indicate points of failure diagnosed by IP Availability Manager. Each root-cause notification indicates a separate failure.
- Event notifications indicate abnormal conditions detected by IP Availability Manager. IP Availability Manager computes these events from status changes gathered from or issued by systems in the managed network and uses them to determine root-cause failures.
- Exception notifications indicate one or more related failures associated with a system or any of the system's components. For example, an exception notification is generated for a router when a card on the router has a problem or the router is down.

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 problems diagnosed by IP Availability 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 Availability 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 2-10
- Network containment 2-20

Before you start

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

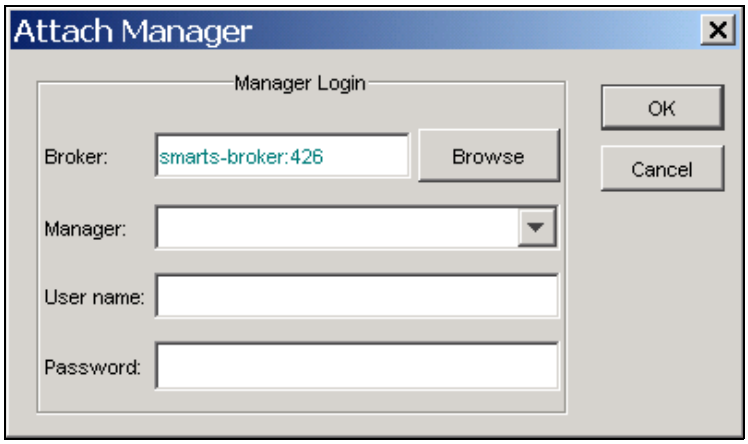

Figure 2-1 Attach Manager dialog box

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.

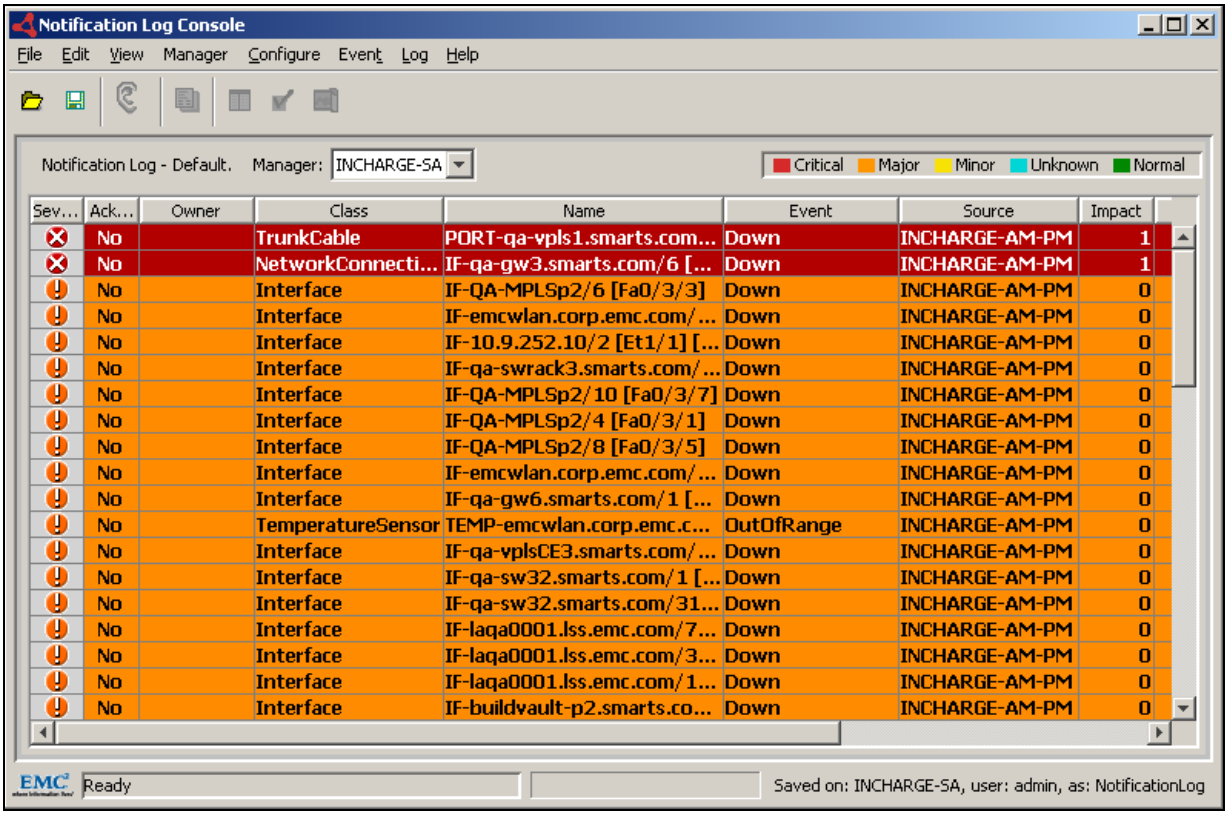

Figure 2-2 Notification Log Console—example

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 Availability 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 Availability 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 an Interface Down problem.

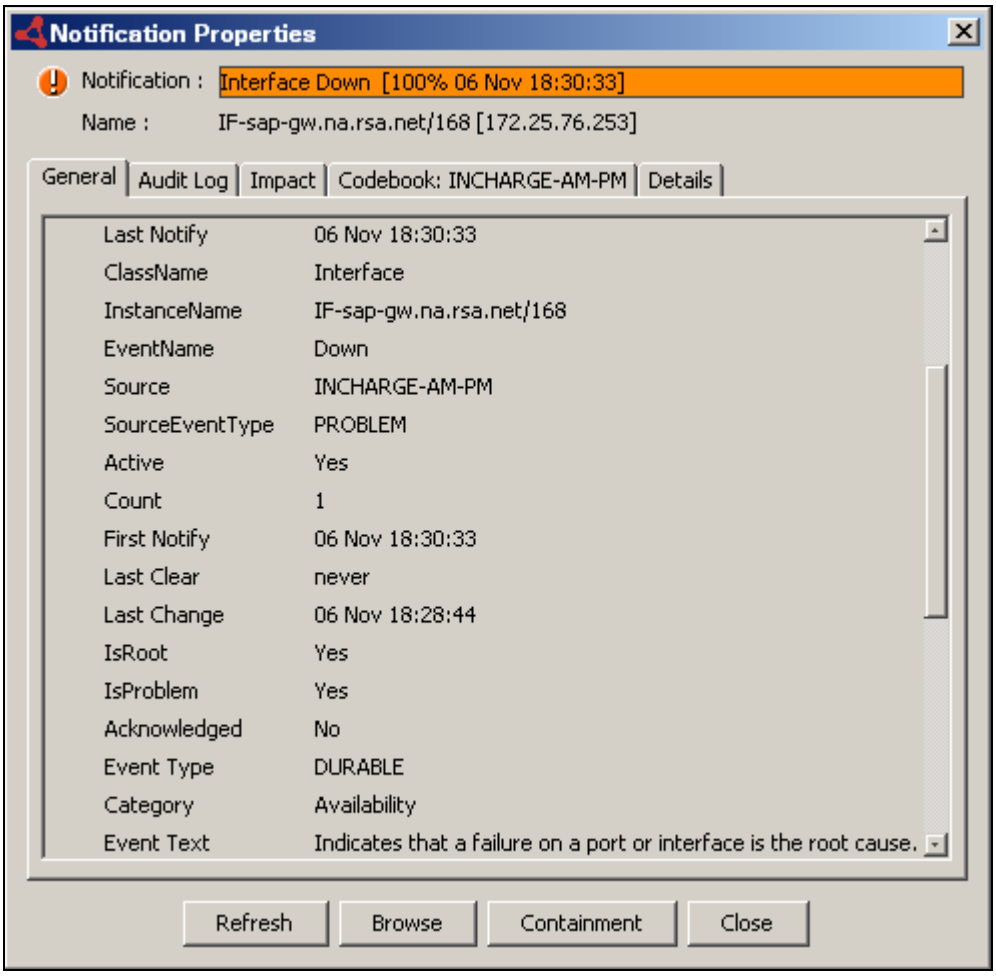

Figure 2-3 Notification Properties dialog box showing an Interface Down problem

In Figure 2-3, attribute IsRoot set to Yes indicates that Interface Down is a root cause, and attribute IsProblem set to Yes indicates that the root cause was diagnosed by IP Availability Manager using event-correlation analysis. Attribute IsRoot is always set to Yes when IsProblem is set to Yes. 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.
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.

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.

Figure 2-4 lists the impacts diagnosed by IP Availability Manager for the Interface Down problem shown in Figure 2-3.

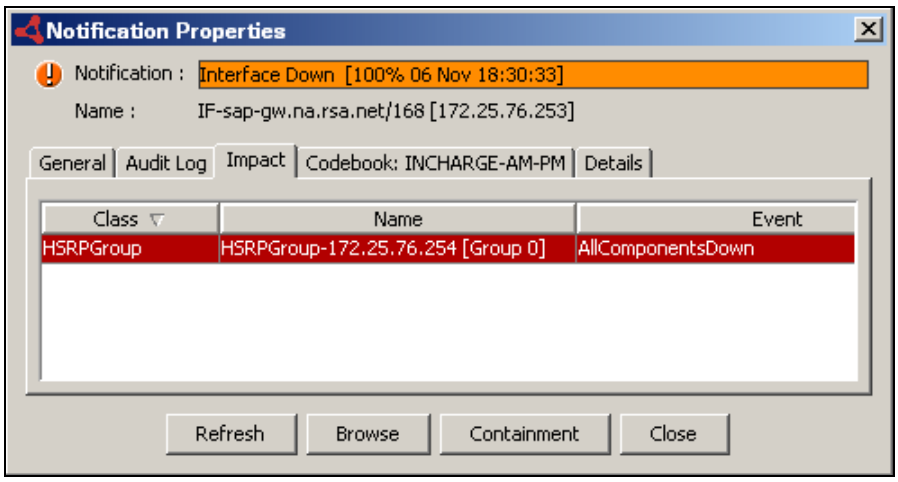

Figure 2-4 Notification Properties dialog box showing the impacts for the Interface Down problem

For a network impact notification, that is, a notification identifying an object impacted by a problem diagnosed by IP Availability Manager, a Caused By tab appears (instead of the Impact tab) in the Notifications Properties dialog box. (See Figure 2-5 for an example.) This tab lists the problem that caused the notification.

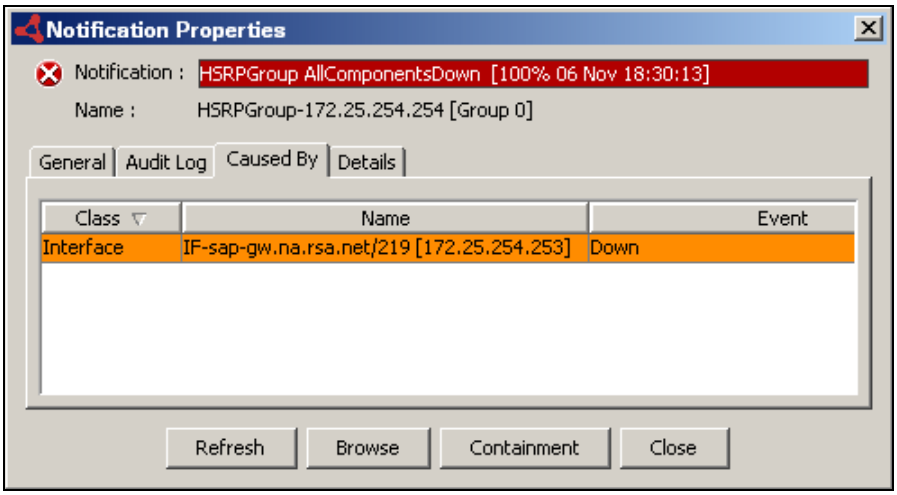

Figure 2-5 **Notification Properties dialog box for a network impact notification**

Viewing details

You view the details for a network notification by clicking the Details tab in the Notification Properties dialog box. The Details tab displays 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.

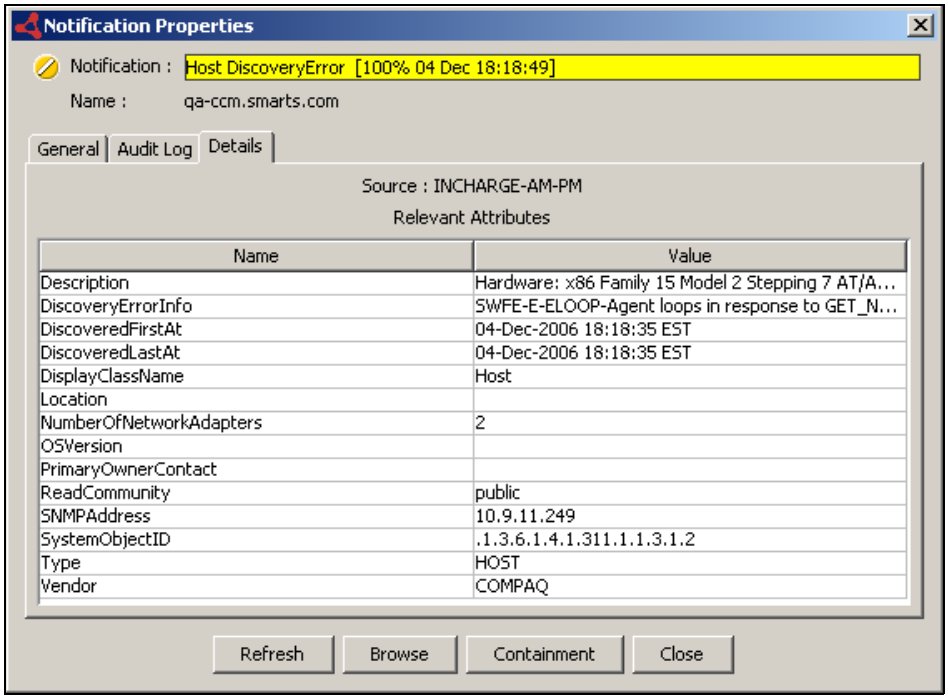

Figure 2-6 **Notification Properties dialog box showing the details for a Host DiscoveryError event**

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 Availability Manager. The imported topology includes systems, physical packages, device connections, logical links, collections, redundancy groups, and duplicate IPs (DuplicateIP and DuplicateIPv6 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, FileServer is a subclass of Host.

- Systems
  - Bridge
  - Host
    - FileServer
  - Hub
  - LoadBalancer
  - Node
  - Probe
  - Router
    - Firewall
    - Multilayer Switch Feature Card (MSFC)
    - Router Switch Feature Card (RSFC)
    - Router Switch Module (RSM)
  - Switch
  - TerminalServer
- Physical packages
  - NASChassis
- Device connections
  - NetworkConnection
    - Cable
    - TrunkCable
- Logical links
  - IPNetwork
  - IPv6Network
  - VLAN
- Collections
  - Partition
- Redundancy groups
  - SystemRedundancyGroup
  - NetworkAdapterRedundancyGroup
  - NetworkConnectionRedundancyGroup
  - HSRPGroup

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. In some cases, depending on the other Domain Managers, "combining" means migrating certain object types imported from IP Availability Manager with certain object types imported from the other Domain Managers. For example, if the other Domain Manager is EMC Smarts Storage Insight for Availability, the Global Manager displays common instances (instances having the same name) of Host and HostSystem as HostSystem objects, and displays common instances of Host and NAS_ControlStation as NAS_ControlStation objects.

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.

