VMware Smart Assurance IP Manager Reference Guide

VMware Smart Assurance 10.0.0

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2019 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

1 Preface 7
- Purpose 7
- Audience 7

2 VMware Smart Assurance IP Manager installation directory 8

3 VMware Smart Assurance IP Manager products 9

4 IP Manager documentation 10

5 Related documentation 11

6 Conventions used in this document 12
- Typographical conventions 12

7 Where to get help 13

8 Your comments 14

9 Network Objects 15
- Network containment 16
- Network Objects, Attributes, Exceptions, Faults, and Events 30
- System 32
- AggregatePort 39
- AggregateLink 44
- ESX Server Certification 45
- Cisco Nexus 1000v certification 45
- Cisco Unified Computing System Certification 46
- Host 60
- Switch 65
- Chassis 69
- Card 71
- Network adapter 74
- Wireless LAN 88
- Wirless LAN attributes in ICF Topology Manager 89
- WirelessAccessPoint 90
- WirelessClient 93
- SSID 95

WirelessController 96
AuthenticationServer 99
Root-cause analysis of a wireless LAN 100
Device connection 101
Service access point 107
Logical link 123
Partition 128
Management agent 129
Redundancy groups 133
Processor 139
Memory 140
Disk 142
File System 144
PowerSupply 145
VoltageSensor 147
TemperatureSensor 148
Fan 150
DuplicateIP 151
NAS IP Elements 155
NAS Chassis 156
Host (Celerra Control Station) 157
FileServer 158
FibreChannelSwitchPort 158
PortLink 159
Events for PortLink and FibreChannelSwitchPort 159
External Polling Support for FibreChannelSwitchPort 160
SM_ElementManager 160

10 Notifications for Network Objects 162
Introduction 162
Summary of root-cause problems, exceptions, and events 163
Problems, events and Notification summary for IP Availability Manager 171
Exception, Fault, Event, and Notification summary for IP Performance Manager 175

11 MIBs Polled and SNMP Traps Processed 178
Standard SNMP MIBs polled by IP Availability Manager 178
Standard SNMP MIBs polled by IP Performance Manager 179
Enterprise MIBs polled by IP Availability Manager 179
Enterprise MIBs polled by IP Performance Manager 182
SNMP traps processed 184

12 Network Topology Naming Conventions 188

DisplayName and Name attributes 188

Naming convention for network objects 189

13 Discovery 194

Discovery probes 194

Seed file format 195

Device entry field descriptions 199

Location, names, and content of discovery hook scripts 202

ECIM-R hierarchies 205

ECIM-R topology collection sets 213

ECIM-R relationships 215

14 Configuration Settings 218

Description of discovery.conf 218

Description of tpmgr-param.conf 227

Description of name-resolver.conf 247

Description of partition.conf 248

Description of tcat.conf 249

Description of oidInfo.conf 250

Description of user-defined-connections.conf 251

Controlling the analysis of wide area networks 252

Parameters for the SystemRestarted event 253

Parameters for the ConfigChange event 254

Interface-matching filters in the tpmgr-param.conf file 255

Optimizing the discovery of ERX devices 263

Problem Impact propagation policy over VLANs setting 265

Default device access setting 266

Default tagging filter groups and settings 267

Possible adapter startup errors 271

15 Polling and Threshold Settings 272

Default polling groups 272

Polling settings 274

Default threshold groups 282

Threshold settings 296

16 IPv6 Address Conventions 308

Overview 308

Conventions for specifying an IPv6 address with port number 309

Conventions for specifying an IPv6 address in a class instance name 310

17 Wildcard Patterns 312

Types of wildcard patterns 312

18 Audit Logging 314

Enhanced Domain Audit Logging Format 314

19 Commands 317

Issuing commands to modify configuration parameters 317

Preface

1

As part of an effort to improve its product lines, VMware periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your VMware technical support professional if a product does not function properly or does not function as described in this document.

Note This document was accurate at publication time. Go to VMware Online Support docs.vmware.com to ensure that you are using the latest version of this document.

This chapter includes the following topics:

- Purpose
- Audience

Purpose

This document provides detailed information on attributes, events, root cause problems, notifications for Network objects, Configuration settings, Discovery, Polling and Thresholds settings, Network topology naming conventions, Audit logging and Wild card patterns.

Audience

This document is intended for IT managers and system administrators.

VMware Smart Assurance IP Manager installation directory

2

In this document, the term BASEDIR represents the location where VMware Smart Assurance software is installed.

- For UNIX, this location is: /opt/InCharge/<productsuite>.

  On UNIX operating systems, IP Manager is, by default, installed to: /opt/InCharge/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.

  The VMware Smart Assurance System Administration Guide provides more information about the directory structure of VMware Smart Assurance software.

VMware Smart Assurance IP Manager products

3

The VMware Smart Assurance IP Manager includes the following products:

- VMware Smart Assurance IP Availability Manager
- VMware Smart Assurance IP Performance Manager
- VMware Smart Assurance IP Availability Manager Extension for NAS

IP Manager documentation

4

The following documents are relevant to users of the IP Manager product. Electronic versions of the updated manuals are available at VMware Smart Assurance Online Support: docs.vmware.com

- VMware Smart Assurance IP Manager Release Notes
- *VMware Smart Assurance Open Source License and Copyright Information*
- *VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers*
- *VMware Smart Assurance IP Manager Deployment Guide*
- *VMware Smart Assurance IP Manager Concepts Guide*
- *VMware Smart Assurance IP Manager User Guide*
- VMware Smart Assurance IP Manager Reference Guide
- VMware Smart Assurance Topology Split Manager User Guide
- VMware Smart Assurance IP Manager Troubleshooting Guide
- *VMware Important Notice*
- *VMware Smart Assurance IP Manager Certification Matrix*

Related documentation

5

The following VMware Smart Assurance publications provide additional information:

- *VMware Smart Assurance System Administration Guide*
- *VMware Smart Assurance Common Information Model (ICIM) 1.11 Reference for Non-Service Assurance Manager Products*
- *VMware Smart Assurance Common Information Model (ICIM) Reference for Service Assurance Manager*
- Smarts Foundation EMC Data Access API (EDAA) Programmer Guide
- *VMware Smart Assurance ASL Reference Guide*
- *VMware Smart Assurance Perl Reference Guide*
- *VMware Smart Assurance MODEL Reference Guide*
- *VMware Smart Assurance Dynamic Modeling Tutorial*

Conventions used in this document

6

VMware uses the following conventions for special notices:

Note NOTICE is used to address practices not related to personal injury.

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

An important notice contains information essential to software or hardware operation.

Typographical conventions

VMware uses the following type style conventions in this document:

Bold	Use for names of interface elements
Italic	Use for full titles of publications referenced in text
`Monospace`	Use for: ■ System output, such as an error message or script ■ System code ■ Pathnames, filenames, prompts, and syntax ■ Commands and options
`Monospace italic`	Use for variables.
`Monospace bold`	Use for user input.
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

7

Smart Assurance support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about VMware Smart Assurance products, go to VMware Online Support at:

support.vmware.com

Technical support

Go to VMware Online Support and click Service Center. You will see several options for contacting VMware Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your VMware sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

8

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Provide your feedback of this document to:docs.vmware.com

Network Objects

9

This chapter includes the following topics:

- Network containment
- Network Objects, Attributes, Exceptions, Faults, and Events
- System
- AggregatePort
- AggregateLink
- ESX Server Certification
- Cisco Nexus 1000v certification
- Cisco Unified Computing System Certification
- Host
- Switch
- Chassis
- Card
- Network adapter
- Wireless LAN
- Wirless LAN attributes in ICF Topology Manager
- WirelessAccessPoint
- WirelessClient
- SSID
- WirelessController
- AuthenticationServer
- Root-cause analysis of a wireless LAN
- Device connection
- Service access point

- Logical link
- Partition
- Management agent
- Redundancy groups
- Processor
- Memory
- Disk
- File System
- PowerSupply
- VoltageSensor
- TemperatureSensor
- Fan
- DuplicateIP
- NAS IP Elements
- NAS Chassis
- Host (Celerra Control Station)
- FileServer
- FibreChannelSwitchPort
- PortLink
- Events for PortLink and FibreChannelSwitchPort
- External Polling Support for FibreChannelSwitchPort
- SM_ElementManager

Network containment

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

Network containment tab pages

The network tab pages that appear in a Containment view for a network object with IPv4 addressing and IPv6 addressing contain the topology information listed in Network classes — Containment tab pages and associated attributes.

Table 9-1. Network classes — Containment tab pages and associated attributes

Class name	Network tab name	Attributes in tab page
WirelessController	Processors	DisplayName CurrentUtilization
	IP Networks	NetworkNumber Netmask
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	Memory	DisplayName Description TotalMemory FreeMemory BufferMissPct BufferUtilizationPct LargestFreeBuffer TotalBufferAllocationFailures
	WirelessAccessPoints	DisplayName IsUnresponsive Status IsRogue
	Network Adapters	DisplayName AdminStatus OperStatus Type Name Mode CurrentUtilization PeerSystemName
WirelessAccessPoint	IP Networks	NetworkNumber Netmask
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus

Table 9-1. Network classes — Containment tab pages and associated attributes (Continued)

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

Table 9-1. Network classes — Containment tab pages and associated attributes (Continued)

Class name	Network tab name	Attributes in tab page
	Memory (Available only if IP Server Performance Manager is in the deployment)	DisplayName Description TotalMemory FreeMemory BufferMissPct BufferUtilizationPct LargestFreeBuffer TotalBufferAllocationFailures
CallServer (continued)	NetworkAdapters	DisplayName AdminStatus OperStatus Type Mode CurrentUtilization PeerSystemName
	IP Address	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	Processors (Available only if IP Server Performance Manager is in the deployment)	DisplayName CurrentUtilization
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 MaxAvgDataRate MaxAvgQueueDepth
	OS	OSType OSVersion AvgIOWaitPct AvgRunnable TotalPhysicalMemory FreePhysicalMemory

Table 9-1. Network classes — Containment tab pages and associated attributes (Continued)

Class name	Network tab name	Attributes in tab page
Host (continued)	Memory (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName Description TotalMemory FreeMemory BufferMissPct BufferUtilizationPct LargestFreeBuffer TotalBufferAllocationFailures
	Network Adapters	DisplayName AdminStatus OperStatus Type 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
FileServer	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName

Table 9-1. Network classes — Containment tab pages and associated attributes (Continued)

Class name	Network tab name	Attributes in tab page
	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
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

Table 9-1. Network classes — Containment tab pages and associated attributes (Continued)

Class name	Network tab name	Attributes in tab page
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
MediaGateway	Processors (Available only if IP Performance Manager or IP Server Performance Manager is in deployment)	DisplayName CurrentUtilization
MediaGateway (continued)	Memory (Available only if IP Performance Manager or IP Server Performance Manager is in deployment)	DisplayName Description TotalMemory FreeMemory BufferMissPct BufferUtilizationPct LargestFreeBuffer TotalBufferAllocationFailures
	NetworkAdapters	DisplayName AdminStatus OperStatus Type Name Mode CurrentUtilization PeerSystemName
	Environment (Available only if IP Performance Manager or IP Server Performance Manager is in deployment)	DisplayName CreationClassName Status
	IP Address	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus

Table 9-1. Network classes — Containment tab pages and associated attributes (Continued)

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

Table 9-1. Network classes — Containment tab pages and associated attributes (Continued)

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

Table 9-1. Network classes — Containment tab pages and associated attributes (Continued)

Class name	Network tab name	Attributes in tab page
	IPv6 Networks	NetworkNumber PrefixLength
Firewall	Processors (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName CurrentUtilization
	Network Adapters	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	IP Addresses	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
Multilayer Switch Feature Card (MSFC) Router Switch Feature Card (RSFC) Router Switch Module (RSM)	Network Adapter	DisplayName AdminStatus OperStatus Mode CurrentUtilization PeerSystemName
	Processors	DisplayName CurrentUtilization
	IP Address	Address Netmask IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus
	Memory	DisplayName Description TotalMemory FreeMemory BufferMissPct BufferUtilizationPct LargestFreeBuffer TotalBufferAllocationFailures

Table 9-1. Network classes — Containment tab pages and associated attributes (Continued)

Class name	Network tab name	Attributes in tab page
	Cards	DisplayName Description Status
Switch	Processors (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName CurrentUtilization
	Memory (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	DisplayName Description TotalMemory FreeMemory BufferMissPct BufferUtilizationPct LargestFreeBuffer TotalBufferAllocationFailures
	Network Adapters	DisplayName AdminStatus OperStatus Type Name 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
TerminalServer	File Systems (Available only if IP Server Performance Manager is in the deployment)	Root StorageSize AvailableSpace UtilizationPct
TerminalServer (continued)	Disks (Available only if IP Server Performance Manager is in the deployment)	DisplayName AvgDataRate AvgQueueDepth

Table 9-1. Network classes — Containment tab pages and associated attributes (Continued)

Class name	Network tab name	Attributes in tab page
	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 9-1. Network classes — 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 Type Name Mode CurrentUtilization PeerSystemName
IP	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
IPv6	IPv6 Addresses	Address PrefixLength IPStatus InterfaceName InterfaceAdminStatus InterfaceOperStatus

Table 9-1. Network classes — Containment tab pages and associated attributes (Continued)

Class name	Network tab name	Attributes in tab page
	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
IPv6Network	Connected Systems	DisplayName Vendor Model Description IsUnresponsive Location PrimaryOwnerName PrimaryOwnerContact
VLAN	Connected Systems	DisplayName Vendor Model Description IsUnresponsive Location PrimaryOwnerName PrimaryOwnerContact

Table 9-1. Network classes — Containment tab pages and associated attributes (Continued)

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

Network Objects, Attributes, Exceptions, Faults, and Events

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

- Systems

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

- Physical packages

  Represent physical objects that contain or host other components. 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, VRRPEndpoint, EVCEndPoints and MAC.

  Note Service access points are often described as protocol endpoints.

- Logical links

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

- Logical devices

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

  - Processor
  - Memory
  - Disk
  - FileSystem

- PowerSupply
- VoltageSensor
- TemperatureSensor
- Fan

  IP Performance Manager also instantiates device connection, collection, management agent, and redundancy group object types, but because IP Performance Manager does no analysis for these object types, they are not discussed here. Appendix A, "ECIM Instrumentation Class," in the VMware Smart Assurance IP Management Suite Discovery Guide describes all of the object types instantiated by IP Performance Manager.