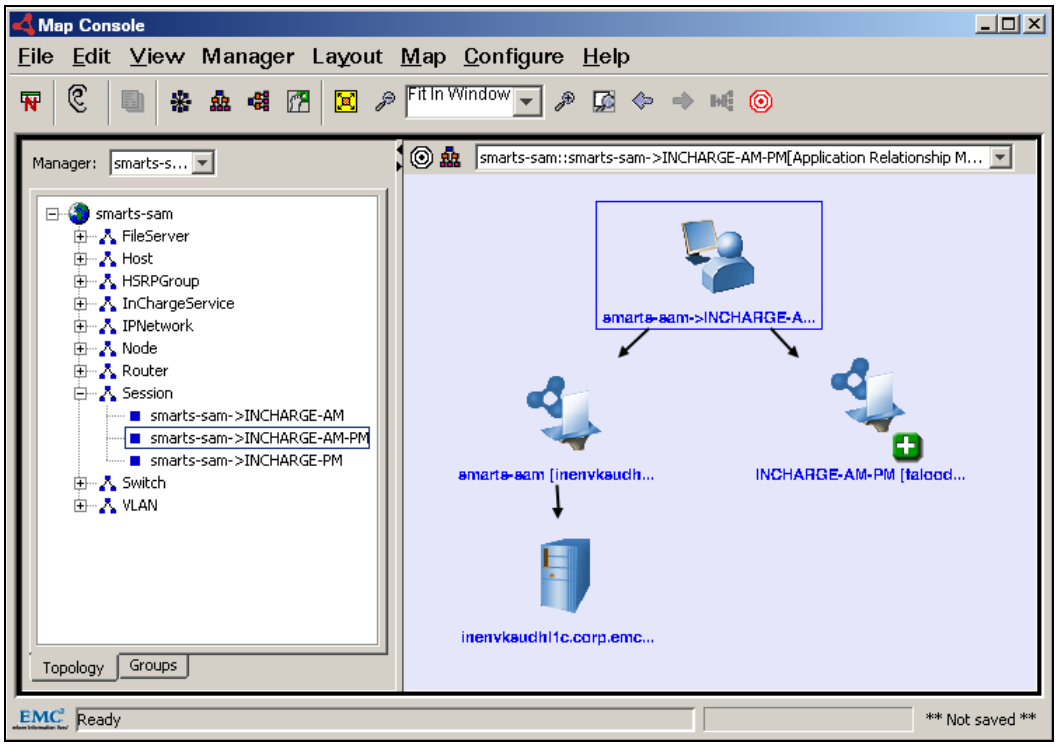

Figure 2-7 Network topology map—example

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 and edges for network topology maps

Icon / Visual Indicator	Description
	Icon can represent a system such as a switch, router, hub, bridge, or host.
	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.

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

Icon / Visual Indicator	Description
	Icon represents a firewall.
	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 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 topology 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
IPNetwork	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.

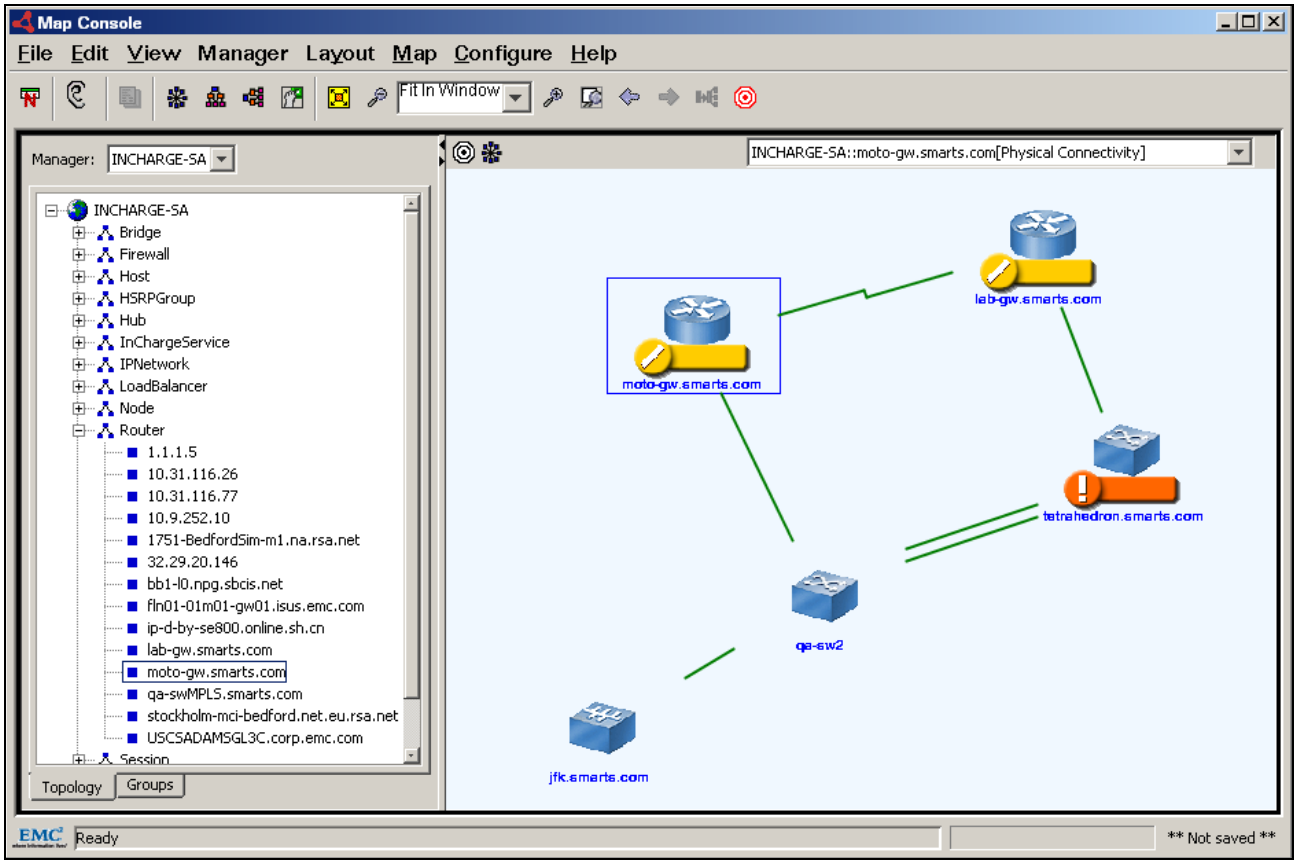

Figure 2-8 Physical Connectivity map

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.

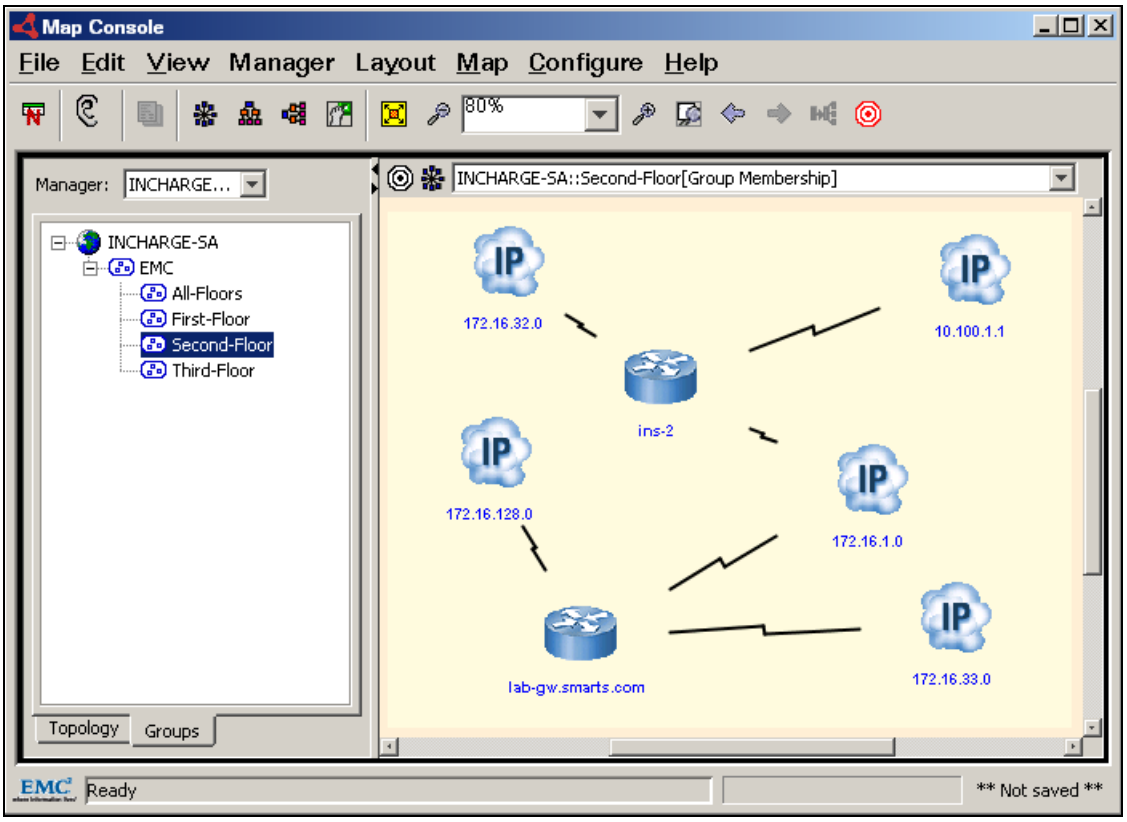

Figure 2-9 Group IP Network Connectivity map

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.

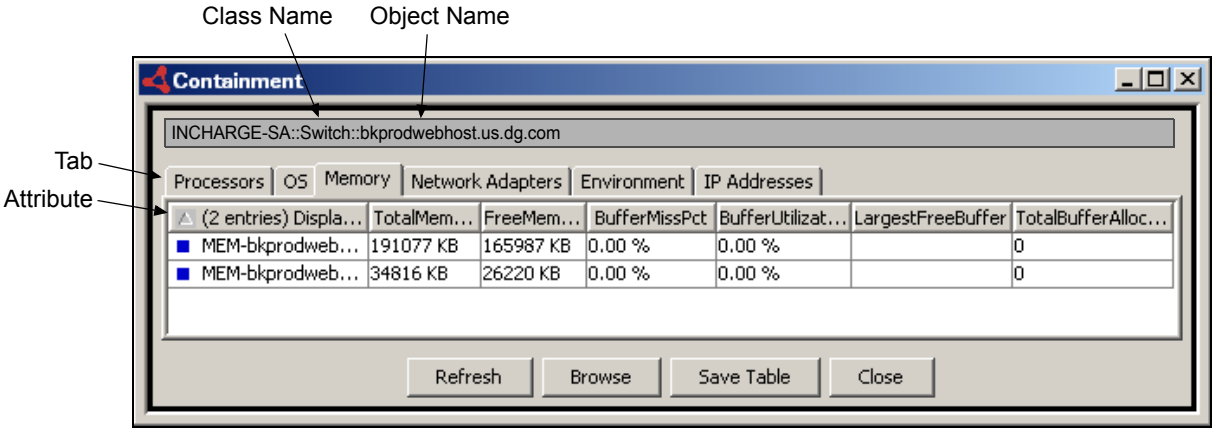

Figure 2-10 Switch Containment dialog box—example

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 Availability Manager and identifies the root-cause failures, symptoms, and exceptions for each object type. It consists of the following sections:

- Summary of root-cause problems, exceptions, and events 3-2
- Network objects, attributes, problems, exceptions, and events 3-7
- System 3-8
- Chassis 3-14
- Card 3-16
- Network adapter 3-19
- Device connection 3-27
- Service access point 3-33
- Logical link 3-47
- Partition 3-50
- Management agent 3-52
- Redundancy group 3-56

Summary of root-cause problems, exceptions, and events

IP Availability Manager diagnoses root-cause problems and detects (computes) events from status changes gathered from or issued by devices in the managed environment. It uses the events as symptoms to diagnose root-cause problems.

Note: Events used as symptoms to diagnose a failure can also be perceived as impacts resulting from the failure.

IP Availability Manager also generates exceptions, or aggregate events, where an exception is a collection of problems or events associated with a particular managed system, IPv6Network, or VLAN. IP Availability Manager generates an exception whenever any of the composite problems or events for the system, IPv6Network, or VLAN occur. For example, IP Availability Manager will generate an exception for a router when a card on the router has a problem or the router is down.

The Global Manager imports all problems diagnosed by IP Availability Manager and certain key events detected by IP Availability Manager. It also imports the IPv6Network inaccessible exception. The problem notifications (one problem per notification), event notifications (one event per notification), and IPv6Network exception notifications (one exception per notification) are displayed in the Global Console.

Root-Cause problems summary

Table 3-1 lists the network root-cause problems diagnosed by IP Availability Manager, including the condition and events for each problem. The table also identifies the managed objects for which the problems are diagnosed.

Table 3-1 Root-cause problems diagnosed by IP Availability Manager

Managed object	Root cause	Condition	Events (symptoms) of root cause
System	Down	None	System MightBeDown
			Network adapter DownOrFlapping
	Unstable	None	SNMPAgent RepeatedRestarts
Chassis	Down	Chassis packages more than one system, and all systems are down.	System Down (all systems are down)
Card	Down	None	Card OperationallyDown
			Card Down (for cards within Card)
			Card SwitchOver
			Network adapter Down
			System Down (for systems packaged by Card)
Network adapter	Down	Port or interface is managed and not connected	Network adapter DownOrFlapping
			System MightBeDown (connected system)
	Unstable	None	Network adapter Flapping
	Disabled	Port or interface is connected or is a physical interface with subinterfaces layered over it	Network adapter AdministrativelyDown
			Network adapter DownOrFlapping
			System MightBeDown (connected system)
	LogicalConnection-Down	No failure symptoms at physical layer	Network adapter DownOrFlapping
		Physical interface with subinterfaces layered over it	System MightBeDown or Flapping (connected system)
Device connection	Down	Physical connection such as cable, serial, or point-to-point	Network adapter Down
		IsLogicalConnection attribute for device connection object = TRUE	Virtual Circuit Unavailable
	Unstable	Physical connection such as cable, serial, or point-to-point	Network adapter DownOrFlapping
		IsNetworkAdapterFlapping attribute for device connection object = TRUE	
Partition	Down	Is not a proxy	System Unresponsive (all systems are unresponsive)
		None	LayeredOver Partition Down
Management agent	NotResponding	None	Management agent Unresponsive

Exceptions summary

Table 3-2 lists the exceptions generated by IP Availability Manager and the problems (p) or events (e) that can cause each exception to be generated.

Table 3-2 Exceptions generated by IP Availability Manager

Managed object	Exception	Cause (problem or event)
System	ConnectivityException	System Down (p)
		System Unstable (p)
		SNMPAgent NotResponding (p)
		Network adapter Down (p)
		Network adapter Unstable (p)
		Network adapter LogicalConnectionDown (p)
		Network adapter Disabled (p)
		Card Down (p)
		Chassis Down (p)
	OperationalException	System Unresponsive (e)
		SNMPAgent Unresponsive (e)
		SNMPAgent RepeatedRestarts (e)
		Card OperationallyDown (e)
		Network adapter DownOrFlapping (e)
		Network adapter BackupActivated (e)
		Network adapter ExceededMaximumUptime (e)
IPv6Network	InaccessibleException *	IPv6 Down (e)
VLAN	ConnectivityException	System Down (p)
		Port Down (p)
		Port Unstable (p)
		Port Disabled (p)
	OperationalException	Port DownOrFlapping (e)
		Port BackupActivated (e)
		Port ExceededMaximumUptime (e)

* Imported by the Global Manager.

Events summary

Table 3-3 lists the events detected by IP Availability Manager for each managed object and used as symptoms to diagnose root-cause problems. The table also shows the associated thresholds for the events. The thresholds can be changed using the Polling

and Thresholds Console, as described in Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide*.

Table 3-3 Events detected by IP Availability Manager

Managed object	Event (symptom)	Threshold (setting)
System	DiscoveryError *	None
	MightBeDown	None
	Unresponsive *	None
Card	OperationallyDown	None
	SwitchOver *	
Network adapter	BackupActivated *	MaximumUptime (Backup Interface Support)
	ExceededMaximumUptime *	MaximumUptime (Backup Interface Support or Dial-On-Demand Interface Support)
	AdministrativelyDown	None
	DownOrFlapping	LinkTrapThreshold LinkTrapWindow (Interface/Port Flapping)
Device connection	DownOrFlapping *	See DownOrFlapping for network adapters
IP	Down	None
	Unresponsive	
DuplicateIP	Duplicate *	None
IPv6	Down *	None
	Unresponsive	
DuplicateIPv6	Duplicate	None
HSRPEndpoint	SwitchOver *	None
Management agent	Unresponsive	None
	RepeatedRestarts	RestartTrapThreshold RestartTrapWindow (Connectivity)
Redundancy group	AllComponentsDown *	AtRiskThreshold (set to 1 by default)
	AtRisk *	
	ReducedRedundancy *	
	SwitchOverFailed * (HSRPGroup only)	

* Imported by the Global Manager.

Note: Appendix C, "Problem, Event, and Notification Summary," provides a summary of the root-cause problems diagnosed by IP Availability Manager, the events correlated by IP Availability Manager to diagnose problems, and the notifications imported by the Global Manager from IP Availability Manager.

Table 3-4 lists the events detected by IP Availability Manager for a managed system that has been restarted or reconfigured. When IP Availability Manager detects a "system restarted" or "configuration change" condition, it creates and sends a SystemRestarted or ConfigChange trap to the EMC Smarts Service Assurance Manager Adapter Platform (Adapter Platform). The Adapter Platform, in turn, transforms the SystemRestarted or ConfigChange trap to a SystemRestarted or ConfigChange event, for import as a notification by the Global Manager.

The table also shows the associated thresholds for the events and the trap messages received from the network that trigger the events. The thresholds can be changed using the Polling and Thresholds Console, as described in Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide*.

Table 3-4 SystemRestarted and ConfigChange events detected by IP Availability Manager

Managed object	Event	Threshold (setting)	Received trap triggering the event
System	SystemRestarted *	EnableGenericOIEvent MaxUpTimeThreshold (Connectivity)	coldStart or warmStart
	ConfigChange *	None	ciscoConfigManEvent or sysConfigChangeTrap

* Imported by the Global Manager through the Adapter Platform.

Chapter 2, "Setting Configuration Parameters," in the *EMC Smarts IP Management Suite Configuration Guide* provides more information about the SystemRestarted and ConfigChange traps and events, including procedures for enabling the generation of the SystemRestarted and ConfigChange traps and events.

Network objects, attributes, problems, exceptions, and events

The sections that follow describe key attributes, diagnosed problems, generated exceptions, and detected events for the following categories of network object types in the IP Availability 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. Physical packages include Card, Chassis, and Rack.

- Network adapters

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

- Device connections

  A device connection represents the path between a pair of network adapters. Device connections include Cable, TrunkCable, and NetworkConnection.

- 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, IPv6, HSRPEndpoint, 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 a logical links are IPNetwork, IPv6Network, and VLAN.

- Collections

  A collection represents a group of managed objects. Collections include Partition.

- Management agents

  A management agent is a logical object that contains the information necessary to represent, configure, or manage some functionality provided by a system or software feature. Management agents include SNMPAgent and VRAgent.

- Redundancy groups

  A redundancy group is a logical object that contains two or more objects that participate in a redundant configuration. Examples of redundancy groups are CardRedundancyGroup, HSRPGroup, and SystemRedundancyGroup.

Appendix A, "ICIM Network Concepts," in the *EMC Smarts IP Management Suite Discovery Guide* describes all of the object types instantiated by IP Availability Manager.

All of the object types instantiated by IP Availability Manager are available to a Global Console attached to IP Availability Manager, and a subset are available to a Global Console attached to the Global Manager. "Network topology" on page 2-10 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 3-5 lists some key attributes for system.

Table 3-5 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 3-5 Attributes for system (continued)

Attribute	Description	Allowed values
NumberOfIPs	Number of IP endpoints (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:** If 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

Root-cause problems for system

A system can be a switch, router, hub, bridge, host, or other computer-based network entity. The following root-cause problems are diagnosed for system:

- Down
- Unstable

System Down

Down indicates that a system has failed. For example, Router Down indicates that a router has failed. A system failure causes all ports or interfaces on the system and all objects accessed through the system to be unreachable.

The events used as symptoms to diagnose Down vary, depending on whether the system is connected to other systems by a physical or logical link. When a system is not connected to other systems, the event is system Unresponsive.

When a system is connected to one or more systems, the events used as symptoms to diagnose system Down include:

- MightBeDown for the system itself and any connected systems.
- DownOrFlapping for any peer network adapter and any peer subinterfaces.

System Unstable

Unstable indicates that a system has repeatedly restarted over a short period of time and is considered unstable. The RestartTrapThreshold and the RestartTrapWindow parameters in the Connectivity setting for the "System Resources Groups" threshold group control the analysis for a system unstable condition. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* provides information about these parameters.

"Diagnosis of Unstable Objects" on page 4-1 provides information about how IP Availability Manager concludes that a system is unstable.

The event used as a symptom to diagnose a system Unstable problem is SNMPAgent RepeatedRestarts.

Exceptions for system

IP Availability Manager generates an exception for a system when it diagnoses one or more root-cause problems for the affected system. For example, when IP Availability Manager diagnoses SNMPAgent NotResponding for a system, IP Availability Manager also generates a ConnectivityException.

Likewise, when IP Availability Manager detects an event such as SNMPAgent RepeatedRestarts for a system, IP Availability Manager generates an OperationalException.

System ConnectivityException

ConnectivityException is an aggregate event that indicates that one or more connectivity-related root-cause problems exist for a particular system or one of its components. For example, if the system is down or one of its ports is down, a ConnectivityException will be generated for the system.

Root-cause problems that result in a ConnectivityException include:

- System Down
- System Unstable
- SNMPAgent NotResponding
- Network adapter Down
- Network adapter Unstable
- Network adapter LogicalConnectionDown
- Network adapter Disabled
- Card Down
- Chassis Down

System OperationalException

OperationalException is an aggregate event that indicates that a system or one of its components is not functioning properly. For example, if the system is unresponsive or its SNMPAgent is repeatedly restarting.

Events that cause an OperationalException include:

- System Unresponsive
- SNMPAgent Unresponsive
- SNMPAgent RepeatedRestarts
- Card OperationallyDown
- Network adapter DownOrFlapping
- Network adapter BackupActivated
- Network adapter ExceededMaximumUptime

Events for system

Table 3-6 lists the events detected for system and used as symptoms for root-cause analysis. Unresponsive and DiscoveryError are exported to the Global Manager.

Table 3-6 Events for system

Event	Description
MightBeDown	Indicates that all of the system's HostAccessPoints (IP interfaces) and HostServices (SNMPAgent) are not responding and that the system is logically near the root-cause problem.
Unresponsive	Indicates that all of the system's HostAccessPoints (IP interfaces) and HostServices (SNMPAgent) are not responding.
DiscoveryError	Indicates that an error occurred while rediscovering the system.

A DiscoveryError indicates that the discovery process did not rediscover a system. Any root-cause problem diagnosed by IP Availability Manager can explain a discovery error. For example, a DiscoveryError might result if a system is diagnosed as Down and is not, therefore, reachable during rediscovery.

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 3-7 lists some key attributes for Chassis.

Table 3-7 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 3-7 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

Root-cause problems for Chassis

The following root-cause problem is diagnosed for Chassis:

Down: Indicates that a chassis has failed. A chassis failure causes all systems in the chassis to fail. If the chassis packages only one system, system Down supersedes chassis Down.

The events used to diagnose chassis Down are system Down events for systems packaged by the chassis, or system Down events for systems packaged by the cards that are a part of the chassis.

Events for Chassis

No events are detected for Chassis.

Card

Similar to a chassis, a card is also a physical package. A card is a physical module or blade of a networking device.

Attributes for Card

Table 3-8 lists some key attributes for Card.

Table 3-8 Attributes for Card

Attribute	Description	Allowed values
DisplayName	Name, as shown in the Global Console, of this Card; for example: CARD-10.9.252.11/16.0.0.96.105.144.4.243.0.0.0.0.0.0.0.0[Fibre Channel Switch. - Fibre Channel Switch.]	String
IsCardNotOperating	TRUE if this Card is not operational.	Boolean: true or false
IsSwitchOverActive	TRUE if this Card has switched over to the active state.	Boolean: true or false
IsSystemUnresponsive	TRUE if this Card is not responding to ICMP pings or SNMP polls. (FALSE if this Card is responding to ICMP pings and/or SNMP polls.)	Boolean: true or false
Location	Specifies the position and address of this Card.	String
Name	Name, as known in the modeled topology, of this Card; for example: CARD-10.9.252.11/16.0.0.96.105.144.4.243.0.0.0.0.0.0.0	String
SerialNumber	Indicates the version of this Card.	String
StandbyStatus	Standby status for this Card. • ACTIVE indicates that this Card is the active card within a card redundancy group. • INACTIVE indicates that this Card is the standby card within a card redundancy group. • ERROR_STANDBY indicates that this Card, the standby (redundant) card within a card redundancy group, has encountered an error. • NOTAPPLICABLE indicates that this Card does not support card redundancy. • OTHER_STANDBY indicates that the status of this Card is other than ACTIVE, INACTIVE, ERROR_STANDBY, NOTAPPLICABLE, or is an unrecognized SNMP error. • UNKNOWN_STANDBY indicates that this Card has yet to be polled.	Enum: • ACTIVE • INACTIVE • ERROR_STANDBY • NOTAPPLICABLE • OTHER_STANDBY • UNKNOWN_STANDBY

Table 3-8 Attributes for Card (continued)

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

Root-cause problems for Card

The following root-cause problem is diagnosed for Card:

Down: Indicates that a card has failed. A card failure causes all ports and interfaces in the card as well as any system functions associated with the card to fail. For example, if a Router Switch Module (RSM) is associated with the card, the routing functions provided by the RSM will fail. The events used to diagnose Card Down include:

- OperationallyDown for the card
- Card Down for any subcards
- SwitchOver for any supervisor cards
- Network adapter Down for any ports or interfaces realized by the card
- System Down for any systems packaged by the card

Events for Card

Table 3-9 lists the events detected for Card and used as symptoms for root-cause analysis. SwitchOver is also exported to the Global Manager.

Table 3-9 Events for Card

Event	Description
OperationallyDown	Indicates that the card is instrumented and the value of the Status attribute is CRITICAL. Typically, OperationallyDown means that the card has failed or has been removed.
SwitchOver	Indicates that the standby status of the card has changed from INACTIVE to ACTIVE within the last 30 minutes. In a topology where a switch has two supervisor cards, the status of a supervisor card can change from standby to active because the card is misconfigured. The switch over does not result in a Card Down or a Redundancy Group AtRisk notification because it is not caused by a physical failure. SwitchOver is detected when the standby status of the card changes, as indicated by the moduleStandbyStatus MIB. In order for the SwitchOver event to be detected, the change in standby status must have occurred within the last 30 minutes. This event automatically clears if the standby status does not change after 30 minutes. Analysis for SwitchOver is only supported for switches that support the CISCO-STACK-MIB and where the moduleStandbyStatus correctly reflects the status of the card.

Network adapter

A network adapter is a logical or physical component of a network system at which the system connects to a network. IP Availability Manager performs connectivity 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 Availability 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 Availability 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 3-10 lists some key attributes for network adapter.

Table 3-10 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 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 3-10 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 3-10 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 3-10 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)

Root-cause problems for network adapter

A network adapter can be a port or an interface. The following root-cause problems are diagnosed for network adapter:

- Down
- Unstable
- Disabled
- LogicalConnectionDown

Network adapter Down

Down indicates that a port or interface has failed or is in testing mode. A Down notification is generated when the port or interface is not physically connected. In addition, a Cable Down notification can encompass Router Down problems multiple hops away.

When a port or interface is physically connected, network adapter Down is superseded by a NetworkConnection Down diagnosis.

For ports, this means that Port Down is superseded by:

- TrunkCable Down if the port is connected through a trunk cable.
- Cable Down if the port is connected through a cable.

For interfaces, this means that Interface Down is superseded by:

- NetworkConnection Down if the interface is connected through a physical network connection.
- Cable Down if the interface is connected through a cable.

Notification of network adapter Down is controlled by the Testing Notification Mode threshold. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* provides information about the Testing Notification Mode threshold.

The events used to diagnose Down include:

- DownOrFlapping for the network adapter and any subinterfaces
- DownOrFlapping for any peer interfaces
- MightBeDown for any logically connected systems

Network adapter Unstable

Unstable indicates that a port or interface repeatedly alternates between up and down states over a short period of time and is considered unstable. The LinkTrapThreshold and LinkTrapWindow parameters contained in the Interface/Port Flapping setting control analysis for the network adapter unstable condition. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* provides information about these parameters.

"Diagnosis of Unstable Objects" on page 4-1 provides more information about how IP Availability Manager concludes that a network adapter is unstable.

An Unstable notification is only generated when the port or interface is not physically connected. When a port or interface is physically connected, network adapter Unstable is superseded by a NetworkConnection Unstable diagnosis.

For ports, this means that Port Unstable is superseded by:

- TrunkCable Unstable if the port is connected through a trunk cable.
- Cable Unstable if the port is connected through a cable.

For interfaces, this means that Interface Unstable is superseded by:

- NetworkConnection Unstable if the interface is connected through a physical network connection.
- Cable Unstable if the interface is connected through a cable.

Note: By default, Interface Unstable analysis is not performed on ISDN B channel, ISDN D channel, backup, or dial-on-demand interfaces. "Unstable notifications for backup or dial-on-demand interfaces" on page 4-5 explains how to enable Interface Unstable analysis for these types of interfaces.

The events used to diagnose Unstable are nearly identical to the events used to diagnose Down:

- DownOrFlapping for the network adapter and any subinterfaces
- DownOrFlapping for any peer interfaces
- MightBeDown for any logically connected systems

One additional condition is used to diagnose Unstable: the value of the IsFlapping attribute for one or both of the connected network adapters must be TRUE.

Network adapter Disabled

Disabled indicates that a port or interface has been turned off by a system administrator. Analysis for the Disabled problem is performed for interfaces with subinterfaces layered over them, and for ports or interfaces that are logically connected.

The events used to diagnose Disabled include:

- AdministrativelyDown for the port or interface
- DownOrFlapping or AdministrativelyDown for all subinterfaces
- DownOrFlapping for all peer subinterfaces
- MightBeDown for all physically or logically connected systems

Network adapter LogicalConnectionDown

LogicalConnectionDown indicates a fault within the Wide Area Network, which could be, for example, a Frame Relay cloud. IP Availability Manager isolates the problem to the nearest physical interface using only symptoms from the logical layer. LogicalConnectionDown is only diagnosed when there are no failure symptoms at the physical layer and the network adapter is a physical interface with subinterfaces layered over it.

The events used to diagnose LogicalConnectionDown are also used to diagnose network adapter Down. However, for LogicalConnectionDown, the DownOrFlapping event for the interface is not present.

The events used to diagnose LogicalConnectionDown include:

- DownOrFlapping for all subinterfaces and peer subinterfaces
- MightBeDown for all logically connected systems

Events for network adapter

Table 3-11 lists the events detected for network adapter and used as symptoms for root-cause analysis. BackupActivated and ExceededMaximumUptime are exported to the Global Manager.

Table 3-11 Events for network adapter

Event	Description
BackupActivated	BackupActivated indicates that a backup port/interface has become operational. By default, interfaces with a value of ISDN for the Type attribute are marked as backup and use the Backup Interface Support setting. Because a backup should not normally be online, IP Availability Manager notifies you when the backup interface or port becomes operational. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* provides information about backup activation.