  The VMware Smart Assurance IP Management Suite Discovery Guide describes all of the object types that are instantiated by IP Availability Manager.

  All of the object types instantiated by IP Availability Manager and IP Performance Manager are available to a Global Console attached to IP Availability Manager and IP Performance Manager, and a subset are available to a Global Console attached to the Global Manager. “Network topology” on page 32 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.
- CallServer — A call server is a computer-based device dedicated to delivering call management and hosting a call manager network service. A host is represented as CallServer by IP Availability Manager and IP Performance Manager if it has VoIP-related data. This allows VoIP domain managers to fetch the topology from IP server for VoIP-specific discovery and root cause analysis.
- 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.

  A blade server is represented as a host. The individual blades are represented as hosts and switches under the ComposedOf relationship.
- Hub — A system that connects multiple physical segments. Active hubs are multiport repeaters, which means that they repeat signals received on any port to all the other ports.
- Hybrid Device — A hybrid device is a device that can be configured as a router, switch, or both. In IP Availability Manager a hybrid device is identified by the relationships between the device and its sub-modules, such as firewalls, wireless controllers, and loadbalancers. One example of a hybrid device supported by IP Availability Manager is the Cisco Catalyst 6509 and 2811 switch.
- LoadBalancer — A system that distributes client traffic across multiple web servers.

- MediaGateway — A Media gateway is a translation device or service that converts digital media streams between disparate telecommunications networks. A switch is represented as MediaGateway by IP Availability Manager and IP Performance Manager if it has VoIP related data. This allows VoIP domain managers to fetch the topology from IP server for VoIP specific discovery and root cause analysis.
- Multilayer Switch Feature Card (MSFC) — A card in a switch that performs routing between VLANs.
- Node — A system that is monitored by 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 towards 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 VMware, Inc..

Attributes for System

Attributes for System lists some key attributes for system.

Table 9-2. 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 by 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, FALSE
IsDiscoveryInProgress	TRUE if discovery is in progress for this system.	Boolean: TRUE, FALSE
IsSeed	TRUE if this system is added as a seed system.	Boolean: TRUE, FALSE
IsUnresponsive	TRUE if this system is not responding to ICMP and ICMPv6 pings or SNMP polls. (FALSE if this system is responding to ICMP pings and/or SNMP polls.)	Boolean: TRUE, 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 9-2. Attributes for System (Continued)

Attribute	Description	Allowed values
NumberOfIPs	Number of IP endpoints (IP addresses) discovered for this system; for example: 13	Integer
NumberOfIPv6s	Number of IPv6 endpoints (IPv6 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 through SNMP.	Boolean: TRUE, 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 ■ MEDIAGATEWAY
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. It depends 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.
- DetectedProblemSymptomImported 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. The VMware Smart Assurance IP Management Suite Configuration Guide provides information about these parameters.

“Diagnosis of Unstable Objects” on page 129 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 by IP Availability Manager

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

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 BackupActivated
- Network adapter ExceededMaximumUptime

Exceptions for System by IP Performance Manager

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

System PerformanceException

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

Network adapter faults that result in a system PerformanceException are described in Network adapter.

System ErrorException

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

The network adapter fault (HighErrorRate) that results in a system ErrorException is described in Network adapter.

System ResourceException

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

Processor, memory, and file system faults that result in a system ResourceException are described in Processor, Memory, and File System.

System OperationalException

A system OperationalException indicates that a system or a system component such as, Card, Disk, File System or NetworkAdapter is experiencing operational failures.

Disk faults that result in a system OperationalException are described in Disk.

System PowerSupplyException

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

Power supply and voltage faults that result in a system PowerSupplyException are described in *PowerSupply* and *VoltageSensor*.

System TemperatureException

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

Temperature and fan faults that result in a system TemperatureException are described in *TemperatureSensor* and *Fan*.

Events for System

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

Table 9-3. 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. (For internal codebook correlation use only.)
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.
DiscoveryInProgress	Indicates that discovering the system is in progress.

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. The VMware Smart Assurance 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 VMware Smart Assurance volume licenses. The VMware Smart Assurance IP Management Suite Discovery Guide provides information about the effects of this event.

AggregatePort

The AggregatePort class represents the logical grouping of ports in the IP Availability Manager.

An AggregatePort is defined by the following relationships:

Relationships

- *AggregatePort Bridges/BridgedVia* relationship with MAC
- *ComposedOf/PartOf* relationship with adapter
- *ConnectedVia/ConnectedSystems* relationship with AggregateLink
- *NeighboringSystems* relationship with Switch
- *PartOf/MemberOf* relationship with Switch and VLAN
- *Peer* relationship with AggregatePort
- *VirtualBridges/VirtualBridgedVia* relationship with MAC

Events and attributes of AggregatePort

Events for the class AggregatePort lists the events generated for the class AggregatePort.

Table 9-4. Events for the class AggregatePort

Events	Description
Disabled	Indicates that a disabled AggregatePort is the root cause.
Down	Indicates that a failure on an AggregatePort is the root cause
LogicalConnectionDown	Indicates a fault within the wide area network
Unstable	Indicates that an AggregatePort is not stable.
ReducedRedundancy	Indicates that at least one component is not functioning but the total number of functioning components is above the AtRiskThreshold.
UnbalancedAdapterUtilization	Indicates that the difference between the mean utilization of the group and utilization of one or more members of the group is above the UtilizationDiscrepancyThreshold. This event is generated when Port 1 deviation or Port 2 deviation > UtilizationDiscrepancyThreshold, where: ■ Port 1 deviation = Absolute (Port 1 Utilization - mean) ■ Port 2 deviation = Absolute (Port 2 Utilization - mean) ■ Mean = (Port 1 utilization + Port 2 utilization)/2

Events of vAggregate Port

Events for vAggregatePort lists the events that are generated for vAggregatePort.

Table 9-5. Events for vAggregatePort

Events	Description
ReducedPeerLink	Indicates that at least one of the constituent adapter of Aggregated Peer Link adapter is operationally down.
ReducedRedundancy	Indicates at least one component is not functioning but the total number of functioning components is above AtRiskThreshold.

Table 9-5. Events for vAggregatePort (Continued)

Events	Description
Impaired	Indicates that all the network adapters related to peer link is down.
AllComponentsDown	Indicates that all the components in the vAggregate port group are down.

Attributes of the class AggregatePort/vAggregatePort lists the attributes of the class AggregatePort/vAggregatePort.

Table 9-6. Attributes of the class AggregatePort/vAggregatePort

Attribute	Allowed values	Description
DesignatedBridge	string	The unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached.
DesignatedPort	unsigned-int	The Port Identifier of the port on the Designated Bridge for this port's segment.
DuplexMode	Enum	Indicates whether the adapter is full-duplex or half-duplex. FULLDUPLEX - indicates the adapter is full-duplex. HALFDUPLEX - indicates the adapter is half-duplex. If the value is UNSPECIFIED then the duplex mode is not available.
DuplexSource	Enum	ASSUMED - Indicates the source for setting the adapter to be full-duplex or half-duplex. A value of ENTERPRISE_MIB indicates the duplex is set by enterprise specific MIB. A value of ETHERLIKE_MIB indicates the duplex is set by the value of dot3StatsDuplexStatus in ETHERLIKE MIB. A value of NEIGHBOR_MIB indicates the duplex is set by neighbor MIB like Cisco CDP MIB. A value of USER_CHANGED indicates the duplex is set by the user. A value of ASSUMED indicates the duplex is set based upon the type of interface. A value of NONE indicates the duplex is not set by any sources. The OTHER_SOURCE value is a placeholder for future use.
InterfaceAlias	String	An alias name for the network adapter as specified by a network manager.
InterfaceCode	Enum	Represents the interface types or protocols or encapsulations.
InterfaceNumber	Integer	The InterfaceNumber is an integer value that uniquely identifies this adapter within the scope of the containing System.
IsConnectedToManagedSystem	Boolean; TRUE, FALSE	TRUE if the device connected to this Port is in the topology and is managed.

Table 9-6. Attributes of the class AggregatePort/vAggregatePort (Continued)

Attribute	Allowed values	Description
IsConnectedToSystem	Boolean; TRUE, FALSE	TRUE if the device connected to this Port is in the topology.
IsConnector	Boolean; TRUE, FALSE	TRUE if this Network Adapter is part of the networking infrastructure, for example, a router or trunk port as opposed to a user access port.
IsFlapping	Boolean; TRUE, FALSE	TRUE - Indicates that the port or interface is flapping. FALSE - Indicates that the port or interface is not flapping.
IsLogicalConnectionDownEnabled	Boolean; TRUE, FALSE	TRUE - if the LogicalConnectionDown problem is enabled.
MaximumUptime	Integer	The maximum length of time, in seconds, that an ONDEMAND or BACKUP NetworkAdapter may be in the UP state before the event ExceededMaximumUptime is notified. If this attribute is set to 0, the event is disabled.
ManagedState	Enum	MANAGED - Used to keep track of the management status of this logical device. Allows the software to restore the device's implicit management status if it is explicitly unmanaged and when remanaged.
MaxSpeed	Integer	The maximum speed, in Bits per Second, for the NetworkAdapter.
MaxTransferUnit	Integer	The size of the largest datagram which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.
Mib2IfType	Integer	A numerical representation of the interface type.
Mode	Enum	Indicates the intended purpose of this adapter: ■ Backup ■ Dial-on-demand ■ Normal The diagnostics applied to a particular adapter will vary based on its mode. For instance, an alert should not be generated when a backup or dial-on-demand adapter is down.
MonitoringEnabled	Boolean; TRUE, FALSE	Indicates whether monitoring is enabled or not.
PortKey	String	A unique value that identifies this Port from other Ports within the scope of the containing System. The PortKey is typically used to identify the Port to the Instrumentation. Depending on the vendor implementation, the PortKey may or may not be equivalent to the PortNumber, which may or may not be equivalent to the InterfaceKey.
PortNumber	Integer	A value that uniquely identifies this Port within the scope of the containing System.

Table 9-6. Attributes of the class AggregatePort/vAggregatePort (Continued)

Attribute	Allowed values	Description
PortType	Enum	The type of Port represented by this object. Valid values: TRUNK ACCESS (default)
SuppressTestingNotifications	Boolean TRUE, FALSE	If TRUE then do not generate a problem alert when the adapter is in testing mode.

Root-cause analysis of vAggregate Port

Root-cause analysis of vAggregatePort lists the root-cause analysis for AggregatePort and the impacted class.

Table 9-7. Root-cause analysis of vAggregatePort

Root-cause	Impacted class	Events on the impacted class	Comments
TrunkCable:Down	vAggregatePort	ReducedPeerLink	This event is generated for vPC peer port failures. **Note** It is not applicable for member ports.
		Impaired	This event is generated for vPC peer port failures. **Note** It is not applicable for member ports.
		ReducedRedundancy/AtRisk	The generation of the vAggregatePort event depends on the value of AtRiskThreshold.
		AllComponentsDown	There can be multiple TrunkCable:Down problems that explain the AllComponentsDown event for vAggregatePort.
Port:Disabled	vAggregatePort	Impaired	This event is generated for vPC peer port failures. **Note** It is not applicable for member ports.
		ReducedRedundancy/AtRisk	The generation of the vAggregatePort event depends on the value of AtRiskThreshold.
Switch:Down	vAggregatePort	Impaired	This event is generated for vPC peer port failures. **Note** It is not applicable for member ports.
		AllComponentsDown	There can be multiple TrunkCable:Down problems that explain the AllComponentsDown event for vAggregatePort.
AggregatePort:Down	vAggregatePort	AllComponentsDown	There can be multiple TrunkCable:Down problems that explain the AllComponentsDown event for vAggregatePort.

AggregateLink

AggregateLink represents the logical link between the AggregatePorts, configured to combine multiple network connections in parallel to increase throughput beyond what a single connection could sustain.

Relationships

The class *AggregateLink* is defined by the following relationships:

- *A_End* relationship with AggregatePort
- *ComposedOf/PartOf* relationship with TrunkCable
- *ConnectedSystems/NeighboringSystems* relationship with Switch/Router
- *ConnectedTo/ConnectedVia* relationship with AggregatePort
- *Z_End* relationship with AggregatePort

Events and attributes of AggregateLink

Events generated for AggregateLink lists the events that are generated for AggregateLink.

Table 9-8. Events generated for AggregateLink

Events	Description
Down	Indicates that the physical connection between two network adapters is down.
DownOrFlapping	Indicates that one or both of the network adapters on either end of the network connection have a value of UP for AdminStatus attribute and a value of DOWN for OperStatus or a value of TRUE for the IsFlapping attribute.
Unstable	Indicates that the physical connection between two network adapters is unstable.

Attributes of AggregateLink lists the attributes of AggregateLink.

Table 9-9. Attributes of AggregateLink

Attribute	Allowed values	Description
VMwareCollectionEnabled	Boolean: TRUE, FALSE	An attribute to enable or disable the discovery of the entity addressed by this ConnectivityCollection.
IsLogicalConnectionDownEnabled	Boolean: TRUE, FALSE	TRUE - If the LogicalConnectionDown problem is enabled.
IsNetworkAdapterDownOrFlapping	Boolean: TRUE, FALSE	TRUE - Indicates that at least one connected port or interface is operationally down or flapping. FALSE - Indicates that no connected port or interface is operationally down or flapping.

Table 9-9. Attributes of AggregateLink (Continued)

Attribute	Allowed values	Description
IsNetworkAdapterFlapping	Boolean: TRUE, FALSE	TRUE - Indicates that at least one connected port or interface is flapping. FALSE - Indicates that no connected port or interface is flapping.
IsNetworkConnectionNotOperating	Boolean: TRUE, FALSE	TRUE - Indicates that the network connection is not operating FALSE - Indicates that the network connection is working.
DuplexMode	Enum	Indicates whether the adapter is full-duplex or half-duplex. A value of FULLDUPLEX indicates that the adapter is full-duplex. A value of HALFDUPLEX indicates that the adapter is half-duplex. If the value is UNSPECIFIED, then the duplex mode is not available.

ESX Server Certification

The VMware ESX server has been certified as a host.

Attributes for ESX Host

The attributes listed in Attributes of ESX Host distinguishes an ESX host from a normal host.