Table 3-11 Events for network adapter (continued)

Event	Description
ExceededMaximumUptime	ExceededMaximumUptime indicates that a backup or dial-on-demand port/interface has been in the Up state for too long. By default, interfaces with one of the following values for the Type or InterfaceCode attribute are marked as backup or dial-on-demand: • ISDNBCHANNEL (Backup) • ISDN (Backup) • PPP or SLIP (Dial-On-Demand) Because a backup should not normally be up for very long, IP Availability Manager notifies you when the MaximumUptime has been exceeded for a device marked as backup or dial-on-demand. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* provides information about the MaximumUptime threshold.
AdministrativelyDown	AdministrativelyDown indicates that a port or interface is down because it has been explicitly disabled, which is indicated by the value of the AdminStatus attribute.
DownOrFlapping	DownOrFlapping indicates that the port/interface is operationally down (value of the AdminStatus attribute is UP and the value of OperStatus is DOWN) or that too many linkDown traps have been received within the link trap window (value of IsFlapping attribute is TRUE). Flapping is a symptom of a network adapter Unstable problem. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* provides information about how IP Availability Manager concludes that a network adapter is unstable.

Device connection

A device connection is a link between two network adapters. ("Network adapter" on page 3-19 provides information about network adapters.) IP Availability Manager performs connectivity analysis on the following device connection object types:

- Cable—A connection between a port and an interface. For example, a cable connects a port on a switch to an interface on a router.
- TrunkCable—A connection between two ports. Switches are often trunked to connect multiple segments or to provide redundant pathways through the network.
- NetworkConnection—A connection between two interfaces. A network connection can be a logical connection or a physical connection. An example of a logical connection is when routers are connected through a virtual circuit and none of the intermediate network devices are included in the topology. An example of a physical connection is when routers are connected through a serial or point-to-point connection.

Attributes for device connection

Table 3-12 lists some key attributes for device connection. The "A_" prefix distinguishes the attributes for the network adapter (port or interface) at the one end of the device connection, and the "Z_" prefix distinguishes the attributes for the network adapter (port or interface) at the other end of the device connection.

Table 3-12 Attributes for device connection

Attribute	Description	Allowed values
A_AdminStatus	Reflects the current administrative status of the network adapter (port or interface) at this end of the device connection. • UP indicates that the network adapter is administratively enabled. • DOWN indicates that the network adapter is administratively disabled. • TESTING indicates that the network adapter is in testing mode. • OTHER indicates that the network adapter is in an unknown state. • NOTPRESENT indicates that the MIB AdminStatus value for the network adapter is missing. • UNKNOWN indicates that the network adapter has yet to be polled. When the value of the network adapter's A_AdminStatus is UP, the value of A_OperStatus determines the state of the adapter. Otherwise, the value of A_AdminStatus determines the state of the adapter.	Enum: • UP • DOWN • TESTING • OTHER • NOTPRESENT • UNKNOWN

Table 3-12 Attributes for device connection (continued)

Attribute	Description	Allowed values
A_DisplayName	Name, as shown in the Global Console, of the network adapter at this end of the device connection. Port example: PORT-10.9.252.2/1 [Gi1/1] Interface example: IF-10.9.252.80/2 [Fa0/1] [10.9.77.3]	String
A_DuplexMode	Indicates whether the network adapter at this end of the device connection is full-duplex or half-duplex. • FULLDUPLEX indicates that the network adapter is full-duplex. • HALFDUPLEX indicates that the network adapter is half-duplex. • UNSPECIFIED indicates that the duplex mode value is not available for the network adapter.	Enum: • FULLDUPLEX • HALFDUPLEX • UNSPECIFIED
A_IsFlapping	TRUE if the network adapter at this end of the device connection is flapping. (FALSE if the network adapter is not flapping.)	Boolean: true or false
A_MaxSpeed	Maximum speed, in bits per second (bps), for the network adapter at this end of the device connection; for example: 10000000 bps	Integer
A_OperStatus	Reflects the current operational status of the network adapter at this end of the device connection. • UP indicates that the network adapter is operationally up. • DOWN indicates that the network adapter is operationally down. • TESTING indicates that the network adapter is in testing mode. • OTHER indicates that the network adapter is in an unknown state. • DORMANT indicates that the network adapter is waiting for an external action to occur before becoming active. • NOTPRESENT indicates that the MIB OperStatus value for the network adapter is missing. • UNKNOWN indicates that the network adapter has yet to be polled.	Enum: • UP • DOWN • TESTING • OTHER • DORMANT • NOTPRESENT • UNKNOWN

Table 3-12 Attributes for device connection (continued)

Attribute	Description	Allowed values
DisplayName	Name, as shown in the Global Console, of this device connection. Cable example: IF-10.9.1.109/10.9.1.109<->PORT-qa-sw2/19 [19] [vlan7.21.p3] TrunkCable example: PORT-10.9.252.2/1 [Gi1/1]<->PORT-qa-core.smarts.com/1.9 [Fa0/9] NetworkConnection example: IF-10.9.252.80/2 [Fa0/1] [10.9.77.3]<->IF-QA-MPLSp2/6 [Fa0/3/3]	String
IsLogicalConnection	TRUE if a logical connection exists for this device connection; that is, the network adapters at the ends of this device connection are not physically connected to one another. (FALSE if a logical connection does not exist for this device connection; that is, the network adapters at the ends of this device connection are physically connected to one another.)	Boolean: true or false
IsLogicalConnectionDown-Enabled	TRUE if a LogicalConnectionDown problem has been diagnosed by IP Availability Manager for this device connection. (FALSE if a LogicalConnectionDown problem has not been diagnosed for this device connection.)	Boolean: true or false
IsNetworkAdapterDown-OrFlapping	TRUE if at least one of the two network adapters connected via this device connection is operationally down or flapping. (FALSE if neither network adapter is operationally down or flapping.)	Boolean: true or false
IsNetworkAdapterFlapping	TRUE if at least one of the two network adapters connected via this device connection is flapping. (FALSE if neither network adapter is flapping.)	Boolean: true or false
Name	Name, as known in the modeled topology, of this device connection: Cable example: LINK-IF-10.9.1.109/10.9.1.109<->PORT-qa-sw2/19 TrunkCable example: LINK-PORT-10.9.252.2/1<->PORT-qa-core.smarts.com/1.9 NetworkConnection example: LINK-IF-10.9.252.80/2<->IF-QA-MPLSp2/6	String
SystemName	Name of the system containing this device connection: for example: 10.9.252.2	String

Table 3-12 Attributes for device connection (continued)

Attribute	Description	Allowed values
Z_AdminStatus	Reflects the current administrative status of the network adapter (port or interface) at this end of the device connection. • UP indicates that the network adapter is administratively enabled. • DOWN indicates that the network adapter is administratively disabled. • TESTING indicates that the network adapter is in testing mode. • OTHER indicates that the network adapter is in an unknown state. • NOTPRESENT indicates that the MIB AdminStatus value for the network adapter is missing. • UNKNOWN indicates that the network adapter has yet to be polled. When the value of the network adapter's Z_AdminStatus is UP, the value of Z_OperStatus determines the state of the adapter. Otherwise, the value of Z_AdminStatus determines the state of the adapter.	Enum: • UP • DOWN • TESTING • OTHER • NOTPRESENT • UNKNOWN
Z_DisplayName	Name, as shown in the Global Console, of the network adapter at this end of the device connection: Port example: PORT-qa-switch.smarts.com/1.9 [Fa0/9] Interface example: IF-QA-MPLSp2/6 [Fa0/3/3]	String
Z_DuplexMode	Indicates whether the network adapter at this end of the device connection is full-duplex or half-duplex. • FULLDUPLEX indicates that the network adapter is full-duplex. • HALFDUPLEX indicates that the network adapter is half-duplex. • UNSPECIFIED indicates that the duplex mode value is not available for the network adapter.	Enum: • FULLDUPLEX • HALFDUPLEX • UNSPECIFIED
Z_IsFlapping	TRUE if the network adapter at this end of the device connection is flapping. (FALSE if the network adapter is not flapping.)	Boolean: true or false
Z_MaxSpeed	Maximum speed, in bits per second (bps), for the network adapter at this end of the device connection; for example: 10000000 bps	Integer

Table 3-12 Attributes for device connection (continued)

Attribute	Description	Allowed values
Z_OperStatus	Reflects the current operational status of the network adapter at this end of the device connection. • UP indicates that the network adapter is operationally up. • DOWN indicates that the network adapter is operationally down. • TESTING indicates that the network adapter is in testing mode. • OTHER indicates that the network adapter is in an unknown state. • DORMANT indicates that the network adapter is waiting for an external action to occur before becoming active. • NOTPRESENT indicates that the MIB OperStatus value for the network adapter is missing. • UNKNOWN indicates that the network adapter has yet to be polled.	Enum: • UP • DOWN • TESTING • OTHER • DORMANT • NOTPRESENT • UNKNOWN

Root-cause problems for device connection

A device connection can be a cable, trunk cable, or network connection. The following root-cause problems are diagnosed for device connection:

- Down
- Unstable

Device connection Down

Down indicates that one or both network adapters linked by a physical connection have failed. A device connection failure breaks connectivity between the management station and each network adapter that the connection links, generating events at both ends.

- A Cable Down diagnosis supersedes a Port Down or an Interface Down diagnosis if the port, interface, or both are down.
- A TrunkCable Down diagnosis supersedes a Port Down diagnosis if one or both ports are down.
- A NetworkConnection Down diagnosis supersedes an Interface Down diagnosis if one or both interfaces are down.

If the network adapters are not physically connected, a network adapter LogicalConnectionDown diagnosis supersedes a device connection Down diagnosis.

The event used to diagnose device connection Down is network adapter DownOrFlapping for one or both of the network adapters. To distinguish device connection Down from device connection Unstable, the value of the IsNetworkAdapterFlapping attribute of the device connection object must also be set to FALSE.

Device connection Unstable

Unstable indicates that one or both network adapters linked by a physical connection are unstable. A network adapter is considered unstable if it alternates between up and down states over a short period of time.

- A Cable Unstable diagnosis supersedes a Port Unstable or Interface Unstable diagnosis if a cable connects a port or an interface that is unstable.
- A TrunkCable Unstable diagnosis supersedes a Port Unstable diagnosis if a trunk cable connects a port that is unstable.
- A NetworkConnection Unstable diagnosis supersedes an Interface Unstable diagnosis if a network connection connects an interface that is unstable to another interface.

The event used to diagnose device connection Unstable is network adapter DownOrFlapping. To distinguish device connection Unstable from device connection Down, the value of the IsNetworkAdapterFlapping attribute of the device connection object must also be set to TRUE.

Note: Flapping for network adapters is diagnosed using the setting described in Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide*. The flapping condition can be diagnosed for network adapters as well as any subinterfaces.

Events for device connection

The following event is detected for device connection and used as a symptom for root-cause analysis:

DownOFlapping: Indicates that one or both of the network adapters on either end of the device connection are operationally down or unstable. This event is used to enhance the display of maps in the Global Console.

DownOrFlapping is also exported to the Global Manager.

Service access point

A service access point describes a logical endpoint that can be used to gain access to some network service. IP Availability Manager performs connectivity analysis on the following service access point object types:

- IP—An endpoint that describes the IP layer characteristics of a network-attached interface. An IP endpoint is designated by a unique IPv4 address.
- IPv6—An endpoint that describes the IP layer characteristics of an IPv6 network-attached interface. An IPv6 endpoint is designated by a unique IPv6 address.
- HSRPEndpoint—An endpoint that describes the Hot Standby Router Protocol (HSRP) characteristics of an HSRP-capable interface. An HSRPEndpoint is defined for each HSRP interface of an HSRPGroup on the hosting router.

IP

An IP endpoint describes the IP layer characteristics of a network-attached interface. An IP endpoint is designated by a unique IPv4 address.

Attributes for IP

Table 3-13 lists some key attributes for IP endpoint.

Table 3-13 Attributes for IP endpoint

Attribute	Description	Allowed values
Address	IP address of this IP endpoint; for example: 1.1.1.1	String
DisplayName	Name, as shown in the Global Console, of this IP endpoint; for example: 1.1.1.1 [emcwlan.corp.emc.com]	String
InterfaceAdminStatus	Reflects the current administrative status of the interface underlying this IP endpoint. • 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

Table 3-13 Attributes for IP endpoint (continued)

Attribute	Description	Allowed values
InterfaceMode	Indicates the intended purpose of the interface underlying this IP endpoint: normal, backup, or dial-on-demand.	Enum: • NORMAL • BACKUP • ONDEMAND
InterfaceName	Name, as shown in the Global Console, of the interface underlying this IP endpoint; for example: IF-emcwlan.corp.emc.com/46 [ge-1/2/0.511] [1.1.1.1]	String
InterfaceOperStatus	Reflects the current operational status of the interface underlying this IP endpoint. • 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 IP endpoint, 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 3-13 Attributes for IP endpoint (continued)

Attribute	Description	Allowed values
IPStatus	Reflects the current state of this IP endpoint as reported by the instrumentation. **Note:** IP objects are typically instrumented using the ICMP (ping) protocol. • 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 IP endpoint; for example: IP-1.1.1.1	String

Table 3-13 Attributes for IP endpoint (continued)

Attribute	Description	Allowed values
InterfaceMode	Indicates the intended purpose of the interface underlying this IP endpoint: normal, backup, or dial-on-demand.	Enum: • NORMAL • BACKUP • ONDEMAND
InterfaceName	Name, as shown in the Global Console, of the interface underlying this IP endpoint; for example: IF-emcwlan.corp.emc.com/46 [ge-1/2/0.511] [1.1.1.1]	String
InterfaceOperStatus	Reflects the current operational status of the interface underlying this IP endpoint. • 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 IP endpoint, 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 3-13 Attributes for IP endpoint (continued)

Attribute	Description	Allowed values
IPStatus	Reflects the current state of this IP endpoint as reported by the instrumentation. **Note:** IP objects are typically instrumented using the ICMP (ping) protocol. • 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 IP endpoint; for example: IP-1.1.1.1	String

Table 3-13 Attributes for IP endpoint (continued)

Attribute	Description	Allowed values
Netmask	Network mask for this IP endpoint; for example: 255.255.255.252	String
NetworkNumber	Network number (computed from the Address and Netmask values) for this endpoint; for example: 1.1.1.0	String
Responsive	TRUE if this IP endpoint is responding to ICMP pings. (FALSE if this IP endpoint is not responding to ICMP pings.)	Boolean: true or false
Status	Current status of this IP endpoint.	Enum: • RESPONSIVE • UNRESPONSIVE • UNKNOWN
SystemName	Name of the system hosting this IP endpoint; for example: wpl01-07m01-gw01.isus.emc.com	String
SystemType	Type of system hosting this IP endpoint; for example: OTHER	Enum: • HOST • ROUTER • SWITCH • PROBE • OTHER

Root-cause problems for IP

No root-cause problems are diagnosed for IP endpoint.

Events for IP

Table 3-14 lists the events detected for IP endpoint. None of the events are used as symptoms for root-cause analysis. The Duplicate event is exported to the Global Manager.

Table 3-14 Events for IP endpoint

Event	Description
Down	Down indicates that an IP endpoint is not responding to ICMP polls and that there is no physical failure in the system or any other related network component to explain why. The value of the IPStatus attribute is not OK or UNKNOWN, and the value of both the AdminStatus and OperStatus attributes for the interface is UP. The problem is most likely at the IP protocol level. For example, the IP protocol on a router interface might be disabled but the physical interface is still up.

Table 3-14 **Events for IP endpoint (continued)**

Event	Description
Unresponsive	Unresponsive indicates that an IP endpoint is not responding to ICMP polls. Similar to Down, the value of the IPStatus attribute is not OK or UNKNOWN.
Duplicate	Duplicate indicates that the discovery process discovered two systems having the same (overlapping) IP address. When this event occurs, IP Availability 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.

IPv6

An IPv6 endpoint describes the IP layer characteristics of an IPv6 network-attached interface. An IPv6 endpoint is designated by a unique IPv6 address.

Attributes for IPv6

Table 3-15 lists some key attributes for IPv6 endpoint.

Table 3-15 **Attributes for IPv6 endpoint**

Attribute	Description	Allowed values
Address	IPv6 address of this IPv6 endpoint; for example: 3FFE:80C0:22C:61:0:0:A09:FE03	String
DisplayName	Name, as shown in the Global Console, of this IPv6 endpoint; for example: 3FFE:80C0:22C:61:0:0:A09:FE03 [10.0.0.1]	String
InterfaceAdminStatus	Reflects the current administrative status of the interface underlying this IPv6 endpoint. • 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

Table 3-15 Attributes for IPv6 endpoint (continued)

Attribute	Description	Allowed values
InterfaceMode	Indicates the intended purpose of the interface underlying this IPv6 endpoint: normal, backup, or dial-on-demand.	Enum: • NORMAL • BACKUP • ONDEMAND
InterfaceName	Name, as shown in the Global Console, of the interface underlying this IPv6 endpoint; for example: IF-10.0.0.1/35 [fe-0/0/0.0] [10.9.254.76]	String
InterfaceOperStatus	Reflects the current operational status of the interface underlying this IPv6 endpoint. • 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 IPv6 endpoint, 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 3-15 Attributes for IPv6 endpoint (continued)

Attribute	Description	Allowed values
IPStatus	Reflects the current state of this IPv6 endpoint as reported by the instrumentation. **Note:** IPv6 objects are instrumented using the IPv6 ICMP (ping) protocol. • 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
IsGlobalUnicast	TRUE if the address for this IPv6 endpoint is global unicast.	Boolean: true or false
IsInterfaceInstrumented	TRUE if "IP LayeredOver Interface" is instrumented.	Boolean: true or false

Table 3-15 **Attributes for IPv6 endpoint (continued)**

Attribute	Description	Allowed values
Name	Name, as known in the modeled topology, of this IPv6 endpoint; for example: IPv6-3FFE:80C0:22C:61:0:0:A09:FE03	String
Prefix	Address prefix for this IPv6 endpoint; for example: 3FFE:80C0:22C:61:0:0:0:0	String
PrefixLength	Length (number of significant leading bits) of the address prefix for this IPv6 endpoint; for example: 64	Integer: in the range 1 through 128; 0 if no value is specified for the Prefix attribute
Responsive	TRUE if this IPv6 endpoint is responding to IPv6 ICMP pings. (FALSE if this IPv6 endpoint is not responding to IPv6 ICMP pings.)	Boolean: true or false
SystemName	Name of the system hosting this IPv6 endpoint; for example: 10.0.0.1	String
SystemType	Type of system hosting this IPv6 endpoint; for example: ROUTER	Enum: • HOST • ROUTER • SWITCH • PROBE • OTHER

Root-cause problems for IPv6

No root-cause problems are diagnosed for IPv6 endpoint.

Events for IPv6

Table 3-14 lists the events detected for IPv6 endpoint. None of the events are used as symptoms for root-cause analysis. The Down event is exported to the Global Manager.

Table 3-16 **Events for IPv6 endpoint**

Event	Description
Down	Down indicates that an IPv6 endpoint is not responding to IPv6 ICMP polls and that there is no physical failure in the system or any other related network component to explain why. The value of the IPStatus attribute is not OK or UNKNOWN, and the value of both the AdminStatus and OperStatus attributes for the interface is UP. The problem is most likely at the IPv6 protocol level. For example, the IPv6 protocol on a router interface might be disabled but the physical interface is still up.

Table 3-16 Events for IPv6 endpoint (continued)

Event	Description
Unresponsive	Unresponsive indicates that an IPv6 endpoint is not responding to IPv6 ICMP polls. Similar to Down, the value of the IPStatus attribute is not OK or UNKNOWN.
Duplicate	Duplicate indicates that the discovery process discovered two systems having the same (overlapping) IPv6 address. When this event occurs, IP Availability Manager proceeds as follows: • Classifies the IPv6 address as a DuplicateIPv6. • 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.

HSRPEndpoint

An HSRPEndpoint is a logical object defined for each interface of an HSRPGroup on the hosting router.

Attributes for HSRPEndpoint

Table 3-17 lists some key attributes for HSRPEndpoint.

Table 3-17 Attributes for HSRPEndpoint

Attribute	Description	Allowed values
DisplayName	Name, as shown in the Global Console, of this HSRPEndpoint; for example: HSRP-10.1.16.254 [Group 16] [IF-wpl01-07m01-gw01.isus.emc.com/16]	String
GroupNumber	Number of the HSRPGroup to which this HSRPEndpoint belongs; for example: 16	String
HSRPEndpointKey	Unique value that distinguishes this HSRPEndpoint from all other HSRPEndpoints; for example: 16-16	String

Table 3-17 Attributes for HSRPEndpoint (continued)

Attribute	Description	Allowed values
InterfaceAdminStatus	Reflects the current administrative status of the interface underlying this HSRPEndpoint. • 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
InterfaceName	Name, as shown in the Global Console, of the interface underlying this HSRPEndpoint; for example: IF-wpl01-07m01-gw01.isus.emc.com/16 [Vl16] [10.1.16.247, ...] [Development Workstations]	String
InterfaceNumber	Number of the interface underlying this HSRPEndpoint; for example: 16	Integer
InterfaceOperStatus	Reflects the current operational status of the interface underlying this HSRPEndpoint. • 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
IsReady	TRUE if this HSRPEndpoint has been polled.	Boolean: true or false
IsSwitchOverActive	TRUE if this HSRPEndpoint has switched over to the active state.	Boolean: true or false

Table 3-17 Attributes for HSRPEndpoint (continued)

Attribute	Description	Allowed values
Name	Name, as known in the modeled topology, of this HSRPEndpoint; for example: HSRP-wpl01-07m01-gw01.isus.emc.com/16-16	String
Priority	Priority defined for this HSRPEndpoint in the HSRP group; for example: 110	Integer
Responsive	TRUE if this HSRPEndpoint is responding to ICMP pings. (FALSE if this HSRPEndpoint is not responding to ICMP pings.)	Boolean: true or false
State	Reflects the current state of this HSRPEndpoint as reported by the instrumentation. • ACTIVE_HSRP indicates that the interface is active. • ERROR_HSRP indicates that an error was encountered during polling. • INITIAL_HSRP indicates that HSRP is not running on the interface. This state is entered through a configuration change or when an interface first comes up. • LEARN_HSRP indicates that the hosting router has not determined the virtual IP address, and has not yet received an authenticated Hello message from the active router. In this state, the router is still waiting to hear from the active router. • LISTEN_HSRP indicates that the hosting router knows the virtual IP address, but is neither the active router nor the standby router. It listens for Hello messages from the routers. • SPEAK_HSRP indicates that the hosting router sends periodic Hello messages and is actively participating in the election of the active and/or standby router. A router cannot enter the Speak state unless it has the virtual IP address. • STANDBY_HSRP indicates that the interface is in the standby state. • UNKNOWN_HSRP indicates that the HSRP state was not polled.	Enum: • ACTIVE_HSRP • ERROR_HSRP • INITIAL_HSRP • LEARN_HSRP • LISTEN_HSRP • SPEAK_HSRP • STANDBY_HSRP • UNKNOWN_HSRP
StateChange	Indicates whether the HSRP state of this HSRPEndpoint has changed. • 0.0 indicates that the endpoint has not changed state. • Any other value indicates that the endpoint has changed state.	Numeric (float)
Status	Current status of this HSRPEndpoint.	Enum: • RESPONSIVE • UNRESPONSIVE • UNKNOWN

Table 3-17 Attributes for HSRPEndpoint (continued)

Attribute	Description	Allowed values
SystemName	Name of the system hosting this HSRPEndpoint; for example: wpl01-07m01-gw01.isus.emc.com	String
VirtualIP	Primary virtual IP address used by the HSRPGroup to which this HSRPEndpoint belongs; for example: 10.1.16.254	String
VirtualMAC	Primary virtual MAC address used by the HSRPGroup to which this HSRPEndpoint belongs.	String

Root-cause problems for HSRPEndpoint

No root-cause problems are diagnosed for HSRPEndpoint.

Events for HSRPEndpoint

The following event is detected for HSRPEndpoint, used as a symptom for root-cause analysis, and exported to the Global Manager:

SwitchOver: Indicates that traffic at this endpoint is switching from an active interface to a standby interface.

Logical link

A logical link models the path that connects service access points to each other. IP Availability Manager performs connectivity analysis on the following logical link object types:

- IPv6Network—A logical link that allows any two IPv6 addresses that are "ConnectedVia" the IPv6Network to communicate with one another.
- VLAN—A logical link that allows any two ports (or MAC addresses) that are "PartOf" the VLAN to communicate with one another.

IPv6Network

An IPv6Network allows traffic to flow between IPv6 endpoints that are "ConnectedVia" the IPv6Netwok.

Attributes for IPv6Network

Table 3-18 lists some key attributes for IPv6Network.

Table 3-18 Attributes for IPv6Network

Attribute	Description	Allowed values
ConnectedSystemsUnresponsive	TRUE if at least one system "ConnectedVia" this IPv6Network is not responding to ICMP pings or SNMP polls. (FALSE if all systems "ConnectedVia this IPv6Network are responding to ICMP pings and/or SNMP polls.)	Boolean: true or false
DisplayName	Name, as shown in the Global Console, of this IPv6Network; for example: 3FFE:80C0:22C:61:0:0:0:0/64	String
Name	Name, as known in the modeled topology, of this IPv6Network; for example: IPv6NET-3FFE:80C0:22C:61:0:0:0:0	String
NetworkNumber	Network number for this IPv6Network; for example: 3FFE:80C0:22C:61:0:0:0.0	String
PrefixLength	Length (number of significant leading bits) of the network prefix for this IPv6Network; for example: 64	Integer: in the range 1 through 128; 0 if there is no network prefix

Exceptions for IPv6Network

IP Availability Manager generates the following exception for IPv6Network:

InaccessibleException: Indicates that at least one IPv6 endpoint "ConnectedVia" the IPv6Network is down. The events that cause an InaccessibleException are IPv6 Down events.

Root-cause problems and events for IPv6Network

No root-cause problems or events are diagnosed/detected for IPv6Network.

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 3-19 lists some key attributes for VLAN.

Table 3-19 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 3-19 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 Availability Manager generates an exception for a VLAN when it diagnoses one or more root-cause problems for the affected VLAN. For example, when IP Availability Manager diagnoses Port Down for a switch that is a member of the VLAN, IP Availability Manager also generates a ConnectivityException.

Likewise, when IP Availability Manager detects an event such as Port DownOrFlapping for a switch that is a member of the VLAN, IP Availability Manager generates an OperationalException.

VLAN ConnectivityException

ConnectivityException is an aggregate event generated for a VLAN. A connectivity exception indicates that one or more connectivity-related root-cause problems exist for a port, card, or switch that is a member of the VLAN.

Root-cause problems that cause a ConnectivityException include:

- System Down
- Port Down
- Port Unstable
- Port Disabled

VLAN OperationalException

OperationalException is an aggregate event generated for a VLAN. An operational exception indicates that one or more operational events exist for a port or card that is a member of the VLAN.

Events that cause an OperationalException include:

- Port DownOrFlapping
- Port BackupActivated
- Port ExceededMaximumUptime

Events for VLAN

No events are detected for VLAN.

Partition

A partition is a group of managed devices formed by IP Availability Manager to help in root-cause analysis. IP Availability Manager builds a topology that describes managed devices in your network and their interconnections. If a device is modeled in the topology, there must be a path in the actual network that connects the device to the management station. Ideally, IP Availability Manager can also have representations of all the devices on that path.

Some devices along the path, however, might not actually be represented in your network topology. For example, those devices might not have SNMPAgents, or IP Availability Manager might not have access to their SNMPAgents, or access to the agents might be blocked by a firewall or some other administrative mechanism. Also, if you do not use autodiscovery, your seed file or information obtained from another Network Management System (NMS) might be incomplete. Or, you might have explicitly unmanaged or deleted some of the devices which are on that path.

IP Availability Manager's root-cause analysis algorithms need to determine the connectivity among managed devices. When the topology is incomplete, IP Availability Manager creates partitions to group all the related managed devices, which helps analysis to proceed.

Within a single partition, any two managed devices are indeed connected by a path. However, objects within distinct partitions have no path between them in the modeled topology, even though they are connected in the actual network.

Because many configurations produce large numbers of apparently isolated objects, usually hosts, IP Availability Manager only creates partitions with two or more devices.

You can assign names to the partitions in your network using the partition.conf file. Chapter 2, "Setting Configuration Parameters," in the *EMC Smarts IP Management Suite Configuration Guide* provides more information about naming partitions.

Attributes for Partition

Table 3-20 lists some key attributes for Partition.

Table 3-20 Attributes for Partition

Attribute	Description	Allowed values
DisplayName	Name, as shown in the Global Console, of this Partition; for example: Partition-0/QAlab	String
Name	Name, as known in the modeled topology, of this Partition; for example: Partition-0/QAlab	String
NumberOfSystems	Number of member systems for this Partition; for example: 140	Integer
PartitionKey	Unique value that distinguishes this Partition from all other Partitions; for example: 0/QAlab	String

Root-cause problems for Partition

The following root-cause problem is diagnosed for Partition:

Down: Indicates that all systems in a partition are unresponsive. This typically means that there is a failure in an unknown or unmanaged device connecting the partition to the managed network. The events used to diagnose Partition Down are system Unresponsive for all members of the partition.

Events for Partition

No events are detected for Partition.

Management agent

A management agent is a logical object that contains the information necessary to represent, configure, or manage some functionality provided by a device or software feature. IP Availability Manager supports connectivity analysis of the following management agent object types:

- SNMPAgent—An agent that manages and monitors network systems and their functions. It implements one or more MIBs and provides access to MIB data for management applications. An SNMPAgent typically listens on UDP port 161.
- VRAgent—An agent that manages and monitors virtual routers, and their functions and interfaces.

Attributes for management agent

Because VRAgent is a subclass of SNMPAgent, the attributes of a VRAgent are the same as the attributes of an SNMPAgent with the following exception: the VRAgent has an additional attribute called RouterID.

Table 3-21 lists some key attributes for management agent.