Table 9-10. Attributes of ESX Host

Attribute	Descripton	Type	Values
Vendor	The name of the system's supplier	String	VMWARE
Model	The name by which the system is generally known.	String	ESX

Root cause, Exceptions, and Events

All Root-cause problems for System are applicable for ESX Server.

All Exceptions for System by IP Availability Manager and Exceptions for System by IP Performance Manager are applicable for ESX Server.

All events listed in Root cause, Exceptions, and Events are applicable for ESX Server.

Cisco Nexus 1000v certification

The Cisco Nexus 1000V switch, with system ObjectID .1.3.6.1.4.1.9.12.3.1.3.840, has been recertified as vSwitch.

Attributes for Cisco Nexus 1000v

Attributes of vSwitch lists the new attribute for the class vSwitch.

Table 9-11. Attributes of vSwitch

Attribute	Description	Allowed Values
Type	The Type attribute coarsely classifies the ComputerSystem. This attribute is used primarily for display purposes only. The actual capabilities of a ComputerSystem are reflected in the LogicalDevices, Services, and ServiceAccessPoints related to it.	Enum: VIRTUALSWITCH

Events and Exceptions

All Exceptions for System by IP Availability Manager and Exceptions for System by IP Performance Manager are applicable for Cisco Nexus 1000V switch.

All events listed in Events and Exceptions are applicable for Cisco Nexus 1000v.

Cisco Unified Computing System Certification

The Cisco Unified Computing System (Cisco UCS) is a next-generation data center platform that unites compute, network, storage access, and virtualization into a cohesive system designed to reduce total cost of ownership (TCO) and increase business agility.

Attributes and MIB Object IDs lists the attributes and the MIB ObjectIDs of the Cisco UCS entity (ComputeFabric) and the Cisco UCS chassis (BladeEnclosureManager).

Table 9-12. Attributes and MIB Object IDs

Managed Object	Attribute	Attribute type	MIB ObjectID
ComputeFabric	CIM_Name, DisplayName	Octet string	cucsTopSystemName 1.3.6.1.4.1.9.9.719.1.49.3.1.7
	SystemName	Octet string	cucsTopSystemAddress 1.3.6.1.4.1.9.9.719.1.49.3.1.4
	SystemMode	Octet string	cucsTopSystemMode 1.3.6.1.4.1.9.9.719.1.49.3.1.6
BladeEnclosureManager	indexVal	Gauge	cucsEquipmentChassisId 1.3.6.1.4.1.9.9.719.1.15.7.1.20
	CIM_Name	Octet string	cucsEquipmentChassisDn 1.3.6.1.4.1.9.9.719.1.15.7.1.2
	AdminState	Integer	cucsEquipmentChassisAdminState 1.3.6.1.4.1.9.9.719.1.15.7.1.4
	SerialNumber	Octet string	cucsEquipmentChassisSerial 1.3.6.1.4.1.9.9.719.1.15.7.1.32
	DisplayName	Octet string	cucsEquipmentChassisUsrLbl 1.3.6.1.4.1.9.9.719.1.15.7.1.34

Table 9-12. Attributes and MIB Object IDs (Continued)

Managed Object	Attribute	Attribute type	MIB ObjectID
	Vendor	String	cucsEquipmentChassisVendor 1.3.6.1.4.1.9.9.719.1.15.7.1.35
	Model	String	cucsEquipmentChassisModel 1.3.6.1.4.1.9.9.719.1.15.7.1.25

Attributes and events

This section describes the attributes and events generated for ComputeFabric and BladeEnclosureManager.

Attributes of ComputeFabric

Attributes of ComputeFabric lists the attributes of ComputeFabric.

Table 9-13. Attributes of ComputeFabric

Attribute	Description	Allowed values
BackplaneUtilization	Percentage of bandwidth utilization for the chassis backplane as reported by the instrumentation.	Numeric (float)
DisplayName	Name, as shown in the Global Console, of this chassis.	String
IsAnySystemResponsive	TRUE if any system packaged by this chassis is responding to ICMP and ICMPv6 pings or SNMP polls or both.	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, Blade-Enclosure-<*name of the blade enclosure instance*>	String
SerialNumber	Indicates the version of this chassis.	String

Table 9-13. Attributes of ComputeFabric (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
Mode	Defines the ComputeFabric configuration mode, whether the ComputeFabric will operate as a standalone element or as a part of a cluster.	String
ManagementAddress	The Management IP address of the ComputeFabric Equipment.	String
IsManaged	The IsManaged attribute determines if an ICIM_ManagedSystemElement should be monitored by the management system. An unmanaged object will never have associated instrumentation. This attribute is read-only.	Boolean: TRUE or FALSE
KEYS	Types and Names of key attributes defined in CIM model.	String
MonitoringEnabled	Indicates if monitoring is enabled for the ComputeFabric.	Boolean: TRUE or FALSE
CreationClassName	The creation class name attribute defined in CIM model.	String
ServiceName	Name of external server used for imported events and instrumented attributes.	String

Table 9-13. Attributes of ComputeFabric (Continued)

Attribute	Description	Allowed values
Status	Reflects the current state of the package as reported by the instrumentation. ■ OK indicates that the package is operating normally. ■ CRITICAL indicates that the package is at critical status. ■ MARGINAL indicates that the package is at marginal status. ■ OTHER indicates that the status of the package is other than the above or unrecognized SNMP error. ■ NOTPRESENT indicates the package MIB value missing. ■ UNKNOWN indicates the default value before SNMP polling.	Enum
Tag	Uniquely identifies the physical element and serves as the element's key. The Tag property can contain information such as an asset tag or serial number. The key for ICIM_PhysicalElement is placed very high in the object hierarchy in order to independently identify the hardware/entity, regardless of physical placement in or on cabinets, adapters. For example, a hot-swappable or removable component may be taken from its containing (scoping) package and be temporarily unused. The object still continues to exist and may even be inserted into a different scoping container. Therefore, the key for physical element is an arbitrary string and is defined independently of any placement or location-oriented hierarchy.	String
Type	Functional type of this physical package.	String

Events for ComputeFabric

Events generated for ComputeFabric lists the events generated for ComputeFabric

Table 9-14. Events generated for ComputeFabric

Events	Description
BackplaneUtilizationException	Indicates that the data being transmitted over the chassis's backplane has exceeded BackplaneUtilizationThreshold.
Down	Indicates that a faulty chassis is the root cause.

Attributes of BladeEnclosureManager

Attributes of BladeEnclosureManager lists the attributes of BladeEnclosureManager.

Table 9-15. Attributes of BladeEnclosureManager

Attributes	Description	Allowed values
AccessMode	The mode to access a system. It can have one of the following values: ■ ICMPONLY ■ SNMPONLY ■ ICMPSNMP	enum
AprioriProbability_Down		Float
BridgeAddress	The bridge address as defined in RFC1493.	String
Certification	Defines the level of certification that this device has in the discovery process: ■ UNSUPPORTED — Deprecated. ■ GENERIC — Indicates that the System Object ID for the device is not recognized and the device will be classified as GENERIC and added to the Node class. Standard ■ MIB-II data is used to perform analysis on the device. ■ TEMPLATE — Indicates that this system is recognized, but no information about the MIBs that this system supports is known. ■ CERTIFIED — Indicates that the device has the highest level of certification and is discovered using enterprise MIBs as well as standard MIB-II data. ■ VALIDATED — Deprecated. ■ UNDISCOVERED — Indicates the system is undiscovered.	enum
DiscoveredFirstAt	The time when the first discovery probe of this system occurred.	String
DiscoveredLastAt	The time when the last discovery probe of this system occurred.	String
DiscoveredLastAtToSeconds	The numeric time when the last discovery probe of this System occurred.	Integer
DiscoveryErrorInfo	A message that describes the last discovery error for this system.	String
Domain	The domain to which the system belongs.	String
HasIPAddresses	Indicates if the BladeEnclosureManager has an IP address.	Boolean: TRUE, FALSE
HasIPv6Addresses	Indicates if the BladeEnclosureManager has an IPv6 address.	Boolean: TRUE, FALSE
indexVal		String
IsAddressable	Set to TRUE if the system is IP addressable.	Boolean: TRUE, FALSE
IsDiscoveryInProgress	TRUE if discovery in progress for this system.	Boolean: TRUE, FALSE
IsEveryIPUnresponsive		Boolean: TRUE, FALSE
IsEveryIPv6Unresponsive		Boolean: TRUE, FALSE

Table 9-15. Attributes of BladeEnclosureManager (Continued)

Attributes	Description	Allowed values
IsEveryNeighborUnresponsive		Boolean: TRUE, FALSE
IsEveryServiceUnresponsive		Boolean: TRUE, FALSE
IsManaged	Determines if an ICIM_ManagedSystemElement should be monitored by the management system. An unmanaged object will never have associated instrumentation. This attribute is read-only.	Boolean: TRUE, FALSE
IsMightBeDown		Boolean: TRUE, FALSE
IsProxy	TRUE - if this is a proxy of remote system.	Boolean: TRUE, FALSE
IsSeed	TRUE if the system is added as seed.	Boolean: TRUE, FALSE
IsUnmanagedOrUnresponsive		Boolean: TRUE, FALSE
IsUnmanagedOrUnresponsive_internal	■ TRUE - Indicates that the system is not responding to ICMP pings or SNMP polls. ■ FALSE - Indicates that the system is responding to ICMP pings and/or SNMP polls.	Boolean: TRUE, FALSE
IsUnresponsive	■ TRUE - Indicates that the system is not responding to ICMP pings or SNMP polls. ■ FALSE - Indicates that the system is responding to ICMP pings and/or SNMP polls.	Boolean: TRUE, FALSE
KEYS	Types and Names of key attributes defined in CIM model.	String
Location	A description of where this System is located.	String
Model	The name by which the System is generally known.	String
MonitoringEnabled	Indicates of monitoring is enabled for the system.	Boolean: TRUE, FALSE
Vendor	The name of the System's supplier.	String
Name	Name of the object. For example, Blade-Enclosure-Manager-1	String
ManagedByAgentIP	The IP address of the SNMP Agent by which the BladeEnclosureManager is being Managed.	String

Events for BladeEnclosureManager

Events generated for BladeEnclosureManager lists the events that are generated for BladeEnclosureManager.

Table 9-16. Events generated for BladeEnclosureManager

Events	Description
ConnectivityException	Indicates that one or more connectivity-related root-cause failures for a particular system or one of its components.
DiscoveryError	Indicates that an error occurred while discovering the system. DiscoveryError is notified under the following circumstances: - SNMP requests times out - SNMP agent encounters a loop - system is unreachable (Down) - Qualified access address not found.
DiscoveryInProgress	Indicates that discovering the system is in progress.
Down	Indicates that the root cause is a failed system.
ErrorException	Indicates that one or more error-related failures exist for the network adapters of a particular system.
MightBeDown	Indicates that the system is not responding to SNMP polls or ICMP pings and is logically near the root-cause problem.
OperationalException	Indicates that one or more operational-related failures exist for a particular system or one of its components.
PerformanceException	Indicates that one or more performance-related failures exist for the network adapters of a particular system.
PowerSupplyException	Indicates that one or more voltage or power supply faults exist for a particular system.
ResourceException	Indicates that one or more processor or memory related faults exist for a particular system.
TemperatureException	Indicates that one or more fan or temperature related faults exist for a particular system.
Unresponsive	Indicates that all of the system's IPv4 and IPv6 addresses not responding and the SNMPAgent is not responding as well.
Unstable	Indicates that the system is continuously restarting itself.

Discovery and monitoring

This section lists the attributes and the MIB Object IDs using which the Cisco UCS components are discovered and monitored.

- Discovery of Cards (Fabric Extender) on the BladeEnclosureManager
- Discovery of Fabric Ports on Cards (Fabric Extender) of the BladeEnclosureManager (Chassis)
- Discovery of Cards on the Fabric Interconnect switch
- Discovery of Ethernet Ports on Cards of the Fabric Interconnect
- Discovery of Trunk Cable Connection between the Fabric Interconnect Switch and the Fabric Extender
- Discovery of Host hosted by BladeServer

Discovery of Cards (Fabric Extender) on the BladeEnclosureManager

The Fabric Extenders that are present on each BladeEnclosureManager are represented as Cards in the IP topology. The existing Card model is being used to represent the Fabric Extenders.

Attribute of cards (Fabric Extender) lists the attributes of card (Fabric Extender).

Table 9-17. Attribute of cards (Fabric Extender)

Attribute	Type	MIB ObjectID	Description
	Integer	cucsEquipmentIOCardPresence 1.3.6.1.4.1.9.9.719.1.15.30.1.31	If the value of the OID is equipped (10) then IP creates the cards.
Name	Octet String	cucsEquipmentIOCardDn 1.3.6.1.4.1.9.9.719.1.15.30.1.2	Card name
Serial Number	Octet String	cucsEquipmentIOCardSerial 1.3.6.1.4.1.9.9.719.1.15.30.1.33	Serial number of the card
Location	Octet String	cucsEquipmentIOCardSide 1.3.6.1.4.1.9.9.719.1.15.30.1.34	Location of the card.
Status (Monitoring)	Integer	cucsEquipmentIOCardOperState 1.3.6.1.4.1.9.9.719.1.15.30.1.25	Provides the overall operation state of the Fabric Extender.

Discovery of Fabric Ports on Cards (Fabric Extender) of the BladeEnclosureManager (Chassis)

Attributes and MIB Object IDs of Fabric port lists the attributes and MIB Object IDs of Fabric port using which you can discover and monitor a Fabric port present on Cards (Fabric Extender).

Table 9-18. Attributes and MIB Object IDs of Fabric port

Attribute	Type	MIB ObjectID	Description
CIM Name	String	cucsEtherSwitchIntFIoDn 1.3.6.1.4.1.9.9.719.1.16.13.1.2	Provides the description of the port.
Admin status	Integer	cucsEtherSwitchIntFIoAdminState 1.3.6.1.4.1.9.9.719.1.16.13.1.5	Provides the admin state of the port.
OperStatus	Integer	cucsEtherSwitchIntFIoOperState 1.3.6.1.4.1.9.9.719.1.16.13.1.17	Provides the operational state of the port.

Discovery of Cards on the Fabric Interconnect switch

Attributes and MIB Object IDs of cards lists the attributes and MIB Object IDs using which you can discover the cards present on the Fabric Interconnect which is a part of the Cisco UCS Manager.