Table 3-21 Attributes for management agent

Attribute	Description	Allowed values
AgentAddress	IP address used by the initial ICMP poll to contact this management agent; for example: 10.9.1.108	String
AgentAddressList	List of IP addresses discovered on the system hosting this management agent. **Note:** The IP address set for the AgentAddress attribute is always the first entry in this list.	String
AuthPass	SNMPv3 only: Authentication password of the user for the SNMP engine of this management agent.	String
AuthProtocol	SNMPv3 only: Protocol used to authenticate the SNMP request sent to this management agent.	Enum: • MD5 • SHA • NONE (default)
DisplayName	Name, as shown in the Global Console, of this management agent; for example: SNMPAgent-asm-swwas0	String
EngineBoots	SNMPv3 only: Number of times that the SNMP engine of this management agent has initialized or reinitialized since its last configuration.	Integer
EngineBootTime	SNMPv3 only: Date and time that the SNMP engine of this management agent last initialized or reinitialized.	String

Table 3-21 Attributes for management agent (continued)

Attribute	Description	Allowed values
EngineID	SNMPv3 only: Identifier that uniquely identifies the SNMP engine of this management agent; for example: 800002b804616263	String
IsSystemUnresponsive	TRUE if the system hosting this management agent is not responding to ICMP pings or SNMP polls. (FALSE if the host system is responding to ICMP pings and/or SNMP polls.)	Boolean: true or false
Name	Name, as known in the modeled topology, of this management agent; for example: SNMPAgent-asm-swwas0	String
PortNumber	Port number used by the first SNMP poll to successfully communicate with this management agent.	Integer: 161 by default
PrivPass	SNMPv3 only: Encryption password of the user for the SNMP engine of this management agent.	String
PrivProtocol	SNMPv3 only: Protocol used to encrypt SNMP request sent to this management agent.	Enum: • DES • AES • NONE (default)
ProbeSuccessful	TRUE if this management agent was successfully probed by the discovery probes.	Boolean: true or false
ReadCommunity	SNMPv1 or v2c only: SNMP read community string used by the first SNMP poll to successfully communicate with this management agent.	String: public by default
RouterID	Applicable to VRAgent only: Identifier (index) for this VRAgent.	Integer
SeedName	Original name specified for the system hosting this management agent; for example: asm-swwas0 The seed name is typically the name listed in a seed file.	String

Table 3-21 Attributes for management agent (continued)

Attribute	Description	Allowed values
SNMPStatus	Current state of this management agent as reported by the instrumentation. • OK indicates that the agent is responding to SNMP requests. • AUTHFAILURE indicates an authentication failure to an SNMP request. • TIMEDOUT indicates that the agent is not responding to SNMP requests but that the host system is responding to ICMP pings. • UNREACHABLE indicates that the host system is not responding to ICMP pings. • OTHER indicates that an unspecified failure occurred. • UNKNOWN indicates that the agent has yet to be polled.	Enum: • OK • AUTHFAILURE • TIMEDOUT • UNREACHABLE • OTHER • UNKNOWN
SNMPVersion	SNMP protocol version used by the first SNMP poll to successfully communicate with this management agent. • V1 indicates that SNMPv1 was used by the first SNMP poll to successfully communicate with the agent. • V2C indicates that SNMPv2c was used by the first SNMP poll to successfully communicate with the agent. • V3 indicates that SNMPv3 was used by the first SNMP poll to successfully communicate with the agent. The SNMPVersion attribute value is set to "'unknown_SNMP_version" for a management agent that does not support any of the SNMP protocol versions.	Enum: • V1 • V2C • V3
Status	Current status of this management agent.	Enum: • RESPONSIVE • UNRESPONSIVE • UNKNOWN
SupportsSNMP	TRUE if this management agent was contacted successfully at least once using the SNMP protocol.	Boolean: true or false
sysDescr	Description of the system hosting this management agent; for example: Ethernet Stackable Switching System	String
sysLocation	Description of where the system hosting this management agent is located; for example: QARack2_ASM_setup	String
sysName	Administratively assigned name for the system hosting this management agent; for example: asm-swwas0 By convention, this name is the host's fully qualified domain name (FQDN).	String

Table 3-21 Attributes for management agent (continued)

Attribute	Description	Allowed values
sysObjectID	System object identifier associated with the vendor of the system hosting this management agent; example: .1.3.6.1.4.1.674.10895.3002	String
SystemName	Name of the system hosting this management agent; for example: asm-swwas0	String
TopologyUpdateInfo	Table of topology information discovered through this management agent.	struct[]
User	SNMPv3 only: Name of the user included in the SNMP request sent to this management agent.	String
WriteCommunity	SNMPv1 or v2c only: SNMP write community string for this management agent.	String

Root-cause problems for management agent

A management agent can be an SNMP agent or a VR agent. The following root-cause problem is diagnosed for management agent:

NotResponding: Indicates that a management agent is not responding to SNMP requests but that the host system is responding to ICMP pings. Typically, this situation is caused by the use of an incorrect community string (SNMPv1 or v2c), or the agent might be hung.

The event used to diagnose management agent NotResponding is management agent Unresponsive.

Events for management agent

Table 3-22 lists the events detected for management agent and used as symptoms for root-cause analysis. Neither event is exported to the Global Manager.

Table 3-22 Events for management agent

Event	Description
Unresponsive	Indicates that the management agent is not responding to SNMP requests but that the system hosting the management agent is responding to ICMP pings.
RepeatedRestarts	Indicates that IP Availability Manager has received an abnormal number of Restart traps from the management agent within a short period of time. This event is used to diagnose system Unstable problems. The RestartTrapThreshold and the RestartTrapWindow parameters in the Connectivity setting for the "System Resources Groups" threshold group control the analysis for a system unstable condition. Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide* provides information about these parameters.

Redundancy group

A redundancy group consists of two or more objects of the same type that are configured in such a way as to provide backup resources for critical network objects. For example, two routers accessing the same host may be modeled as a redundancy group containing the two routers. If one router fails, the redundancy is "at risk." If both fail, all capability is lost.

IP Availability Manager supports the creation and analysis of redundancy groups for the following objects:

- CardRedundancyGroup—Consists of two or more Card objects that participate in a redundant configuration.
- NetworkAdapterRedundancyGroup—Consists of two or more Port or Interface objects that participate in a redundant configuration.
- NetworkConnectionRedundancyGroup—Consists of two or more NetworkConnection, Cable, or TrunkCable objects that participate in a redundant configuration.
- SystemRedundancyGroup—Consists of two or more system (Switch, Router, Hub, Bridge, Host) objects that participate in a redundant configuration.
- HSRPGroup—Consists of two or more Cisco devices that support the Hot Standby Router Protocol (HSRP) and are configured to ensure that user traffic recovers immediately and transparently from first hop failures in network edge devices or access circuits. The devices are connected to the same segment of a network and, using HSRP, work together to present the appearance of a single router on the LAN. The devices in an HSRPGroup share an IP address and a MAC (Layer 2) address.

Attributes for redundancy group

Table 3-23 lists some key attributes for redundancy group.

Table 3-23 Attributes for redundancy group

Attribute	Description	Allowed values
AtRiskThreshold	Set to a value representing the number of responsive or operational member objects in this redundancy group. By default, AtRiskThreshold is set to 1.	Integer
IsAnyComponentDown	TRUE if at least one member object in this redundancy group is unresponsive or non-operational. (FALSE if all member objects in this redundancy group are responsive or operational.)	Boolean: true or false

Table 3-23 Attributes for redundancy group (continued)

Attribute	Description	Allowed values
IsEveryComponentDown	TRUE if all member objects in this redundancy group are unresponsive or non-operational. (FALSE if at least one member object in this redundancy group is responsive or operational.)	Boolean: true or false
NumberOfComponents	Number of member objects in this redundancy group.	Integer
NumberOfFaultyComponents	Number of member objects in this redundancy group that are unresponsive or non-operational.	Integer

Root-cause problems for redundancy group

No root-cause problems are diagnosed for redundancy group.

Events for redundancy group

Table 3-24 lists the events detected for redundancy group and exported to the Global Manager. None of the events are used as symptoms for root-cause analysis.

Table 3-24 Events for redundancy group

Event	Description
AllComponentsDown	None of the member objects in the redundancy group are responsive or operational.
AtRisk	The number of responsive or operational members in the redundancy group is less than or equal to the AtRiskThreshold value (set to 1 by default) but is not zero. **Note:** If the number of responsive or operational members is zero, an AllComponentsDown event occurs. For example, and assuming AtRiskThreshold = 1, the state of a three-member redundancy group having one responsive or operational member (and two unresponsive or non-operational members) is AtRisk.
ReducedRedundancy	The number of responsive or operational members in the redundancy group is greater than the AtRiskThreshold value but is less than the total number of members in the redundancy group. For example, and assuming AtRiskThreshold = 1, the state of a three-member redundancy group having two responsive or non-operational members (and one unresponsive or non-operational member) is ReducedRedundancy.

As shown in Table 3-24, the state of a redundancy group is based on the status of its member objects and the value of the AtRiskThreshold attribute (set to 1 by default). If all members of a redundancy group are responsive or operational, the state of the redundancy group is Normal.

Attributes for HSRPGroup

Table 3-25 lists some key attributes for HSRPGroup.

Table 3-25 Attributes for HSRPGroup

Attribute	Description	Allowed values
AtRiskThreshold	Set to a value representing the number of responsive or operational member HSRPEndpoints in this HSRPGroup. By default, AtRiskThreshold is set to 1.	Integer
DisplayName	Name, as shown in the Global Console, of this HSRPGroup; for example: HSRPGroup-10.1.16.254 [Group 16]	String
GroupNumber	Number assigned to this HSRPGroup; for example: 16	String
HsrpEpStateChanged	TRUE if one or more member HSRPEndpoints in this HSRPGroup are not operational. (FALSE if all member HSRPEndpoints in this HSRPGroup are operational.)	Boolean: true or false
IsAnyComponentDown	TRUE if at least one member HSRPEndpoint in this HSRPGroup is not operational. (FALSE if all member HSRPEndpoints in this HSRPGroup are operational.)	Boolean: true or false
IsAnyHSRPEndpointActive	TRUE if at least one HSRPEndpoint in this HSRPGroup is active. (FALSE if no HSRPEndpoint in this HSRPGroup is active.)	Boolean: true or false
IsEveryComponentDown	TRUE if all member HSRPEndpoints in this HSRPGroup are unresponsive or non-operational. (FALSE if at least one member HSRPEndpoint in this HSRPGroup is responsive or operational.)	Boolean: true or false
IsEveryHSRPEndpointReady	TRUE if all HSRPEndpoints in this HSRPGroup have been polled.	Boolean: true or false
IsGroupPartOfSingle-UnresponsiveSystem	TRUE if all HSRPEndpoints in this HSRPGroup are part of a single, unresponsive system.	Boolean: true or false
Name	Name, as known in the modeled topology, of this HSRPGroup; for example: HSRP-GROUP-10.1.16.254	String
NumberOfComponents	Number of member HSRPEndpoints in this HSRPGroup; for example: 2	Integer

Table 3-25 Attributes for HSRPGroup (continued)

Attribute	Description	Allowed values
NumberOfFaultyComponents	Number of member HSRPEndpoints in this HSRPGroup that are unresponsive or non-operational; for example: 0	Integer
VirtualIP	Primary virtual IP address used by this HSRPGroup; for example: 10.1.16.254	String
VirtualMAC	Primary virtual MAC address used by this HSRPGroup.	String

Root-cause problems for HSRPGroup

No root-cause problems are diagnosed for HSRPGroup.

Events for HSRPGroup

The following event is detected for HSRPGroup and exported to the Global Manager:

SwitchOverFailed: Indicates that traffic fails to switch from an active interface to a standby interface in an HSRPGroup and that all interfaces in the HSRPGroup are inactive.

The SwitchOver event is not used as a symptom for root-cause analysis.

Monitoring and analysis of a redundancy group

Monitoring and analysis of a redundancy group occurs automatically when a redundancy group is created and its member objects are inserted into the group. Appendix D, “Redundancy Group Creation,” provides information about how redundancy groups are created.

4

Diagnosis of Unstable Objects

This chapter describes how IP Availability Manager determines whether a system or a network adapter is unstable. It consists of the following sections:

- Overview of trap analysis 4-2
- Thresholds associated with unstable analysis 4-3
- Example of unstable analysis 4-4
- Unstable notifications for backup or dial-on-demand interfaces 4-5

Overview of trap analysis

A system or network adapter is considered to be unstable if it fluctuates too often between up and down states over a short period of time.

IP Availability Manager monitors a system or network adapter's state through the SNMP traps it receives. IP Availability Manager determines when to generate an Unstable notification based on a combination of fixed values and user-controlled settings. IP Availability Manager also calculates a stable time in which to wait before clearing an Unstable notification.

IP Availability Manager monitors the following SNMP traps to determine a change in an object's state:

- coldStart and warmStart traps for a system
- linkUp or linkDown traps for a network adapter

Monitoring these traps is described in Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide*.

Note: IP Availability Manager primarily uses linkDown traps for the analysis of unstable network adapters. However, for devices that only send linkUp traps, IP Availability Manager does use linkUp traps. When a device sends both linkUp and linkDown traps, IP Availability Manager uses linkDown traps for the unstable analysis.

Thresholds associated with unstable analysis

IP Availability Manager uses the following values to diagnose an object as unstable:

- Minimum Traps—The minimum number of Link/Restart traps received in order to conclude that the object is unstable. This variable is set by the LinkTrapThreshold parameter (contained in the Interface/Port Flapping setting) for network adapters and the RestartTrapThreshold parameter (contained in the Connectivity setting) for systems.
- Trap Window—The period within which the Minimum Traps must be received to declare the object unstable. This window is set by the LinkTrapWindow parameter (contained in the Interface/Port Flapping setting) for network adapters and the RestartTrapWindow parameter (contained in the Connectivity setting) for systems. Once an object is declared unstable, IP Availability Manager computes the Stable Time.
- Stable Time—The amount of time that must elapse without additional Link/Restart traps before IP Availability Manager declares the object stable again. Stable Time depends on the length of time that the object was unstable. This is at least as large as the unstable length of time, and at least as large as the Trap Window. However, the stable time cannot be longer than one hour.

Example of unstable analysis

Figure 4-1 illustrates how a system or network adapter is diagnosed as being unstable.

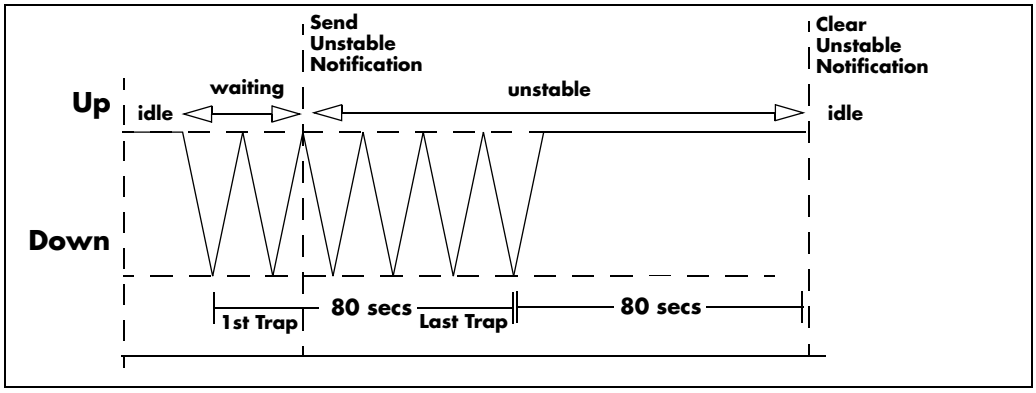

Figure 4-1 **Unstable system/network adapter diagnosis**

In the example, assume that the Link/RestartTrapWindow parameter has a value of 30 seconds and that the Link/RestartTrapThreshold parameter has a value of 2. IP Availability Manager performs the following actions:

1. As soon as IP Availability Manager receives a linkDown trap from a physical port or interface (or a coldStart/warmStart trap from a system), it begins counting.
2. When IP Availability Manager receives two or more traps within the 30-second Trap Window, it considers the network adapter or system to be unstable and sends an Unstable notification. The Minimum Traps variable (set by the Link/RestartTrapWindow parameter) determines the number of traps (2) that IP Availability Manager must receive within the Trap Window (set by the Link/RestartTrapWindow parameter) before IP Availability Manager considers an object unstable.
3. IP Availability Manager continues to receive traps for 80 seconds after the initial trap. This results in a Stable Time of 80 seconds.

   The Stable Time is the amount of time IP Availability Manager waits before it clears the Unstable notification. In our example, the Stable Time is set at 80 seconds since it is greater than the Trap Window (30 seconds) and less than one hour.

As you can see, IP Availability Manager uses a relative measure to determine how long an object must be stable before it clears the Unstable notification. This measure is proportional to the amount of time an object is unstable. The longer an object is unstable the longer it must be stable before the Unstable notification is cleared. Because the object in our example remains stable for 80 seconds, IP Availability Manager clears the Unstable notification no sooner than 80 seconds after it receives the final trap.

Unstable notifications for backup or dial-on-demand interfaces

By default, the Interface/Port Flapping (Unstable) setting is not associated with backup interfaces or with dial-on-demand interfaces. This means, by default, that IP Availability Manager will not generate Unstable notifications for the interfaces in those groups.

To enable diagnosis of Unstable notifications for backup interfaces or dial-on-demand interfaces, perform these steps:

1. Add the Interface/Port Flapping setting to the Backup or Dial-on-Demand groups.
2. Configure the Interface/Port Flapping setting's parameters accordingly.
3. Reconfigure your Polling and Thresholds groups using the Reconfigure toolbar button on the Domain Manager Administration Console.

Table 4-1 summarizes the notifications that may appear after you apply the Interface/Port Flapping setting to backup interfaces or dial-on-demand interfaces.

Table 4-1 Combined settings and their notifications

Settings	Resulting Notifications
Interface/Port Flapping Backup Interface Support	• The Down notification is not generated if the interface is down. • The BackupActivated notification is generated if the interface comes up. • The ExceededMaximumUptime notification is generated if the interface stays up too long. • The Unstable notification is generated if the interface or port is going up and down.
Interface/Port Flapping Dial-On-Demand Interface Support	• The Down notification is not generated if the interface is down. • The ExceededMaximumUptime notification is generated if the interface stays up too long. • The Unstable notification is generated if the interface or port is going up and down.

Chapter 5, "Using the Polling and Thresholds Console," in the *EMC Smarts IP Management Suite Configuration Guide* provides instructions for working with groups and settings.

A

MIBs Polled and SNMP Traps Processed

This appendix identifies the MIBs and SNMP traps used by IP Availability Manager to diagnose connectivity 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 Availability Manager polls the following standard MIBs:

- ATM-MIB (RFC 2515)
- BRIDGE-MIB (RFC 1493)
- DS3-MIB (RFC 2496)
- ENTITY-MIB (RFC 2737)
- ETHERLIKE-MIB (RFC 1650)
- FDDI-MIB (1285)
- FDDI-SMT73-MIB (RFC 1512)
- FRAME-RELAY-DTE-MIB (RFC 2115)
- IF-MIB (RFC 1573)
- IP-MIB (RFC 2011)
- IPSEC-ISAKMP-IKE-DOI-TC SNMP MIB
- ISDN-MIB (RFC 2127)
- RFC1406-MIB (RFC 1406)
- RFC1286-MIB
- SNMP MIB-II (RFC 1213)

Enterprise MIBs polled

IP Availability Manager polls the following vendor-specific MIBs:

- AI194HUB-MIB
- AI198CLC-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-FRAME-RELAY-MIB
- CISCO-FRU-CONTROL-MIB
- CISCO-HSRP-MIB
- CISCO-IETF-IP-MIB
- CISCO-PAGP-MIB
- CISCO-PROCESS-MIB
- CISCO-RF-MIB
- CISCO-RHINO-MIB
- CISCO-STACK-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- OLD-CISCO-INTERFACES-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)
- JUNIPER-MIB
- JUNIPER-IPv6-MIB
- LANPLEX-SYSTEM-MIB-1-1-1
- NRC-MultiGate MIB
- RAPID CITY
- REPEATER-REV4-MIB (Cabletron)
- SSG-5000-CHASSIS-MIB (Shasta)
- STRATACOM-MIB
- SW-MIB (BCSI)
- SYNOPTICS-LS-ETHERNET-MIB
- UNISPHERE-DATA-ERX-SYSTEM-MIB
- Wellfleet-CCT-NAME-MIB
- Wellfleet-HARDWARE-MIB
- Wellfleet-IP-MIB
- XYLAN-BASE-MIB

SNMP traps processed

IP Availability 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 SNMPAgent

IP Availability 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 Availability Manager for discovery purposes.

Table A-1 SNMP traps processed by IP Availability 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 Availability Manager processes this trap but takes no action.
** IP Availability 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 Availability Manager place the associated device (which is already in the modeled topology) on the Pending Devices list. During the next pending discovery, IP Availability 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 Availability Manager extracts the information from the trap message and updates the appropriate device attributes.

Note: IP Availability Manager uses trap messages and the results obtained from periodic SNMP polling to diagnose network failures that interrupt network connectivity.

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

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

Trap type	Trap name	MIB module
Generic traps	coldStart	Standard SNMP (RFC 1215 MIB)
	warmStart	
	linkUp	
	linkDown	
Enterprise-specific traps for Applied Innovation	<Smart Line Card> Down For example: AI294 Down	AI198CLC-MIB
	<Smart Line Card> Up	
Enterprise-specific traps for Cisco	cefcModuleStatusChange	CISCO-ENTITY-FRU-CONTROL-MIB
	cHsrpStateChange	CISCO-HSRP-MIB
	ciscoConfigManEvent	CISCO-CONFIG-MAN-MIB
	demandNbrlayer2Change	CISCO-ISDN-MIB
	moduleDown	CISCO-STACK-MIB
	moduleUp	
	sysConfigChangeTrap	
Enterprise-specific traps for MRV Communications	(card fault)	NSTACK-MIB
	(port fault)	
Enterprise-specific traps for Riverstone Networks	rsEnvirBackupControl-ModuleOnline (card fault)	RIVERSTONE-NOTIFICATIONS-MIB

Upon receiving a coldStart, warmStart, ciscoConfigManEvent, or sysConfigChangeTrap trap for a device already in the modeled topology, IP Availability Manager places the device on the Pending Devices list and generates a SystemRestarted or ConfigChange trap for input to the EMC Smarts Service Assurance Manager Adapter Platform (Adapter Platform). During the next pending discovery, IP Availability Manager will send SNMP polls to the device to rediscover the device and its components.

Chapter 2, "Setting Configuration Parameters," in the *EMC Smarts IP Management Suite Configuration Guide* provides more information about the SystemRestarted and ConfigChange traps, including procedures for enabling the generation of these traps.

B

Network Topology Naming Conventions

This appendix describes the naming conventions used by IP Availability 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).

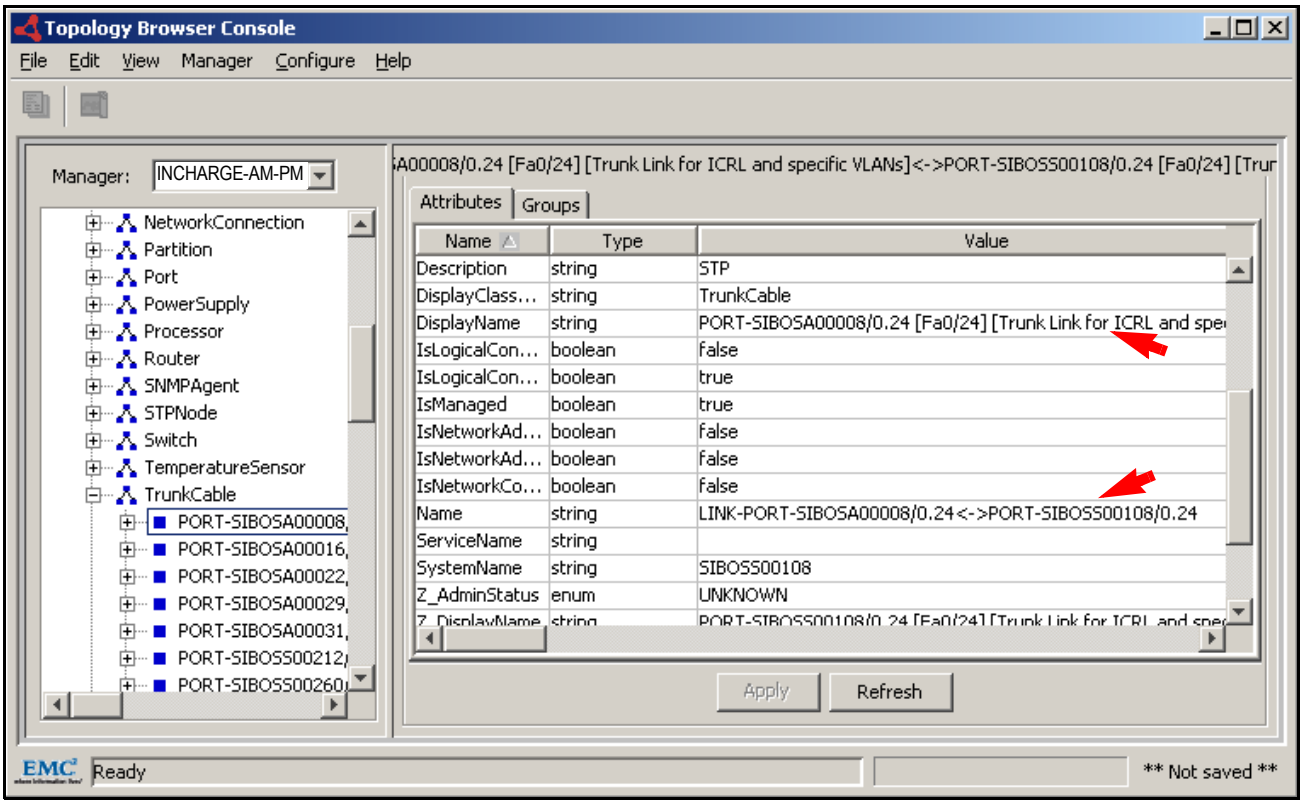

Figure B-1 **DisplayName and Name attributes for a network object**

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 Availability 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 Availability 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 Availability 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/FQDN*>/INDEX
	Display Name: NAME [SLOT] [CARDTYPE]
Chassis	Name: CHASSIS-<*IP/FQDN*>
	Display Name: CHASSIS-<*IP/FQDN*>
Rack	Name: RACK-<*IP/FQDN*>
	Display Name: RACK-<*IP/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/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: NAME [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: NAME
Logical devices	
Disk	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	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

Problem, Event, and Notification Summary

This appendix summarizes the root-cause problems diagnosed by IP Availability Manager, the events correlated by IP Availability Manager to diagnose the problems, and the notifications imported by the Global Manager. It consists of the following sections:

- Problems and events C-2
- Notifications C-4

Problems and events

Table C-1 lists, on a managed object basis, the root-cause problems (p) diagnosed by IP Availability Manager and the events (e) detected by IP Availability Manager to diagnose problems.

Table C-1 Problems and events diagnosed/detected by IP Availability Manager

Managed object	Event	Class of origin
System	Down (p)	UnitaryComputerSystem
	Unstable (p)	
	Unresponsive (e)	
	DiscoveryError (e)	
Chassis	Down (p)	Chassis
Card	Down (p)	Card
	OperationallyDown (e)	
	SwitchOver (e)	
Network adapter	Down (p)	NetworkAdapter
	Unstable (p)	
	Disabled (p)	
	LogicalConnectionDown (p)	
	BackupActivated (e)	NetworkAdapter_Fault
	ExceededMaximumUptime (e)	
	AdministrativelyDown (e)	
	DownOrFlapping (e)	
Device connection	Down (p)	ICIM_NetworkDeviceConnection
	Unstable (p)	
	DownOrFlapping (e)	
IP	Down (e)	IP
	Unresponsive (e)	
IPv6	Down (e)	IPv6
	Unresponsive (e)	
DuplicateIP	Duplicate (e)	DuplicateIP
HSRPEndpoint	SwitchOver (e)	HSRPEndPoint
Partition	Down (p)	Partition
SNMPAgent	NotResponding (p)	SNMPAgent
	Unresponsive (e)	SNMPAgent_Fault (an instrumentation object)
	RepeatedRestarts (e)	

Table C-1 Problems and events diagnosed/detected by IP Availability Manager (continued)

Managed object	Event	Class of origin
VRAgent	NotResponding (p)	VRAgent
	Unresponsive (e)	VRAgent_Fault (an instrumentation object)
	RepeatedRestarts (e)	
CardRedundancyGroup	AllComponentsDown (e)	CardRedundancyGroup
	AtRisk (e)	
	ReducedRedundancy (e)	
NetworkAdapter-RedundancyGroup	AllComponentsDown (e)	NetworkAdapterRedundancyGroup
	AtRisk (e)	
	ReducedRedundancy (e)	
NetworkConnection-RedundancyGroup	AllComponentsDown (e)	NetworkConnectionRedundancyGroup
	AtRisk (e)	
	ReducedRedundancy (e)	
SystemRedundancyGroup	AllComponentsDown (e)	SystemRedundancyGroup
	AtRisk (e)	
	ReducedRedundancy (e)	
HSRPGroup	SwitchOverFailed (e)	HSRPGroup
	AllComponentsDown (e)	
	AtRisk (e)	
	ReducedRedundancy (e)	
KEY (p) = Root-cause problem (e) = Event		

Note: IP Availability Manager does not use IP Down, IP Unresponsive, IPv6 Down, or IPv6 Unresponsive events to diagnose any root-cause problems.

Note: IP Availability Manager also generates an IPv6Network Inaccessible exception, which contains one or more IPv6 Down events.

Notifications

Table C-2 lists, on a managed object basis, all of the IP Availability Manager notifications imported by the Global Manager.

Table C-2 IP Availability Manager notifications imported by the Global Manager

Managed object	Event	Class of Origin
System	Down (p)	UnitaryComputerSystem
	Unstable (p)	
	DiscoveryError (e)	
	Unresponsive (e)	
Chassis	Down (p)	Chassis
Cards	Down (p)	Card
	SwitchOver (e)	
Network adapter	Down (p)	NetworkAdapter
	Disabled (p)	
	LogicalConnectionDown (p)	
	Unstable (p)	NetworkAdapter_Fault (an instrumentation object)
	BackupActivated (e)	
	ExceededMaximumUptime (e)	
Device connection	Down (p)	ICIM_NetworkDeviceConnection
	Unstable (p)	
	DownOrFlapping (e)	
IPv6	Down (e)	IPv6
DuplicateIP	Duplicate (e)	DuplicateIP
HSRPEndpoint	SwitchOver (e)	HSRPEndPoint
Partition	Down (p)	Partition
SNMPAgent	NotResponding (p)	SNMPAgent
VRAgent	NotResponding (p)	VRAgent
CardRedundancyGroup	AllComponentsDown (e)	CardRedundancyGroup
	AtRisk (e)	
	ReducedRedundancy (e)	
NetworkAdapter-RedundancyGroup	AllComponentsDown (e)	NetworkAdapterRedundancyGroup
	AtRisk (e)	
	ReducedRedundancy (e)	

Table C-2 IP Availability Manager notifications imported by the Global Manager (continued)

Managed object	Event	Class of Origin
NetworkConnection-RedundancyGroup	AllComponentsDown (e)	NetworkConnectionRedundancyGroup
	AtRisk (e)	
	ReducedRedundancy (e)	
SystemRedundancyGroup	AllComponentsDown (e)	SystemRedundancyGroup
	AtRisk (e)	
	ReducedRedundancy (e)	
HSRPGroup	SwitchOverFailed (e)	HSRPGroup
	AllComponentsDown (e)	
	AtRisk (e)	
	ReducedRedundancy (e)	
KEY (p) = Root-cause problem (e) = Event		

Note: The Global Manager also imports the IPv6Network Inaccessible exception.

D

Redundancy Group Creation

This appendix discusses the automatic and manual creation of redundancy groups. It consists of the following sections:

- Creation of card redundancy groups D-2
- Creation of system redundancy groups D-3
- Creation of network adapter redundancy groups D-4
- Creation of HSRPGroups D-6

Creation of card redundancy groups

IP Availability Manager automatically creates CardRedundancyGroups during discovery for Cisco devices that support the CISCO-STACK-MIB. Each such group is composed of two cards. You can view the card redundancy groups and their members using the Domain Manager Administration Console.

In addition, you can create redundancy groups for cards that do not support the CISCO-STACK-MIB. The process for manually creating a card redundancy group is similar to that for creating a system redundancy group, described in the following section. First, create an instance of the CardRedundancyGroup class and then insert the cards that participate in the redundancy group into the ComposedOf relationship.

Creation of system redundancy groups

Redundancy groups for network adapters, network connections, and systems must be manually created using the dmctl utility or an Adapter Scripting Language (ASL) script.

To create a redundancy group for one of these types of objects:

1. Create an instance of one of the redundancy group classes.
2. Insert the objects that participate in the redundancy group into the ComposedOf relationship of the redundancy group.