Table 9-19. Attributes and MIB Object IDs of cards

Attribute	Type	MIB Object IDs	Description
	Integer	cucsEquipmentSwitchCardState 1.3.6.1.4.1.9.9.719.1.15.70.1.16	If the value of the OID is online (4) then IP creates the cards.
Name	Octet string	cucsEquipmentSwitchCardDn 1.3.6.1.4.1.9.9.719.1.15.70.1.2	Card name
Description	Octet string	cucsEquipmentSwitchCardDescr 1.3.6.1.4.1.9.9.719.1.15.70.1.4	Description of the card which specifies whether it is a Supervisor Module or the FC Module.
Serial Number	Octet string	cucsEquipmentSwitchCardSerial 1.3.6.1.4.1.9.9.719.1.15.70.1.15	Serial number of the card.
Status (Monitoring)	Integer	cucsEquipmentSwitchCardOperState 1.3.6.1.4.1.9.9.719.1.15.70.1.9	It provides the overall operation state of the Card

Discovery of Ethernet Ports on Cards of the Fabric Interconnect

MIB Object IDs of Fabric port on cards lists the Object IDs using which you can discover the Ethernet Ports on cards present in the Fabric Interconnect.

Table 9-20. MIB Object IDs of Fabric port on cards

Attribute	Type	MIB OID	Description
CIM Name	Octet string	cucsEtherPIoDn 1.3.6.1.4.1.9.9.719.1.16.6.1.2	Port description
Underlying MAC	Octet string	cucsEtherPIoMac 1.3.6.1.4.1.9.9.719.1.16.6.1.12	MAC address associated with the port
Admin Status	Integer	cucsEtherPIoAdminState 1.3.6.1.4.1.9.9.719.1.16.6.1.4	Admin status of the port.
Type	Integer	cucsEtherPIoMode 1.3.6.1.4.1.9.9.719.1.16.6.1.13	Mode of the port
AdminStatus (monitoring)	Integer	cucsEtherPIoAdminState 1.3.6.1.4.1.9.9.719.1.16.6.1.4	Provides the administrative state of the Port.
OperStatus (monitoring)	Integer	cucsEtherPIoOperState 1.3.6.1.4.1.9.9.719.1.16.6.1.17	Provides the operational state of the Port.

Discovery of Trunk Cable Connection between the Fabric Interconnect Switch and the Fabric Extender

MIB Object IDs of Ethernet Ports lists the MIB Object IDs using which you can discover the connections present between the Fabric Interconnect Switch and the Fabric Extenders (BladeEnclosureManager).

Table 9-21. MIB Object IDs of Ethernet Ports

MIB Object IDs	Type	Description
cucsEtherPIoDn 1.3.6.1.4.1.9.9.719.1.16.6.1.2	Integer	Ethernet port name
cucsEtherPIoPeerDn 1.3.6.1.4.1.9.9.719.1.16.6.1.18	Octet string	Peer Port Name
cucsEtherSwitchIntFIoDn 1.3.6.1.4.1.9.9.719.1.16.13.1.2	Octet string	Fabric Ports Name

Discovery of Host hosted by BladeServer

MIB Object IDs of Host (Blade Server) on the BladeEnclosureManager lists the MIB Object IDs using which you can discover the connections present between the Fabric Interconnect Switch and the hosts in a Blade Server.

Table 9-22. MIB Object IDs of Host (Blade Server) on the BladeEnclosureManager

MIB Object IDs	Description
cucsVnicEtherAddr 1.3.6.1.4.1.9.9.719.1.53.9.1.5	Virtual NIC Ethernet Address
cucsVnicEtherEquipmentDn 1.3.6.1.4.1.9.9.719.1.53.9.1.9	Name of the Equipment

To discover the host in the Blade Server present in the Cisco UCS chassis, IP stores all the MAC addresses relevant to Blade Servers in the memory. When you discover the host independently and the MAC address that belongs to the list of MAC addresses found from the Cisco UCS, then IP creates the *ComposedOf* relationship between the host and the chassis. The creation of this relationship takes place during post-processing.

Note The Object IDs are the Ethernet Address (MAC) of the each entities (BladeServers) present on the Cisco UCS Chassis.

Faults and Exceptions

Faults and exceptions generated for BladeEnclosureManager lists the components of a Blade Enclosure Manager that is monitored by IP Performance Manager.

Table 9-23. Faults and exceptions generated for BladeEnclosureManager

Managed Object	Exception	Component	Fault	Threshold
BladeEnclosureManager	PowerSupply	PowerSupply	StateNotNormal	None
		VoltageSensor	OutOfRange	RelativeVoltageThreshold (Environment)

Table 9-23. Faults and exceptions generated for BladeEnclosureManager (Continued)

Managed Object	Exception	Component	Fault	Threshold
	Temperature	TemperatureSensor	OutOfRange	RelativeTemperatureThreshold (Environment)
		Fan	StateNotNormal	None

Faults for PowerSupply

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

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

- OK
- CRITICAL
- OTHER
- UNKNOWN

Faults for Fan

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

A Fan *StateNotNormal* fault indicates that the state of fan is in CRITICAL state. The Fan state can be one of four states:

- OK
- CRITICAL
- OTHER
- UNKNOWN

Faults for TemperatureSensor

Faults and related thresholds for TemperatureSensor lists the faults detected for TemperatureSensor.

Table 9-24. Faults and related thresholds for TemperatureSensor

Temperature Fault	Description	Threshold
OutOfRange	Indicates that the temperature for this system is outside the normal operating range and exceeds the RelativeTemperatureThreshold.	RelativeTemperatureThreshold

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

Note When the *HighThreshold* value exceeds the set value, then the TemperatureException is generated by IP Performance Manager. The default value is set at 45 degrees. You can change the threshold setting of this attribute in the Polling and Thresholds console to have the exception generated for a desired value.

Faults for VoltageSensor

Faults for VoltageSensor lists the faults detected for VoltageSensor.

Table 9-25. Faults and related thresholds for VoltageSensor

Voltage Fault	Description	Threshold
OutOfRange	Indicates that the voltage for this system is outside the normal operating range and exceeds the RelativeVoltageThreshold.	RelativeVoltageThreshold

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

Fabric Interconnect performance monitoring

IP Performance Manager discovers and monitors the following components of a Fabric Interconnect switch:

- Temperature sensors
- Voltage sensors
- Power supply
- Fan
- Memory

Note The discovery and monitoring of a processor is not supported as the MIB information is not present.

Discovery and monitoring of temperature sensors

MIB Object ID of temperature sensor used for discovery lists the MIB Object IDs used for discovery of temperature sensor in a Fabric Interconnect.

Table 9-26. MIB Object ID of temperature sensor used for discovery

Attributes in IP	MIB Attribute type	MIB Object ID
DisplayName	String	cucsSwEnvStatsDn 1.3.6.1.4.1.9.9.719.1.46.4.1.2
NA	Integer	cucsSwEnvStatsFanCtrlrInlet1 1.3.6.1.4.1.9.9.719.1.46.4.1.4
NA	Integer	cucsSwEnvStatsFanCtrlrInlet2 1.3.6.1.4.1.9.9.719.1.46.4.1.8
NA	Integer	cucsSwEnvStatsFanCtrlrInlet3 1.3.6.1.4.1.9.9.719.1.46.4.1.12
NA	Integer	cucsSwEnvStatsFanCtrlrInlet4 1.3.6.1.4.1.9.9.719.1.46.4.1.16
NA	Integer	cucsSwEnvStatsMainBoardOutlet1 1.3.6.1.4.1.9.9.719.1.46.4.1.21
NA	Integer	cucsSwEnvStatsMainBoardOutlet2 1.3.6.1.4.1.9.9.719.1.46.4.1.25
NA	Integer	cucsSwEnvStatsPsuCtrlrInlet1 1.3.6.1.4.1.9.9.719.1.46.4.1.29
NA	Integer	cucsSwEnvStatsPsuCtrlrInlet2 1.3.6.1.4.1.9.9.719.1.46.4.1.33

MIB Object IDs of temperature sensor used for performance monitoring lists the MIB Object IDs used for monitoring of temperature sensor in a Fabric Interconnect.

Table 9-27. MIB Object IDs of temperature sensor used for performance monitoring

Attribute in IP	MIB Attribute type	MIB Object ID
CurrentValue	Integer	cucsSwEnvStatsFanCtrlrInlet1 1.3.6.1.4.1.9.9.719.1.46.4.1.4
CurrentValue	Integer	cucsSwEnvStatsFanCtrlrInlet2 1.3.6.1.4.1.9.9.719.1.46.4.1.8
CurrentValue	Integer	cucsSwEnvStatsFanCtrlrInlet3 1.3.6.1.4.1.9.9.719.1.46.4.1.12
CurrentValue	Integer	cucsSwEnvStatsFanCtrlrInlet4 1.3.6.1.4.1.9.9.719.1.46.4.1.16
CurrentValue	Integer	cucsSwEnvStatsMainBoardOutlet1 1.3.6.1.4.1.9.9.719.1.46.4.1.21
CurrentValue	Integer	cucsSwEnvStatsMainBoardOutlet2 1.3.6.1.4.1.9.9.719.1.46.4.1.25
CurrentValue	Integer	cucsSwEnvStatsPsuCtrlrInlet1 1.3.6.1.4.1.9.9.719.1.46.4.1.29
CurrentValue	Integer	cucsSwEnvStatsPsuCtrlrInlet2 1.3.6.1.4.1.9.9.719.1.46.4.1.33

Discovery and monitoring of Voltage sensor

MIB Object IDs used for discovery and monitoring of voltage sensor lists the MIB Object IDs used for discovery and monitoring of voltage sensor in a Fabric Interconnect.

Table 9-28. MIB Object IDs used for discovery and monitoring of voltage sensor

Purpose	Attribute in IP	MIB attribute type	MIB Object ID
Discovery	DisplayName	String	cucsEquipmentPsuInputStatsDn 1.3.6.1.4.1.9.9.719.1.15.58.1.2
	NA	Integer	cucsEquipmentPsuInputStatsVoltage 1.3.6.1.4.1.9.9.719.1.15.58.1.18
Monitoring	CurrentValue	Integer	cucsEquipmentPsuInputStatsVoltage 1.3.6.1.4.1.9.9.719.1.15.58.1.18

Discovery and monitoring of Power supply

MIB Object IDs used for discovery and monitoring of Power Supply in Fabric Interconnect lists the MIB Object IDs used for discovery and monitoring of power supply present in a Fabric Interconnect. The MIB Object IDs are used during discovery of the Power supply present on the Fabric Interconnect.

Table 9-29. MIB Object IDs used for discovery and monitoring of Power Supply in Fabric Interconnect

Purpose	Attribute in IP	MIB attribute type	MIB Object ID
Discovery	DisplayName	String	cucsEquipmentPsuDn .1.3.6.1.4.1.9.9.719.1.15.56.1.2
	NA	Integer	cucsEquipmentPsuPresence . 1.3.6.1.4.1.9.9.719.1.15.56.1.11
Monitoring	Status	Integer	cucsEquipmentPsuOperState 1.3.6.1.4.1.9.9.719.1.15.56.1.7

Discovery and monitoring of Fan

MIB Object IDs used for discovery of fan in Fabric Interconnect lists the MIB Object IDs used for discovery and monitoring of fan instances in a Fabric Interconnect.

Table 9-30. MIB Object IDs used for discovery of fan in Fabric Interconnect

Purpose	Attribute in IP	MIB attribute type	MIB Object ID
Discovery	NA	Integer	cucsEquipmentFanPresence 1.3.6.1.4.1.9.9.719.1.15.12.1.13
	DisplayName	String	cucsEquipmentFanDn 1.3.6.1.4.1.9.9.719.1.15.12.1.2
Monitoring	Status	Integer	cucsEquipmentFanOperState 1.3.6.1.4.1.9.9.719.1.15.12.1.9

Discovery and monitoring of Memory

MIB Object IDs for discovery and monitoring of memory instances in Fabric Interconnect lists the MIB Object IDs used for discovery and monitoring of memory instance in a Fabric Interconnect.

Table 9-31. MIB Object IDs for discovery and monitoring of memory instances in Fabric Interconnect

Purpose	Attribute in IP	MIB attribute type	MIB Object ID
Discovery	DisplayName	String	cucsSwSystemStatsDn 1.3.6.1.4.1.9.9.719.1.46.28.1.2
	NA	String	cucsNetworkElementDn 1.3.6.1.4.1.9.9.719.1.32.1.1.2
Monitoring	TotalMemory	Gauge	cucsNetworkElementTotalMemory 1.3.6.1.4.1.9.9.719.1.32.1.1.18
	BufferUtilizationPct	Integer	cucsSwSystemStatsLoad 1.3.6.1.4.1.9.9.719.1.46.28.1.5

Root cause analysis for external switch Down

Root cause analysis for External Switch Down lists the root cause analysis for Switch (external) Down.

Table 9-32. Root cause analysis for External Switch Down

Class	Root cause		Events/Exception	Description	Impacted class
Switch (External switch)	Down	Indicates	Unresponsive	Indicates that the system is not responding to ICMP pings or SNMP polls.	Switch (Fabric Interconnect)
			Unresponsive	Indicates that the system is not responding to ICMP pings or SNMP polls.	BladeEnclosureManager
			Down/Unresponsive	Indicates that the host has failed.	Host
Card **Note** Card has a *ComposedOf* relationship with the ComputeFabric.	Down	Indicates	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.	BladeEnclosureManager

Host

A Host is a computer such as a workstation or server.

Attributes for Host

Attributes for Host lists the attributes for the class Host.

Table 9-33. Attributes for Host

Attribute	Descripton	Allowed values
AccessMode	The mode to access a system. It can have one of the following values: ICMPONLY, SNMPONLY, or ICMPSNMP.	Enum
AprioriProbability_Down		Float
BridgeAddress	The bridge address as defined in RFC1493.	String
Certification	The Certification attribute defines the level of certification that this device has in the discovery process: ■ UNSUPPORTED deprecated. ■ GENERIC indicates that the OID for the device is not recognized and the device will be classified as GENERIC and added to the Node class. Standard MIB-II data is used to perform analysis on the device. ■ TEMPLATE indicates that the device is recognized but that no information about the MIBs this device supports is unknown. ■ CERTIFIED indicates that the device has the highest level of certification and is discovered using enterprise MIBs as well as standard MIB-II data. ■ VALIDATED deprecated. ■ UNDISCOVERED indicates the system is undiscovered.	Enum
CIM_CreationClassName	CreationClassName attribute defined in CIM model.	String
CIM_Description	The Description property provides a textual description of the object.	String
CIM_Name	Name attribute defined in CIM model. It defines the label by which the object is known. When subclassed, the Name property can be overridden to be a Key property.	String
CreationClassName	The name of the most-derived class of this instance.	String
Description	A textual description of the object.	String
DiscoveredFirstAt	The time when the first discovery probe of this System occurred.	String
DiscoveredLastAt	The time when the last discovery probe of this System occurred.	String
DiscoveredLastAtToSeconds	The numeric time when the last discovery probe of this System occurred.	Unsigned-Integer
DiscoveryErrorInfo	A message describing the last discovery error for this System.	String
DiscoveryTime	The length of time it took for the last discovery probe of this System.	String
DisplayClassName	The string shown in the GUI when this object's class is displayed.	String
DisplayName	The string shown in the GUI when this object's name is displayed.	String
Domain	The domain to which the system belongs.	String

Table 9-33. Attributes for Host (Continued)

Attribute	Descripton	Allowed values
HasIPAddresses		Boolean
HasIPv6Addresses		Boolean
indexVal		String
IsAddressable	Set to TRUE if the system is IP addressable.	Boolean
IsDiscoveryInProgress	TRUE if discovery in progress for this system.	Boolean
IsEveryIPUnresponsive		Boolean
IsEveryIPv6Unresponsive		Boolean
IsEveryNeighborUnresponsive		Boolean
IsEveryServiceUnresponsive		Boolean
IsEverySNMPAgentUnresponsive		Boolean
IsManaged	The IsManaged attribute determines if an ICIM_ManagedSystemElement should be monitored by the management system. An unmanaged object will never have associated instrumentation. This attribute is readonly.	Boolean
IsMgmtStation	TRUE if this node is the Network Management Station.	Boolean
IsMightBeDown		Boolean
IsProxy	TRUE if this is a proxy of remote system.	Boolean
IsSeed	TRUE if the system is added as seed.	Boolean
IsUnmanagedOrUnresponsive		Boolean
IsUnmanagedOrUnresponsive_internal		Boolean
IsUnresponsive	TRUE indicates that the system is not responding to ICMP pings or SNMP polls. FALSE indicates that the system is responding to ICMP pings and/or SNMP polls.	Boolean
IsUnresponsive_internal		Boolean
KEYS	Types and Names of key attributes defined in CIM model.	String
Location	A description of where this System is located.	String
LossProbability_Unresponsive		Float
Model	The name by which the System is known.	String
MonitoringEnabled		Boolean
Name	Name of object.	String

Table 9-33. Attributes for Host (Continued)

Attribute	Descripton	Allowed values
NameFormat	The ComputerSystem object and its derivatives are Top Level Objects of ICIM. They provide the scope for numerous components. Having unique System keys is required. A heuristic is defined to create the ComputerSystem Name to attempt to always generate the same Name, independent of discovery protocol. This prevents inventory and management problems where the same asset or entity is discovered multiple times, but cannot be resolved to a single object. Use of the heuristic is optional, but recommended. The NameFormat property identifies how the ComputerSystem Name is generated, using a heuristic. The heuristic is outlined, in detail, in the CIM V2 System Model specification. It assumes that the documented rules are traversed in order, to determine and assign a Name. The NameFormat Values list defines the precedence order for assigning the ComputerSystem Name. Several rules do map to the same Value. Note that the ComputerSystem Name calculated using the heuristic is the System's key value. Other names, or Aliases, that better describe a business, can be assigned and used for the ComputerSystem.	Enum
NumberOfInterfaces		Unsigned-Integer
NumberOfIPs		Unsigned-Integer
NumberOfIPv6s		Unsigned-Integer
NumberOfNetworkAdapters		Unsigned-Integer
NumberOfPorts		Unsigned-Integer
OSVersion	The software version of this System's operating system.	String
PrimaryOwnerContact	A string that provides information on how the primary system owner can be reached (e.g., phone number, email address).	String
PrimaryOwnerName	The name of the primary owner of the ICIM_System.	String
ReadCommunity	The SNMP read community string.	String
ReconfiguredAfter	The DiscoveredLastAt value for which the last reconfigure is performed.	String
RemoveComponents	Enable or disable component deletion functionality for ICIM_System instances. This is used by remove() function. Default value is set to FALSE.	Boolean
ServiceName	Name of external server used for imported events and instrumented attributes.	String
ShortDiscoveredFirstAt	The time when the first discovery probe of this System occurred.	String

Table 9-33. Attributes for Host (Continued)

Attribute	Descripton	Allowed values
ShortDiscoveredLastAt	The time when the first discovery probe of this System occurred.	String
ShortDiscoveryTime	The time for the last discovery probe of this System.	String
SNMPAddress	The primary address used to contact the SNMP agent running on this System. Note that if this System hosts more than one network address, it may be possible that another address is currently being used to contact the agent.	String
SourceAddress	The system level source address. All the IP addresses that are hosted by the system use the address as source address unless each IP address has its own source address.	String
SupportsSNMP	TRUE if this system is manageable via SNMP.	Boolean
SystemName	The name of this ICIM_System object.	String
SystemObjectID	The System Object Identifier associated with the Vendor of this ComputerSystem.	String
Type	The Type attribute coarsely classifies the ComputerSystem. This attribute is used primarily for display purposes only. The actual capabilities of a ComputerSystem are reflected in the LogicalDevices, Services, and ServiceAccessPoints related to it.	Enum
UseBridgingRelationship	TRUE to use Bridging relationship in correlation.	Boolean
Vendor	The name of the System's supplier.	String

Events and Exceptions for Host

Events and Exceptions for Host lists the events and exceptions that are generated for Host by IP Availability Manager.

Table 9-34. Events and Exceptions for Host

Events	Description
ConnectivityException	Indicates that one or more connectivity-related root cause failures for a particular system or one of its components exist.
DiscoveryError	Indicates that an error occurred while discovering the system.
DiscoveryInProgress	Indicates that the discovery process is in progress.
Down	Indicates that the root cause is a failed system.
ErrorException	Indicates that one or more error-related failures exist for the network adapters of a particular system.
MightBeDown	Indicates that the system is not responding to SNMP polls or ICMP pings.
OperationalException	Indicates that one or more operational failures exist for a particular system or one of its components.

Table 9-34. Events and Exceptions for Host (Continued)

Events	Description
PerformanceException	Indicates that one or more performance-related failures exist for a particular system or one of its components.
PowerSupplyException	Indicates that power supply or voltage conditions around a system present a potential hazard.
ResourceException	Indicates that processor or memory faults are occurring because a system does not have enough processor or memory resources to process the current traffic load.
TemperatureException	Indicates that the temperature conditions around the system present a potential hazard.
Unresponsive	Indicates that all of the system's IPV4 and IPV6 addresses are not responding and the SNMP Agent is not responding.
Unstable	Indicates that the system is continuously restarting itself.

Switch

A system that switches packets, typically at wire speeds, between physically separate network segments.

Attributes of Switch

Attributes of Switch lists the attributes for the class Switch.

Table 9-35. Attributes of Switch

Attribute	Description	Allowed values
AccessMode	The mode to access a system. It can have one of the following values: ICMPONLY, SNMPONLY, or ICMPSNMP.	Enum
AprioriProbability_Down		Float
BridgeAddress	The bridge address as defined in RFC1493.	String
Certification	The Certification attribute defines the level of certification that this device has in the discovery process: ■ UNSUPPORTED deprecated. ■ GENERIC indicates that the OID for the device is not recognized and the device will be classified as GENERIC and added to the Node class. Standard MIB-II data is used to perform analysis on the device. ■ TEMPLATE indicates that the device is recognized but that no information about the MIBs this device supports is unknown. ■ CERTIFIED indicates that the device has the highest level of certification and is discovered using enterprise MIBs as well as standard MIB-II data. ■ VALIDATED deprecated. UNDISCOVERED indicates the system is undiscovered.	Enum
CIM_CreationClassName	CreationClassName attribute defined in CIM model.	String

Table 9-35. Attributes of Switch (Continued)

Attribute	Description	Allowed values
CIM_Description	The Description property provides a textual description of the object.	String
CIM_Name	Name attribute defined in CIM model. It defines the label by which the object is known. When subclassed, the Name property can be overridden to be a Key property.	String
CreationClassName	The name of the most-derived class of this instance.	String
Description	A textual description of the object.	String
DesignatedRoot	The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol as executed by this Bridge. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.	String
DesignatedRootPort	The port number of the port which offers the lowest cost path from this Bridge to the root Bridge.	Integer
DiscoveredFirstAt	The time when the first discovery probe of this System occurred.	String
DiscoveredLastAt	The time when the last discovery probe of this System occurred.	String
DiscoveredLastAtToSeconds	The numeric time when the last discovery probe of this System occurred.	Unsigned-Integer
DiscoveryErrorInfo	A message describing the last discovery error for this System.	String
DiscoveryTime	The time taken for the last discovery probe of this System.	String
DisplayClassName	The string shown in the GUI when this object's class is displayed.	String
DisplayName	The string shown in the GUI when this object's name is displayed.	String
Domain	The domain to which the system belongs.	String
HasIPAddresses		Boolean
HasIPv6Addresses		Boolean
indexVal		String
IsAddressable	Set to TRUE if the system is IP addressable.	Boolean
IsDiscoveryInProgress	TRUE if discovery is in progress for this system.	Boolean
IsEveryIPUnresponsive		Boolean
IsEveryIPv6Unresponsive		Boolean
IsEveryNeighborUnresponsive		Boolean
IsEveryServiceUnresponsive		Boolean
IsManaged	The IsManaged attribute determines if an ICIM_ManagedSystemElement should be monitored by the management system. An unmanaged object will never have associated instrumentation. This attribute is readonly.	Boolean

Table 9-35. Attributes of Switch (Continued)

Attribute	Description	Allowed values
IsMightBeDown		Boolean
IsProxy	TRUE if this is a proxy of remote system.	Boolean
IsSeed	TRUE if the system is added as seed.	Boolean
IsUnmanagedOrUnresponsive		Boolean
IsUnmanagedOrUnresponsive_internal		Boolean
IsUnresponsive	TRUE indicates that the system is not responding to ICMP pings or SNMP polls. FALSE indicates that the system is responding to ICMP pings and/or SNMP polls.	Boolean
IsUnresponsive_internal	TRUE indicates that the system is not responding to ICMP pings or SNMP polls. FALSE indicates that the system is responding to ICMP pings and/or SNMP polls.	Boolean
KEYS	Types and Names of key attributes defined in CIM model.	String
Location	A description of where this System is located.	String
Model	The name by which the System is generally known.	String
MonitoringEnabled		Boolean
Name	Name of object	String
NameFormat	The ComputerSystem object and its derivatives are Top Level Objects of ICIM. They provide the scope for numerous components. Having unique System keys is required. A heuristic is defined to create the ComputerSystem Name to attempt to always generate the same Name, independent of discovery protocol. This prevents inventory and management problems where the same asset or entity is discovered multiple times, but cannot be resolved to a single object. Use of the heuristic is optional, but recommended. The NameFormat property identifies how the ComputerSystem Name is generated, using a heuristic. The heuristic is outlined, in detail, in the CIM V2 System Model spec. It assumes that the documented rules are traversed in order, to determine and assign a Name. The NameFormat Values list defines the precedence order for assigning the ComputerSystem Name. Several rules do map to the same Value. Note that the ComputerSystem Name calculated using the heuristic is the System's key value. Other names, or Aliases, that better describe a business, can be assigned and used for the ComputerSystem.	Enum
NumberOfInterfaces		Unsigned-Integer
NumberOfIPs		Unsigned-Integer
NumberOfIPv6s		Unsigned-Integer

Table 9-35. Attributes of Switch (Continued)

Attribute	Description	Allowed values
NumberOfNetworkAdapters		Unsigned-Integer
NumberOfPorts		Unsigned-Integer
OSVersion	The software version of this System's operating system.	String
PrimaryOwnerContact	A string that provides information on how the primary system owner can be reached (e.g., phone number, email address).	String
PrimaryOwnerName	The name of the primary owner of the ICIM_System.	String
ReadCommunity	The SNMP read community string.	String
ReconfiguredAfter	The DiscoveredLastAt value for which the last reconfigure is performed.	String
RemoveComponents	Enable or disable component deletion functionality for ICIM_System instances. This is used by remove() function. Default value is set to FALSE.	Boolean
ServiceName	Name of external server used for imported events and instrumented attributes.	String
ShortDiscoveredFirstAt	The time when the first discovery probe of this System occurred.	String
ShortDiscoveredLastAt	The time when the first discovery probe of this System occurred.	String
ShortDiscoveryTime	The time for the last discovery probe of this System.	String
SNMPAddress	The primary address used to contact the SNMP agent running on this System. Note that if this System hosts more than one network address, it may be possible that another address is currently being used to contact the agent.	String
SourceAddress	The system level source address. All the IP addresses that are hosted by the system use the address as source address unless each IP address has its own source address.	String
SupportsSNMP	TRUE if this system is manageable via SNMP.	Boolean
SystemName	The name of this ICIM_System object.	String
SystemObjectID	The System Object Identifier associated with the Vendor of this ComputerSystem.	String
Type	The Type attribute coarsely classifies the ComputerSystem. This attribute is used primarily for display purposes only. The actual capabilities of a ComputerSystem are reflected in the LogicalDevices, Services, and ServiceAccessPoints related to it.	Enum
UseBridgingRelationship	TRUE to use Bridging relationship in correlation.	Boolean
Vendor	The name of the System's supplier.	String

Events and Exceptions for Switch

All the Events and Exceptions listed in Events and Exceptions for Switch are applicable for Switch.

Chassis

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

Attributes for Chassis

Attributes for Chassis lists some key attributes for Chassis.

Table 9-36. 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 and ICMPv6 pings or SNMP polls or both.	Boolean: TRUE, 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 9-36. 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
IsManaged	Determines if an ICIM_ManagedSystemElement should be monitored by the management system. An unmanaged object do not have associated instrumentation. This attribute is readonly.	Boolean: TRUE, FALSE

Root-cause problem 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

Events for Chassis lists the events detected for Chassis.