The following example uses the dmctl utility to create an instance of a system redundancy group and inserts two members into the group.

```
/opt/InCharge7/IP/smarts/bin/dmctl -s INCHARGE-AM-PM
Server INCHARGE-AM-PM User: admin
admin's Password: XXXXXXXX
Domain Manager Control Program (V7.0.0.0) -- Type 'help' for a list of
   commands.
Attached to 'INCHARGE-AM-PM'
dmctl> create SystemRedundancyGroup::RouterRedundancyGroup
dmctl> insert SystemRedundancyGroup::RouterRedundancyGroup::
   ComposedOf Router::router1.smarts.com
dmctl> insert SystemRedundancyGroup::RouterRedundancyGroup::
   ComposedOf Router::router2.smarts.com
```

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

Network adapter, network connection, and system redundancy groups can be viewed through the Domain Manager Administration Console or the Topology Browser view of the Global Console.

Creation of network adapter redundancy groups

The status of a network adapter redundancy group changes when at least one adapter in the group is flapping or has a status of down, disabled, not present, or testing.

Note: By default, a value of testing for the network adapter's status results in a Down notification. You can modify this behavior with the Testing Notification Mode, which is described in Chapter 7, "Customizing Polled Data Thresholds," in the *EMC Smarts IP Management Suite Configuration Guide*.

In addition, you can create a network adapter redundancy group where the status calculation considers the state of the system containing the adapter. System status is useful when the group's members come from multiple systems. You determine the behavior by the topology you create. When all the network adapters in a group come from the same system, you can make the group PartOf a UnitaryComputerSystem. This prevents the unresponsive status of the system from affecting the status calculation.

The following examples use ASL code fragments to show several different network adapter redundancy groups.

In the first example, both network adapters are part of the host named host_1. Because of this, the redundancy group is inserted into the PartOf relationship with the host. If host_1 is unresponsive, IP Availability Manager does not generate any notifications about the redundancy group. If the group is not part of the system, IP Availability Manager would notify AllComponentsDown when host_1 is unresponsive.

Also note the use of the LayeredOver relationship from the network adapter redundancy group to the system. This information is used to draw maps of network adapter redundancy groups in the Global Manager.

```
rg = create("NetworkAdapterRedundancyGroup",
         My-Redundancy-Group");
//
// Turns off system status calc
rg->PartOf += object("Host", "host_1");
//
// For service map
rg->LayeredOver += object("Host", "host_1");
//
rg->ComposedOf += object("Interface", "IF-host_1/1");
rg->ComposedOf += object("Interface", "IF-host_1/2");
```

In the next example, the network adapters are from different systems. Because of this, the redundancy group is not inserted into the PartOf relationship with any system. As a result, the status of this redundancy group is based on the status of the adapters and the responsive state of their containing systems.

```
rg = create("NetworkAdapterRedundancyGroup",
         My-Redundancy-Group");
//
rg->ComposedOf += object("Interface", "IF-host_1/1");
rg->ComposedOf += object("Interface", "IF-host_2/2");
//
// For service map
rg->LayeredOver += object("Host", "host_1");
rg->LayeredOver += object("Host", "host_2");
```

In the next example, the network adapters are from a single system but the system status is considered in the status calculation because the group is not a part of a system.

```
rg = create("NetworkAdapterRedundancyGroup",
         My-Redundancy-Group");
//
// For service map
rg->LayeredOver += object("Host", "host_3");
//
rg->ComposedOf += object("Interface", "IF-host_3/1");
rg->ComposedOf += object("Interface", "IF-host_3/2");
```

In the final example, the network adapters are from a single system but the system status is not included in the status calculation for the redundancy group. Again, this is because the group is inserted into the PartOf relationship with the system which is composed of the network adapters.

```
rg = create("NetworkAdapterRedundancyGroup",
         My-Redundancy-Group");
//
// Turns off system status calc
rg->PartOf += object("Host", "host_4");
//
// For service map
rg->LayeredOver += object("Host", "host_4");
//
rg->ComposedOf += object("Interface", "IF-host_4/1");
rg->ComposedOf += object("Interface", "IF-host_4/2");
```

Creation of HSRPGroups

During discovery, IP Availability Manager automatically creates HSRPGroups for Cisco devices that support the CISCO-HSRP-MIB and are configured in an HSRPGroup. Each such group is composed of two or more routers and their interfaces.

You can view the HSRPGroups and their members using the Domain Manager Administration Console and the Global Console. Analysis and monitoring of a HSRPGroup occurs automatically after the group is created and its member routers are inserted into the group.

Index

A

AdminStatus attribute 3-20, 3-26, 3-38, 3-42
All components down 3-57
Analysis 1-3
At risk 3-57
AtRiskThreshold 3-57
Attribute
    AdminStatus 3-20, 3-26, 3-38, 3-42
    AtRiskThreshold 3-57
    Card
        StandbyStatus 3-16
        Status 3-17
    Certification 3-9
    Chassis
        BackplaneUtilization 3-14
        Status 3-15
    DiscoveryErrorInfo 3-13
    DisplayName B-3
    IPStatus 3-35, 3-37, 3-38, 3-41, 3-42
    IsFlapping 3-21, 3-25, 3-26
    IsLogicalConnection 3-3
    IsNetworkAdapterDownOrFlapping 3-29
    IsNetworkAdapterFlapping 3-3, 3-29, 3-32
    IsSwitchOverActive 3-44
    IsUnresponsive 3-9
    Name B-3
    OperStatus 3-22, 3-38, 3-42
    StandbyStatus 3-16
    State 3-45
    StateChange 3-45
    Status 3-17
Attributes
    DisplayName B-2
    Name B-2

B

BackplaneUtilization attribute 3-14
Backup interface support setting
    Unstable notification 4-5
Bridge 3-8

C

Cable 3-27
Card 3-16
    Down 3-3, 3-17
        Symptoms of 3-17
    Operationally down 3-5, 3-18
    Redundancy group 3-56
    Switch over 3-5, 3-18
Certification attribute 3-9
Chassis 3-14
    Down 3-3, 3-15
        Symptoms of 3-15
Codebook 1-3
Connectivity exception
    System 3-12
    VLAN 3-49
Connectivity setting 4-3
    Restart trap threshold 3-11, 3-55
    Restart trap window 3-11, 3-55
    Testing notification mode 3-24
Containment 2-20
Containment dialog box 2-20
    Opening 2-20

D

Device connection 3-27
    Cable 3-27
    Down 3-3, 3-31
        Symptoms of 3-31
    Down or flapping 3-5, 3-32
    Network connection 3-27
    Trunk cable 3-27
    Unstable 3-3, 3-32
        Symptoms of 3-32
Device support
    MSFCs 2-13
    Physical routers 2-13
    RSFCs 2-13
    RSMs 2-13
    Virtual routers 2-13
Dial-on-demand interface setting
    Unstable notification 4-5
Disabled

Network adapter 3-25
Discovery error 3-13
discovery.conf
MinimumDemandGet 2-9
DiscoveryErrorInfo attribute 3-13
DisplayName attribute B-2, B-3
Domain Manager
Containment 2-20
Down
Card 3-17
Chassis 3-15
Device connection 3-31
IP 3-38, 3-42
Network adapter 3-23
Partition 3-51
System 3-11
Duplicate
Duplicate IP 3-39, 3-43
Duplicate IP
Duplicate 3-5, 3-39, 3-43

E

Edges
Table of 2-12, 2-13
Event 1-4
Card
Operationally down 3-5, 3-18
Switch over 3-5, 3-18
Device connection down or flapping 3-5, 3-32
Duplicate IP
Duplicate 3-5, 3-39, 3-43
HSRP endpoint
Switch over 3-46
HSRP group
Switch Over 3-5
Switch over failed 3-5, 3-59
IP
Down 3-5, 3-38, 3-42
Unresponsive 3-5, 3-39, 3-43
Network adapter
Administratively down 3-5, 3-26
Backup activated 3-5, 3-25
Down or flapping 3-5, 3-26
Exceeded maximum uptime 3-5, 3-26
Redundancy group
All components down 3-5, 3-57
At risk 3-5, 3-57
Reduced redundancy 3-5
ReducedRedundancy 3-57
SNMP agent
Repeated restarts 3-5, 3-55
Unresponsive 3-5, 3-55
System
Discovery error 3-5, 3-6, 3-12
Might be down 3-5, 3-12
Unresponsive 3-5, 3-12
Event notification
See Notification
Exception 1-4
Definition of 1-4
IPv6Network
Inaccessible 3-47
Operational 3-4
Summary table 3-4
System
Connectivity 3-4, 3-12
Operational 3-4, 3-12
VLAN
Connectivity 3-4
Operational 3-4, 3-49

F

File server 3-8
Firewall 3-8

G

Global Console 1-4, 2-1
Containment dialog box 2-20
Notification Properties dialog box 2-5, 2-20
Overview 2-4
Type of
Map Console 2-4, 2-5, 2-11
Notification Log Console 1-4, 2-5
Topology Browser Console B-2
Global Manager 1-4, 2-5

H

Host 3-8
HSRP endpoint
Switch over 3-46
HSRP Group 3-33, 3-43
Hub 3-8

I

ICMP polls 1-3
Inaccessible exception 3-47
Infrastructure
Containment 2-20
Interface 3-19
Interface/port flapping setting 4-3
Link trap threshold 3-24
Link trap window 3-24
IP
Down 3-5, 3-38, 3-42
Unresponsive 3-5, 3-39, 3-43
IP Availability Manager
Analysis 1-3
Monitoring 1-3
Notifications 1-4
IP network 2-15
Connectivity map 2-16
Membership map 2-16
IPStatus attribute 3-35, 3-37, 3-38, 3-41, 3-42
IPv6Network
Inaccessible exception 3-47
Operational exception 3-4
IsFlapping attribute 3-21, 3-25, 3-26
IsLogicalConnection attribute 3-3

IsNetworkAdapterDownOrFlapping attribute 3-29
IsNetworkAdapterFlapping attribute 3-3, 3-29, 3-32
IsSwitchOverActive attribute 3-44
IsUnresponsive attribute 3-9

L

Link trap threshold 3-24, 4-3
Link trap window 3-24, 4-3
Load balancer 3-8
Logical connection down 3-25

M

Map
- Background 2-14
- Type of 2-15
  - IP network connectivity 2-16
  - IP network membership 2-16
  - Physical connectivity 2-15, 2-17
  - VLAN connectivity 2-16
  - VLAN membership 2-16

Map Console 2-4
- Icons and indicators 2-12, 2-13
- Type of map 2-15
  - IP network connectivity 2-16
  - IP network membership 2-16
  - Physical connectivity 2-15, 2-17
  - VLAN connectivity 2-16
  - VLAN membership 2-16
- Type of maps 2-15

Maps
- IS-IS topology 2-11
- Opening 2-12

MinimumDemandGet 2-9
moduleStandbyStatus 3-18
Monitoring 1-3
Multilayer switch feature card (MSFC) 3-8

N

Name attribute B-2, B-3
Naming convention B-2
Network adapter
- Administratively down 3-5, 3-26
- Backup activated 3-5, 3-25
- Disabled 3-3, 3-25
  - Symptoms of 3-25
- Down 3-3, 3-23
  - Symptoms of 3-24
- Down or flapping 3-5, 3-26
- Exceeded maximum uptime 3-5, 3-26
- Interface 3-19
- Logical connection down 3-3, 3-25
  - Symptoms of 3-25
- Port 3-19
- Redundancy group 3-56
- Subinterface 3-19
- Unstable 3-3, 3-24
  - Symptoms of 3-24

Network connection 3-27
- Redundancy group 3-56

Node 3-8
Nodes
- Table of 2-12, 2-13

Not responding
- SNMP agent 3-55

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
- Root-cause
  - see Root-cause

Notification Log Console 1-4, 2-5
Notification Properties dialog box 2-5, 2-20
- Opening 2-5

Notifications 1-4
- Event 3-2
- Exception 3-2
- Problem 3-2

O

Object
- Naming convention B-2
- Unique name B-2

Opening a Containment dialog box 2-20
Opening a Map 2-12
Opening a Notification Properties dialog box 2-5
Operational exception
- System 3-12
- VLAN 3-49

OperStatus attribute 3-22, 3-38, 3-42

P

Partition 3-50
- Down 3-3, 3-51
  - Symptoms of 3-51

partition.conf 3-50
Permanent Virtual Circuit (PVC) 2-14
Physical connectivity map 2-15, 2-17
Polling
- ICMP 1-3
- SNMP 1-3

Port 3-19
Probe 3-8
Processing
- SNMP traps 1-3

R

Redundancy group 2-14, 3-56
- All components down 3-5
- At risk 3-5
- AtRiskThreshold 3-57

Reduced redundancy 3-5
ReducedRedundancy 3-57
Redundancy groups
States
All components down 3-57
At risk 3-57
Normal 3-57
ReducedRedundancy 3-57
Restart trap threshold 3-11, 3-55, 4-3
Restart trap window 3-11, 3-55, 4-3
Root cause 1-4
Card down 3-3, 3-17
Chassis down 3-3, 3-15
Device connection
Down 3-3, 3-31
Unstable 3-3, 3-32
Network adapter
Disabled 3-3, 3-25
Down 3-3, 3-23
Logical connection down 3-3, 3-25
Unstable 3-3, 3-24
Partition down 3-3, 3-51
SNMP agent not responding 3-3, 3-55
Summary table 3-2
System
Down 3-3, 3-11
Unstable 3-3, 3-11
Router 3-8
Router switch feature card (RSFC) 3-8
Router switch module (RSM) 3-8

S

SNMP
Polls 1-3
Trap 4-2
coldStart 4-2
linkDown 4-2
linkUp 4-2
List of A-5
warmStart 4-2
Traps 1-3
Traps for analysis purposes
List of A-6
Traps for discovery purposes
List of A-5
SNMP agent 3-52
Not responding 3-3, 3-55
Symptoms of 3-55
Repeated restarts 3-5, 3-55
Unresponsive 3-5, 3-55
SNMP trap message processing 1-3
Stable time 4-3
StandbyStatus attribute 3-16
State attribute 3-45
StateChange attribute 3-45
Status attribute 3-15, 3-17
Subinterface 3-19
Switch 3-8
Switch over
HSRP endpoint 3-46
System 3-8
Bridge 3-8
Connectivity exception 3-4, 3-12
Discovery error 3-5, 3-6, 3-12, 3-13
DisplayName attribute B-3
Down 3-3, 3-11
Symptoms of 3-11
File server 3-8
Firewall 3-8
Host 3-8
Hub 3-8
Load balancer 3-8
Might be down 3-5, 3-12
Multilayer switch feature card 3-8
Name attribute B-3
Node 3-8
Operational exception 3-4, 3-12
Probe 3-8
Router 3-8
Router switch feature card 3-8
Router switch module 3-8
Switch 3-8
Terminal server 3-8
Uncertified 3-8
Unresponsive 3-5, 3-12
Unstable 3-3, 3-11
Symptoms of 3-11
System redundancy group 3-56

T

Terminal server 3-8
Testing notification mode 3-24
Threshold
AtRiskThreshold 3-57
Restart trap threshold 3-11
Restart trap window 3-11, 3-55
Testing notification mode 3-24
Topology
Containment 2-20
Topology Browser B-2
Topology Maps
See Maps 2-15
Topology object
Naming convention B-2
Unique name B-2
Trunk cable 3-27

U

Uncertified 3-8
Unresponsive
IP 3-39, 3-43
SNMP agent 3-55
System 3-12
Unstable
Device connection 3-32
Example of diagnosis 4-4
Minimum traps used to diagnose 4-3
Network adapter 3-24
System 3-11

Trap window used to diagnose 4-3

V

VLAN 2-15, 3-47, 3-48
Connectivity exception 3-4, 3-49
Connectivity map 2-16
Membership map 2-16
Operational exception 3-4, 3-49

Z

Aggregate event
see Exception