Table 9-37. Events for Chassis

Events	Description	Subscribed to by the Global Manager
HighBackplaneUtilization	Indicates that the percentage of bandwidth utilization for the Chassis backplane is reported by the instrumentation	Yes
OperationallyDown	Indicates that the physical element is in a critical condition.	No

Exceptions for Chassis by IP Availability Manager

Exceptions for Chassis lists the exceptions for Chassis.

Table 9-38. Exceptions for Chassis

Exceptions	Description
HighBackplaneUtilizationException	Indicates that the data being transmitted over the Chassis's backplane has exceeded BackplaneUtilizationThreshold
OperationalException	Indicates that the physical element is operationally down.

Exceptions for Chassis by IP Performance Manager

IP Performance Manager generates the following exception for Chassis.

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

Faults for Chassis

IP Performance Manager detects the following fault for Chassis.

HighBackplaneUtilization fault: The data being transmitted over the Chassis' backplane has exceeded the BackplaneUtilizationThreshold. This threshold is contained in the Processor and Memory setting, described in the VMware Smart Assurance IP Management Suite Configuration Guide.

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

Attributes for Card lists some key attributes for Card.

Table 9-39. 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, FALSE
IsSwitchOverActive	TRUE if this Card has switched over to the active state.	Boolean: TRUE, FALSE
IsSystemUnresponsive	TRUE if this Card is not responding to ICMP and ICMPv6 pings or SNMP polls. (FALSE if this Card is responding to ICMP pings or SNMP polls or both.)	Boolean: TRUE, 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-10.9.252.11/16.0.0.96.105.144.4.243.0.0.0.0.0.0.0.0	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 9-39. 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 and any system functions associated with the card to fail. For example, if an RSM (Router Switch Module) 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

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

Table 9-40. 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 and IP Performance Manager performs performance analysis on the following network adapter object types:

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

  IP Availability Manager and IP Performance Manager separate ports into two groups: trunk ports and access ports. An access port is any port that provides a connection for end users or node devices, such as routers or servers.

  A trunk port is a port that interconnects switches. A trunk port is a member of all the VLANs that exist on the switch and carry traffic for all those VLANs between the switches. All the other ports are access ports. Access ports are assigned to a single VLAN and provide a connection for end users or node devices, such as a router or server.

  Note By default, IP Performance Manager monitors trunk ports and also access ports (as long as the system to which the access port is connected is managed). However, if you so choose, you can enforce a management policy that manages access ports, as described in the VMware Smart Assurance 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

Attributes for Network adapter lists some key attributes for network adapter.

Table 9-41. 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 **Note** In IP 9.1, if ports and interfaces do not have instrumentation, then the CurrentUtilization value will be displayed as zero.	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 9-41. 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, 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
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

Table 9-41. Attributes for Network adapter (Continued)

Attribute	Description	Allowed values
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)
SystemName	Name of the system containing this network adapter; for example: 10.9.1.108	String

Table 9-41. Attributes for Network adapter (Continued)

Attribute	Description	Allowed values
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 **Note** The configuration file InterfaceType.conf has the exhaustive list of allowed values. The configuration file is located at:BASEDIR/smarts/conf/discovery

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.

There are physical interfaces that underlie logical interfaces. These physical interfaces may not have a direct network connection associated with them, but the logical interfaces that are layered over those physical interfaces have a direct network connection. In such a scenario, if a physical interface goes down, it will be the root cause of network connections for logical interfaces going down. In this case, Interface Down will be the root cause and will have network connection alerts as its impact.

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. The VMware Smart Assurance IP Management Suite Configuration Guide provides information about the Testing Notification Mode threshold.

The events used to diagnose Down include:

- DownOrFlapping
- System 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. The VMware Smart Assurance IP Management Suite Configuration Guide provides information about these parameters.

“Diagnosis of Unstable Objects” on page 129 provides more information about how IP Availability Manager concludes that a network adapter is unstable. (In concepts guide)

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. “Diagnosis of Unstable Objects” on page 129 explains how to enable Interface Unstable analysis for these types of interfaces. (in concepts guide)

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

- DownOrFlapping
- 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.

The events used to diagnose Disabled include:

- AdministrativelyDown
- DownOrFlapping
- System MightBeDown for all 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 by 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:

- Network Adapter DownOrFlapping
- System MightBeDown for all logically connected systems

Events for Network adapter

Events for Network adapter 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 9-42. 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. The VMware Smart Assurance IP Management Suite Configuration Guide provides information about backup activation.
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. The VMware Smart Assurance 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 experiencing transient functional problems.
OperationallyDown	OperationallyDown indicates that the port/interface is down, but is supposed to be up.

Faults for Network adapter

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

- HighBroadcastRate
- HighDiscardRate
- HighQueueDropRate
- HighCollisionRate
- HighUtilization

- HighErrorRate

  Note To enable subinterface performance analysis, see the Generic Interface/Port Performance setting description or the Ethernet Interface/Port Performance setting description in Chapter 7, Customizing Polled Data Thresholds, in the VMware Smart Assurance IP Management Suite Configuration Guide.

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

HighBroadcastRate fault

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

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

HighDiscardRate fault

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

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

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

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

HighQueueDropRate fault

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

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

HighCollisionRate fault

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

This threshold is contained in the Ethernet Interface/Port Performance setting. The VMware Smart Assurance IP Management Suite Configuration Guide describes this setting.

Note This fault is detected only for Ethernet adapters.

HighUtilization fault

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

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

- The speed of a port or interface is the maximum rate at which it can transport information. Speed is usually expressed in bits per second (bps).
- The duplex mode for a port or interface controls whether data transmission is full-duplex or half-duplex. With full-duplex transmission, both ends of a network connection can send data simultaneously. With half-duplex transmission, only one end of a network connection can send data at a time. If the duplex mode is unspecified, IP Performance Manager cannot monitor the adapter for HighUtilization faults. Duplex-mode discovery for Network adapters provides more information about how IP Performance Manager determines duplex mode for a port or interface.

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

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

- If the system is full-duplex, the limiting factor is the more heavily loaded (outgoing or incoming) wire. For a full-duplex, 100,000 bps system, each wire can carry 1,000,000 bits in 10 seconds. The outgoing wire carried 450,000 bits, or 45 percent of the theoretical capacity; the incoming wire carried 400,000 bits, or 40 percent of capacity. IP Performance Manager defines the current utilization as 45 percent, the higher percentage.

- If the system is half-duplex, the total traffic has to go over a single wire. In this case, a total of 850,000 bits moved over the wire, which could have carried 1,000,000. Hence, the current utilization is 85 percent.

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

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

HighErrorRate fault

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

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

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

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

  The ErrorThreshold and the MinimumTrafficThreshold are contained in the Generic Interface/Port Performance setting and the Ethernet Interface/Port Performance setting. Chapter 7, "Customizing Polled Data Thresholds," in the VMware Smart Assurance IP Management Suite Configuration Guide describes these settings.

Duplex-mode discovery for Network adapters

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

- If duplex mode is full-duplex or half-duplex, IP Performance Manager calculates current utilization for the adapter and monitors the adapter for HighUtilization faults.

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

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

Determining duplex-mode

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

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

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

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

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

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

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

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

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

Understanding the DuplexAssumed parameter

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

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

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

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

  Note Be aware that monitoring all network adapters in the topology requires considerable system resources. Ensure that your server is sized properly to accommodate the size of your environment, as described in the VMware Smart Assurance IP Manager Deployment Guide.

  A value of FALSE means that IP Performance Manager will monitor *only* those network adapters that can be determined as full-duplex or half-duplex by reading the Enterprise MIB, ETHERLIKE-MIB, and Neighbor MIB. Any network adapter having an unspecified duplex mode setting will be ignored.Chapter 2, "Setting Configuration Parameters," in the VMware Smart Assurance IP Management Suite Configuration Guide provides information about the discovery.conf file.

Using the setDuplexMode command

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

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

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

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

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

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

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

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

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

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

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

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

Other network adapters that are not monitored

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

- If the network adapter is unmanaged, it is not monitored.
- If the network adapter uses the description of “*Vlan” for a Cisco device, it is not monitored.

  If the interface is a subinterface, it is not monitored unless subinterface performance analysis is enabled, which is explained in the Generic Interface/Port Performance setting or the Ethernet Interface/Port Performance setting. The VMware Smart Assurance IP Management Suite Configuration Guide describes these settings.

Wireless LAN

A wireless LAN consists of wireless controllers, WirelessAccessPoints, WirelessClients and SSIDs.

IP 9.1 provides support for Wireless LAN network for two vendors, namely Cisco and Aruba. The certification of the two vendors can be found in the following conf files:

- oid2Type_Cisco.conf in <*BASEDIR*>\IP\smarts\conf\discovery
- oid2Type_Aruba.conf in <*BASEDIR*>\IP\smarts\conf\discovery

  List of certified Wireless Controllers and WirelessAccessPoints lists the WirelessControllers and the WirelessAccessPoints that have been certified.

Table 9-43. List of certified Wireless Controllers and WirelessAccessPoints

Wireless LAN Vendor	Components of a wireless LAN network			
	Wireless Controller	System Object ID	Access Points	System Object ID
Aruba	Aruba 2400	.1.3.6.1.4.1.14823.1.1.2		
	Aruba 650	1.3.6.1.4.1.14823.1.1.19		
	Aruba 3400	1.3.6.1.4.1.14823.1.1.15		
	Aruba 3600	1.3.6.1.4.1.14823.1.1.17		
	Aruba 6000	1.3.6.1.4.1.14823.1.1.4		
Cisco	Cisco 4402-25 WLAN Controller	.1.3.6.1.4.1.14179.1.1.4.3	Aironet Access Point 1210	.1.3.6.1.4.1.9.1.525

Table 9-43. List of certified Wireless Controllers and WirelessAccessPoints (Continued)

Wireless LAN Vendor	Components of a wireless LAN network			
	Wireless Controller	System Object ID	Access Points	System Object ID
	Cisco 5508	1.3.6.1.4.1.9.1.1069		
	Cisco 2106	1.3.6.1.4.1.9.1.828		
	Cisco 6509 WISM	1.3.6.1.4.1.14179.1.1.4.4		

Wirless LAN attributes in ICF Topology Manager

Wireless license and wireless LAN related attributes in ICF Topology Manager lists the wireless license and wireless LAN related attributes in ICF Topology Manager.

Table 9-44. Wireless license and wireless LAN related attributes in ICF Topology Manager

Attributes	Description	Allowed values
WIFILicenseEnabled	Indicates whether wireless license is available or not.	Boolean: TRUE, FALSE
RemainingWirelessAccessPointCounts	Indicates the total Wireless Access Point block licenses available in the license server.	Unsigned-Int
RemainingWirelessControllerCounts	Indicates the total Wireless Controller block licenses available in the license server.	Unsigned-Int
TotalWirelessController	Indicates the total Wireless Controllers in the topology.	Unsigned-Int
TotalWirelessAccessPoints	Indicates the total Wireless Access Points in the topology.	Unsigned-Int
TotalWirelessClients	Indicates the total Wireless Clients in the topology.	Unsigned-Int
TotalWirelessAuthenticationServer	Indicates the total Wireless Authentication Servers in the topology.	Unsigned-Int
TotalWirelessControllerLicenseCheckedOut	Indicates the total Wireless Controller license checked out from the license server.	Unsigned-Int
TotalWirelessAccessPointsLicenseCheckedOut	Indicates the total Wireless Access Points license checked out from the license server.	Unsigned-Int
WirelessAccessPointLicenseExceeded	Indicates that the total Wireless Access Point license count exceeds the limit in the license server.	Boolean: TRUE, FALSE
WirelessControllerLicenseExceeded	Indicates that the total Wireless Controller license count exceeds the limit in the license server.	Boolean: TRUE, FALSE

WirelessAccessPoint

WirelessAccessPoint is a device that logically connects WirelessClients operating in a network to one another. It provides access to a distribution system, if connected, which is typically an enterprise wired network. This device is managed by the WirelessController. It acts as a central transmitter and receiver of WLAN radio signals. WirelssClients are connected to the WirelessAccessPoint switches.

Relationship

A WirelessAccessPoint is defined by the following relationships:

- *ControlledBy/Controls* relationship with WirelessController
- *Hosts/HostedBy* relationship with Station
- *HostsAccessPoints/HostedBy* relationship with IP and MAC
- *ListsOfHostsAccessPoints/HostedBy* relationship with IP and MAC

Attributes of WirelessAccessPoints

Attributes of WirelessAccessPoints lists the attributes of WirelessAccessPoints.

Table 9-45. Attributes of WirelessAccessPoints

Attributes	Description	Values
AccessMode	The mode to access a system. It can have one of the following values: ICMPONLY, SNMPONLY, or ICMPSNMP.	Enum
WirelessAccessPointMode	Mode of the access point. Values can be master, adhoc or monitor.	String
BSSID	The Basic Service Set IDentifier that uniquely identifies the BSS.	String
BridgeAddress	The bridge address as defined in RFC1493.	String
Certification	The Certification attribute defines the level of certification that this device has in the discovery process: UNSUPPORTED deprecated. GENERIC indicates that the OID for the device is not recognized and the device will be classified as GENERIC and added to the Node class. Standard MIB-II data is used to perform analysis on the device. TEMPLATE indicates that the device's certification is provided based on a family of devices it is part of it, but the completeness of the certification is not observed. CERTIFIED indicates that the device has the highest level of certification and is discovered using enterprise MIBs as well as standard MIB-II data. VALIDATED deprecated. UNDISCOVERED indicates the system is undiscovered.	Enum
Channel	The current operating frequency channel.	Integer

Table 9-45. Attributes of WirelessAccessPoints (Continued)

Attributes	Description	Values
DesignatedRoot	The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol as executed by this Bridge. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.	String
DesignatedRootPort	The port number of the port which offers the lowest cost path from this Bridge to the root Bridge.	
ESSID	The Extended Service Set IDentifier that uniquely identifies the ESS.	String
IsRogue	Indicates whether this WirelessAccessPoint is a Rogue WirelessAccessPoint or not. A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack.	Boolean: TRUE, FALSE Default value: FALSE.
RogueType	Indicates the type of identified Rogue WirelessAccessPoint.	Values can be: ■ valid ■ interfering ■ unsecure ■ dos ■ unknown ■ knownInterfering ■ suspectedUnsecure ■ initializing ■ pending ■ alert ■ detectedLrad ■ known ■ acknowledge ■ contained ■ threat ■ containedPending ■ knownContained ■ trustedMissing Default value: Uninitialized
IsSeed	TRUE if the system is added as seed.	Boolean: TRUE, FALSE
IsThinClient	Indicates whether the WirelessAccessPoint is a thin client or not.	Boolean: TRUE, FALSE
PhysicalLayerProtocol	The physical layer support protocol for the WirelessAccessPoint.	String
RemoveComponents	Enable or disable component deletion functionality for ICIM_System instances. This is used by remove() function. Default value is set to FALSE.	Boolean: TRUE, FALSE

Table 9-45. Attributes of WirelessAccessPoints (Continued)

Attributes	Description	Values
SourceAddress	The system level source address. All the IP addresses that hosted by the system use the address as source address unless each IP address has its own source address.	String: 0.0.0.0
WirelessClientThreshold	Maximum number of WirelessClient devices that can be associated with this WirelessAccessPoint at a given time.	Integer
SystemObjectID	The System Object Identifier associated with the Vendor of this system.	String

Events and Exceptions

Events and Exceptions of WirelessAccessPoints lists the events and exceptions generated for WirelessAccessPoints.

Table 9-46. Events and Exceptions of WirelessAccessPoints

Events	Description
RogueWirelessAccessPointDetected	Indicates that this WirelessAccessPoint is a Rogue WirelessAccessPoint. This event is generated only if a WirelessAccessPoint is managed and monitored, and the attribute IsRogue = TRUE.
Disabled	Indicates that a disabled WirelessAccessPoint is the root cause.
DiscoveryError	Indicates that an error occurred while discovering the system. DiscoveryError is notified under the following circumstances: - SNMP requests times out - SNMP agent encounters a loop - system is unreachable (Down) - Qualified access address not found
Down	Indicates that a failure on a WirelessAccessPoint is the root cause.
DiscoveryInProgress	Indicates that discovering the system is in progress.
MightBeDown	Indicates that the system is not responding to SNMP polls or ICMP pings and is logically near the root-cause problem.
OutOfWapLicense	Indicates that the WirelessAccessPoint block license has exceeded its limit in the license server.
LowOnWapLicenseCount	Indicates that the WirelessAccessPoint license count has reached its threshold. **Note** This event is generated when the license count exceeds the value set for the parameter *LicenseThresholdPercentage* in the discovery.conf file. Default value = 90%.
ThresholdReached	Indicates that the maximum number of Stations that can be connected to this WirelessAccessPoint has reached.
Unresponsive	Indicates that IPv4 and IPv6 addresses of the system are not responding. Also, indicates that the SNMP Agent is not responding.
Unstable	Indicates that the system is restarting itself continuously.
OperationalException	Indicates that one or more operational related failures exist for a particular system or one of its components.

Table 9-46. Events and Exceptions of WirelessAccessPoints (Continued)

Events	Description
PerformanceException	Indicates that one or more performance-related failures exist for the network adapters of a particular system.
PowerSupplyException	Indicates that one or more voltage or power supply faults exist for a particular system.
ResourceException	Indicates that one or more processor or memory related faults exist for a particular system.
TemperatureException	Indicates that one or more fan or temperature related faults exist for a particular system.
ErrorException	Indicates that one or more error-related failures exist for the network adapters of a particular system.
ConnectivityException	Indicates that one or more connectivity-related root-cause failures for a particular system or one of its components.
WirelessClientThresholdExceeded	Indicates that the maximum number of WirelessClients that can be connected to this WirelessAccessPoint has exceeded the threshold.

WirelessClient

A WirelessClient is a mobile device such as a laptop, personal digital assistant, IP phone, smart phone, or any fixed device such as a desktop or workstation that is equipped with a wireless LAN interface which allows communication with a WirelessAccessPoint.

Relationships

A WirelessClient is defined by the following relationships:

- *HostedBy/Hosts* relationship with WirelessAccessPoint
- *HostsWirelessAccessPoints/HostedBy* relationship with MAC
- *ListsOfHostsAccessPoints/HostedBy* relationship with MAC

Attributes of WirelessClient

Attributes of WirelessClient list the attributes of a WirelessClient.

Table 9-47. Attributes of WirelessClient

Attribute	Description	Value
AccessMode	The mode to access a system. It can have one of the following values: ICMPONLY, SNMPONLY, or ICMPSNMP.	Enum
BridgeAddress	The bridge address as defined in RFC1493.	Value

Table 9-47. Attributes of WirelessClient (Continued)

Attribute	Description	Value
Certification	The Certification attribute defines the level of certification that this device has in the discovery process: UNSUPPORTED deprecated. GENERIC indicates that the OID for the device is not recognized and the device will be classified as GENERIC and added to the Node class. Standard MIB-II data is used to perform analysis on the device. TEMPLATE indicates that the device's certification is provided based on a family of devices it is part of it, but the completeness of the certification is not observed. CERTIFIED indicates that the device has the highest level of certification and is discovered using enterprise MIBs as well as standard MIB-II data. VALIDATED deprecated. UNDISCOVERED indicates the system is undiscovered.	Enum
SignalStrength	Indicates the wireless signal strength from the WirelessAccesspoint. The unit is dBm.	Integer
SourceAddress	The system level source address. All the IP addresses that hosted by the system use the address as source address unless each IP address has its own source address.	String
SupportsSNMP	TRUE if this system is manageable via SNMP.	Boolean
SystemObjectID	The System Object Identifier associated with the Vendor of this system.	String
Type	The Type attribute coarsely classifies the system. This attribute is used primarily for display purposes only. The actual capabilities of a system are reflected in the LogicalDevices, Services, and ServiceAccessPoints related to it.	Enum
UseBridgingRelationship	TRUE to use Bridging relationship in correlation.	Boolean

Events and Exceptions of WirelessClient

Exceptions and events of WirelessClient lists the events and exceptions generated for a WirelessClient.

Table 9-48. Exceptions and events of WirelessClient

Events and Exception	Description
DiscoveryError	Indicates that an error occurred while discovering the system. DiscoveryError is notified under the following circumstances: SNMP requests times out SNMP agent encounters a loop system is unreachable (Down) Qualified access address not found
DiscoveryInProgress	Indicates that discovering the system is in progress.
Down	Indicates that a failure on a WirelessClient is the root cause.
MightBeDown	Indicates that the system is not responding to SNMP polls or ICMP pings. Logically, this also indicates that it is near the root-cause problem.
Unstable	Indicates that the system is continuously restarting itself.
Unresponsive	Indicates that all of the system's IPv4 and IPv6 addresses not responding and the SNMPAgent is not responding as well.

Table 9-48. Exceptions and events of WirelessClient (Continued)

Events and Exception	Description
ConnectivityException	Indicates that one or more connectivity-related root-cause failures for a particular system or one of its components.
ErrorException	Indicates that one or more error-related failures exist for the network adapters of a particular system.
OperationalException	Indicates that one or more operational-related failures exist for a particular system or one of its components.
PerformanceException	Indicates that one or more performance-related failures exist for the network adapters of a particular system.
PowerSupplyException	Indicates that one or more voltage or power supply faults exist for a particular system.
ResourceException	Indicates that one or more processor or memory related faults exist for a particular system.
TemperatureException	Indicates that one or more fan or temperature related faults exist for a particular system.

SSID

A service set identifier (SSID) is a sequence of characters that uniquely names a wireless local area network (WLAN). It is advertised by the WirelessAccessPoint for a wireless LAN. An SSID is also referred to as a *network name*.

Each set of wireless devices communicating directly with each other is called a basic service set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS).

Note The Service Set Identifier uniquely identifies the ESS.

Relationship

SSID is defined by the *UsedBy* relationship with WirelessClient. Conversely, a WirelessClient is defined by the *Uses* relationship with SSID.

Attributes of SSID

Attributes of SSID lists attributes of SSID.

Table 9-49. Attributes of SSID

Attribute	Description	Value
ApplicationName	ApplicationName is equal to the Name of the SoftwareService that this connection is PartOf. If there is no containing application then it is set to the empty string. A connection should be modeled as a component of an application when it represents an internal communication pathway between components. For example, the transaction between the web container and a servlet within an Application Server.	String
CIM_Name	This attribute is defined in CIM model. It defines the label by which the object is known.	String
ProfileNames	List of profile names corresponding to this SSID.	String

WirelessController

The wireless LAN controller is modelled as a WirelessController class in the IP topology.

WirelessController is a centralized device in a network, to which all the WirelessAccessPoints on the network are directly or indirectly connected. It also configures and manages the WirelessAcccessPoints.

Relationship

A WirelessController is defined by the following relationships:

- *ComposedOf/PartOf* relationship with Interface, Memory, PowerSupply, Processor, TemperatureSensor
- *ConnectedVia/ConnectedSystems* relationship with IP network
- *Controls/ControlledBy* relationship with WirelessAccessPoint
- *HostsWirelessAccessPoints/HostedBy* relationship with IP and MAC
- *HostsServices/HostedBy* relationship with SNMP Agent
- *HostsStations/HostedBy* relationship with WirelessClient
- *ListsOfHostsAccessPoints/HostedBy* relationship with IP and MAC
- *SystemPackagedIn/PackagesSystems* relationship with Chassis

Attributes of WirelessControllers

Attributes of WirelessController lists the attributes of a WirelessController.

Table 9-50. Attributes of WirelessController

Attributes	Description	Values
AccessMode	The mode to access a system. It can have one of the following values: ICMPONLY, SNMPONLY, or ICMPSNMP.	Enum
ApThreshold	Maximum number of WirelessAccessPoints that can be associated with this Controller at a given time.	Integer

Table 9-50. Attributes of WirelessController (Continued)

Attributes	Description	Values
BridgeAddress	The bridge address as defined in RFC1493.	string
Certification	The Certification attribute defines the level of certification that this device has in the discovery process: UNSUPPORTED deprecated. GENERIC indicates that the OID for the device is not recognized and the device will be classified as GENERIC and added to the Node class. Standard MIB-II data is used to perform analysis on the device. TEMPLATE indicates that the device's certification is provided based on a family of devices it is part of it, but the completeness of the certification is not observed. CERTIFIED indicates that the device has the highest level of certification and is discovered using enterprise MIBs as well as standard MIB-II data. VALIDATED deprecated. UNDISCOVERED indicates the system is undiscovered.	Enum
DesignatedRoot	The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol as executed by this Bridge. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.	String
DesignatedRootPort	The port number of the port which offers the lowest cost path from this Bridge to the root Bridge.	Integer
NumberOfAPs	Number of WirelessAccessPoints currently associated with this Controller.	Integer
RemoveComponents	Enable or disable component deletion functionality for ICIM_System instances. This is used by remove() function. Default value is set to FALSE.	Boolean: TRUE, FALSE
Role	Indicates the role of the controller. Master, Local and Backup are the valid three values.	String
SourceAddress	The system level source address. All the IP addresses that hosted by the system use the address as source address unless each IP address has its own source address.	String
SystemObjectID	The System Object Identifier associated with the Vendor of this system.	String
UseBridgingRelationship	TRUE to use Bridging relationship in correlation.	Boolean

Events of WirelessController

Events of WirelessController lists the events that are generated for WirelessController.

Table 9-51. Events of WirelessController

Events	Description
APThresholdReached	
DiscoveryError	Indicates that an error occurred while discovering the system. DiscoveryError is notified when: SNMP requests times out SNMP agent encounters a loop System is unreachable (Down) Qualified access address not found
DiscoveryInProgress	Indicates that discovery process for the system is in progress.
Down	Indicates that the root cause is a failed system.
MightBeDown	Indicates that the system is not responding to SNMP polls or ICMP pings and is logically near the root-cause problem.
OutOfWctlLicense	Indicates that the WirelessController block license has exceeded its limit in the license server.
LowOnWctlCountLicense	Indicates that the WirelessController license count has reached its threshold. **Note** This event is generated if the license count exceeds the value set for the parameter *LicenseThresholdPercentage* in the discovery.conf file. Default value = 90%.
StationThresholdReached	
Unresponsive	Indicates that all the IPv4 and I Pv6 addresses for the system are not responding. Also indicates that the SNMPAgent is not responding.
Unstable	Indicates that the system is restarting itself continuously .
TemperatureException	Indicates that one or more fan or temperature related faults exist for a particular system.
ResourceException	Indicates that one or more processor or memory related faults exist for a particular system.
PowerSupplyException	Indicates that one or more voltage or power supply faults exist for a particular system.
PerformanceException	Indicates that one or more performance-related failures exist for the network adapters of a particular system.
OperationalException	Indicates that one or more operational-related failures exist for a particular system or one of its components.
ErrorException	Indicates that one or more error-related failures exist for the network adapters of a particular system.
ConnectivityException	Indicates that one or more connectivity-related root-cause failures for a particular system or one of its components.
WirelessAccessPointThresholdExceeded	Indicates that the maximum number of WirelessAccessPoints that can be connected to this WirelessController has exceeded the threshold.
WirelessClientThresholdExceeded	Indicates that the maximum number of WirelessClients that can be connected to this WirelessController has exceeded the threshold.

AuthenticationServer

The IP Manager discovers and monitors the athentication server. An authentication server provides authentication service for different network element such as WirelessClient. Authentication servers are connected to WirelessController. The request for authentication pass through the WirelessController from WirelessClient to the authentication server. IP Manager discovers the authentication server while discovering the WirelessController.

In IP topology, the authentication server is represented by the class *AuthenticationServer*. It is defined by the *AuthenticationServiceTo* relationship with the WirelessController. The WirelessController provide the MIB information for authentication server. The discovery of authentication server by IP is done while discovering the WirelessController.

Note IP server does not generate any alert if the status of the Authentication Server is UNKNOWN. So if the WirelessController is *Down,* the related Authentication Server status is UNKNOWN. Therefore, to get the proper status of the Authentication Server, rediscover the running WirelessContoller that is serviced by same Authentication Server.

Attributes of an Authentication Server

Attributes of AuthenticationServer lists the attributes of an Authentication Server.

Table 9-52. Attributes of AuthenticationServer

Attributes	Description	Allowed values
AuthServerType	Indicates the type of Authentication Server.	String
BridgeAddress	This is the bridge address as defined in RFC1493.	String
ControllingEntity	The SystemName of the Controlling System. By default, System controls itself.	String
PortNumber	The port to which the authentication server is listening.	Integer

Events of an AuthenticationServer

Table 9-53. Events of an AuthenticationServer

Events	Description
AuthenticationServerDisabled	Indicates that the Authentication Server is disabled. This is the supporting event for Disabled problem.
Disabled	Indicates that a disabled AuthenticationServer is the root-cause of the symptom.
AuthServerNotReachable	Indicates that Authentication server is not reachable through the WirelessController.

Events of an AuthenticationServer lists the events that are generated for an AuthenticationServer.

Root-cause analysis of a wireless LAN

IP 9.1 provides root-cause analysis of wireless LAN for three different deployment scenarios:

- **Thin Client Centralized Deployment** as listed in Root-cause analysis of a wireless LAN Thin client centralized deployment. Here, the WirelessController is responsible for providing the monitoring data for WirelessAccessPoint and WirelssClient.

  Note In IP, the WirelessController SNMP Agent is used to poll the status of the WirelessAccessPoint and WirelessClient.

- **Thin Client Distributed Deployment** as listed in Root-cause analysis for thin client distributed deployment. Here, the WirelessController is responsible for providing the monitoring data for WirelessAccessPoint and WirelssClient, for multiple distributed network.
- **Thick Client Autonomous Deployment** as listed in Root-cause analysis for thick client autonomous deployment. In an autonomous deployment, the WirelessAccessPoint provides the monitoring data for WirelssClient.

  Note In IP, the WirelessAccessPoint SNMP Agent is used to poll the status of the WirelessClient.

  Root-cause analysis of a wireless LAN Thin client centralized deployment lists the root-cause analysis done for thin client centralized deployment.

Table 9-54. Root-cause analysis of a wireless LAN Thin client centralized deployment

Class	Root-cause	Events (symptoms of root-cause)	Impacted system
WirelessController	Down	WirelessController Unresponsive WirelessController MightBeDown.	WirelessAccessPoint WirelessClient
WirelessAccessPoint		Down This event is generated when: The SNMP status of the WirelessAccessPoint is DOWN or NOTPRESENT, and The WirelessController is responsive	WirelessClient
WirelessClient		Disconnected This event is generated when: The WirelessClient is enabled for monitoring, and Host WirelessAccessPoint is responsive	None

Root-cause analysis for thin client distributed deployment lists the root-cause analysis done for a thin client distributed deployment.

Table 9-55. Root-cause analysis for thin client distributed deployment

Class	Root-cause	Events (symptoms of root-cause)	Impacted classes
Switch	Down	WirelessAccessPoint Unresponsive WirelessAccessPoint MIghtBeDown	WirelessAccessPoint WirelessClient
WirelessController	Down	WirelessController Unresponsive WirelessController MIghtBeDown	WirelessAccessPoint WirelessClient
WirelessAccessPoint		Down. This event is generated when: The SNMP status of the WirelessAccessPoint is DOWN or NOTPRESENT, and The WirelessController is responsive	WirelessClient
WirelessClient		Disconnected This event is generated when: The WirelessClient is enabled for monitoring, and Host WirelessAccessPoint is responsive	None

Root-cause analysis for thick client autonomous deployment lists the root-cause analysis done for a thick client automous deployment.

Table 9-56. Root-cause analysis for thick client autonomous deployment

Class	Root-cause	Events (symptoms of root-cause)	Impacted classes
WirelessController	Down	WirelessController Unresponsive WirelessController MIghtBeDown	WirelessAccessPoint WirelessClient
WirelessAccessPoint		Down. This event is generated when: ■ The SNMP status of the WirelessAccessPoint is DOWN or NOTPRESENT, and ■ The WirelessController is responsive	WirelessClient
WirelessClient		Disconnected This event is generated when: ■ The WirelessClient is enabled for monitoring, and ■ Host WirelessAccessPoint is responsive	None

Device connection

A device connection is a link between two network adapters. *Network adapter* provides information about network adapters. IP Availability Managerperforms 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 NetworkConnection 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

Attributes for Device connection 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 9-57. 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
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

Table 9-57. Attributes for Device connection (Continued)

Attribute	Description	Allowed values
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, 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
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

Table 9-57. Attributes for Device connection (Continued)

Attribute	Description	Allowed values
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, 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 enabled for this device connection.)	Boolean: TRUE, FALSE
IsNetworkAdapterNotOperating	TRUE if at least one of the two network adapters connected through this device connection is operationally down or flapping. (FALSE if neither network adapter is operationally down or flapping.)	Boolean: TRUE, FALSE
IsNetworkAdapterFlapping	TRUE if at least one of the two network adapters connected through this device connection is flapping. (FALSE if neither network adapter is flapping.)	Boolean: TRUE, 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 9-57. 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, FALSE

Table 9-57. Attributes for Device connection (Continued)

Attribute	Description	Allowed values
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
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, by 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 NetworkConnection 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 by using the setting described in the VMware Smart Assurance IP Management Suite Configuration Guide. The flapping condition can be diagnosed for network adapters and 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 and IP Performance Manager performs performance analysis on the following service access point object types:

- IP
- IPv6
- HSRPEndpoint
- VRRPEndpoint

- EVCEndPoints

IP

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

With the IP tagging feature, create an IP tag filter for each group of systems that is using an overlapping address space. Included in each filter is a user-specified tag value and a range of overlapping IP addresses. The VMware Smart Assurance IP Management Suite Configuration Guide provides more information on IP tagging feature.

Attributes for IP

Attributes for IP endpoint lists some key attributes for IP endpoint.

Table 9-58. 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 [vmwarewlan.corp.vmware.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
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-vmwarewlan.corp.vmware.com/46 [ge-1/2/0.511] [1.1.1.1]	String

Table 9-58. Attributes for IP endpoint (Continued)

Attribute	Description	Allowed values
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 **Note** The configuration file InterfaceType.conf has the exhaustive list of allowed values. The configuration file is located at:BASEDIR/smarts/conf/discovery
RoundTripTime	Reflects the latency (in ms) observed during the last poll by the instrumentation. IP objects are typically instrumented using the ICMP (ping) protocol.	Integer
MaximumLatency	A non-zero value that sets the time (in ms) for ICMP request/response pair. If any pair takes longer than that (but does not time out), it will generate the IP::SlowResponseTime event.	Integer

Table 9-58. 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, FALSE
Name	Name, as known in the modeled topology, of this IP endpoint; for example: IP-1.1.1.1	String
Netmask	Network mask for this IP endpoint; for example: 255.255.255.252	String

Table 9-58. Attributes for IP endpoint (Continued)

Attribute	Description	Allowed values
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, 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.vmware.com	String
SystemType	Type of system hosting this IP endpoint; for example: OTHER	Enum: ■ HOST ■ ROUTER ■ SWITCH ■ HUB ■ SERVER ■ BRIDGE ■ REPEATER ■ PROBE ■ OTHER ■ TERMINALSERVER ■ MEDIAGATEWAY

Root-cause problems for IP

No root-cause problems are diagnosed for IP endpoint.

Events for IP

Events for IP endpoint lists the events detected for IP endpoint. The Duplicate event is exported to the Global Manager.

Table 9-59. 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.
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.
DuplicateIP	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. The VMware Smart Assurance 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

Attributes for IPv6 endpoint lists some key attributes for IPv6 endpoint.

Table 9-60. 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 9-60. 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 **Note** The configuration file InterfaceType.conf has the exhaustive list of allowed values. The configuration file is located at:BASEDIR/smarts/conf/discovery

Table 9-60. 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 ICMPv6 (ping) protocol. ■ OK indicates that the IP interface is responding to ICMPv6 pings. ■ NETUNREACHABLE indicates that the IP network is unreachable. ■ HOSTUNREACHABLE indicates that the host is unreachable. ■ PROTOCOLUNREACHABLE indicates that the ICMPv6 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 ICMPv6 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, FALSE
IsInterfaceInstrumented	TRUE if "IP LayeredOver Interface" is instrumented.	Boolean: TRUE, FALSE
Name	Name, as known in the modeled topology, of this IPv6 endpoint; for example: IPv6-3FFE:80C0:22C:61:0:0:A09:FE03	String

Table 9-60. Attributes for IPv6 endpoint (Continued)

Attribute	Description	Allowed values
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 ICMPv6 pings. (FALSE if this IPv6 endpoint is not responding to ICMPv6 pings.)	Boolean: TRUE, 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 ■ HUB ■ SERVER ■ BRIDGE ■ REPEATER ■ PROBE ■ OTHER ■ TERMINALSERVER ■ MEDIAGATEWAY
IPv6DiscoveryEnabled	TRUE if IPv6 discovery is enabled. FALSE if IPv6 discovery is not enables.	Boolean: TRUE, FALSE

Root-cause problems for IPv6

No root-cause problems are diagnosed for IPv6 endpoint.

Events for IPv6

Events for IPv6 endpoint 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 9-61. Events for IPv6 endpoint

Event	Description
Down	Down indicates that an IPv6 endpoint is not responding to ICMPv6 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.
Unresponsive	Unresponsive indicates that an IPv6 endpoint is not responding to ICMPv6 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. The VMware Smart Assurance IP Management Suite Discovery Guide provides information about correcting Duplicate notifications.

HSRPEndpoint

An endpoint that describes the Hot Standby Router Protocol (HSRP) characteristics of an HSRP-capable interface. An HSRPEndpoint is a logical object defined for each HSRP interface of an HSRPGroup on the hosting router.

Attributes for HSRPEndpoint

Attributes for HSRPEndpoint lists some key attributes for HSRPEndpoint.

Table 9-62. 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.vmware.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
HsrpEpStateChanged	The status of the HSRP endpoint has changed since the last polling.	Boolean: TRUE, FALSE

Table 9-62. 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.vmware.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, FALSE
IsSwitchOverActive	TRUE if this HSRPEndpoint has switched over to the active state.	Boolean: TRUE, FALSE
Name	Name, as known in the modeled topology, of this HSRPEndpoint; for example: HSRP-wpl01-07m01-gw01.isus.vmware.com/16-16	String
Priority	Priority defined for this HSRPEndpoint in the HSRP group; for example: 110	Integer

Table 9-62. Attributes for HSRPEndpoint (Continued)

Attribute	Description	Allowed values
Responsive	TRUE if this HSRPEndpoint is responding to ICMP and ICMPv6 pings. (FALSE if this HSRPEndpoint is not responding to ICMP and ICMPv6 pings.)	Boolean: TRUE, FALSE
ServiceName	Name of external server used for imported events and instrumented attributes.	String
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
SystemName	Name of the system hosting this HSRPEndpoint; for example: wpl01-07m01-gw01.isus.vmware.com	String

Table 9-62. Attributes for HSRPEndpoint (Continued)

Attribute	Description	Allowed values
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.

Event 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.

Note Separate alerts are generated for HSRPGroups. Event for HSRPEndpoint provides the list of events that are generated for HSRPGroups.

VRRPEndpoint

VRRPEndpoint is composed of a logical element defined per interface per VRRPGroup on a VRRP router. The VRRPGroup is created for each Virtual Router Identifier (VRID). VRRPEndpoints belonging to the same VRRPGroup (that is, having the same VRID) have a common Virtual IP and a Virtual MAC. The Virtual MAC is defined as xx-xx-xx-xx-xx-VRID. The VRRP enabled router having the highest priority is considered as the master router and all other routers are considered as backup routers.

Attributes for VRRPEndpoints

Attributes for VRRP Endpoints provides the key attributes for VRRPEndpoints.

Table 9-63. Attributes for VRRP Endpoints

Attributes	Description	Allowed Values
Display Name	Name, as shown in the Global Console, of this VRRPEndpoint; for example: VRRP-10.1.16.254 [Group 16] [IF-wpl01-07m01-gw01.isus.vmware.com/16]	String
GroupNumber	Number of the VRRPGroup to which this VRRPEndpoint belongs; for example: 16	String
VRRPEndpoint Key	Unique value that distinguishes this VRRPEndpoint from all other VRRPEndpoints; for example: 16.16	String

Table 9-63. Attributes for VRRP Endpoints (Continued)

Attributes	Description	Allowed Values
VrrpEpStateChanged	The status of the VRRPEndpoint that has changed since the last polling.	Boolean: TRUE, FALSE
InterfaceAdminStatus	Reflects the current administrative status of the interface underlying this VRRPEndpoint. ■ 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 VRRPEndpoint; for example: IF-wpl01-07m01-gw01.isus.vmware.com/16 [Vl16] [10.1.16.247, ...] [Development Workstations]	String
InterfaceNumber	Number of the interface underlying the VRRPEndpoint. For example: 16.	Integer

Table 9-63. Attributes for VRRP Endpoints (Continued)

Attributes	Description	Allowed Values
InterfaceOperStatus	Reflects the current operational status of the interface underlying this VRRPEndpoint: ■ 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 VRRPEndpoint has been polled.	Boolean: TRUE, FALSE
IsSwitchOverActive	TRUE if this VRRPEndpoint has switched over to the active state.	Boolean: TRUE, FALSE
Name	Name, as known in the modeled topology, of this VRRPEndpoint; for example: VRRP-wpl01-07m01-gw01.isus.vmware.com/16-16	String
Responsive	TRUE if the current state as reported by the instrumentation is MASTER_VRRP. MASTER_VRRP indicates that the virtual router is forwarding packets for IP addresses that are associated with it.	Boolean: TRUE, FALSE

Table 9-63. Attributes for VRRP Endpoints (Continued)

Attributes	Description	Allowed Values
State	Reflects the current state of this VRRPEndpoint as reported by the instrumentation: ■ UNKNOWN_VRRP indicates that the VRRP state was not polled. ■ INITIALIZE_VRRP indicates that all the virtual routers are waiting for a startup event. ■ BACKUP_VRRP indicates that the virtual router is monitoring the availability of the master router. ■ MASTER_VRRP indicates that the virtual router is forwarding packets for IP addresses that are associated with it. ■ ERROR_VRRP indicates that an error was encountered during polling.	Enum: ■ UNKNOWN_VRRP ■ INITIALIZE_VRRP ■ BACKUP_VRRP ■ MASTER_VRRP ■ ERROR_VRRP
OperState	Indicates whether the VRRP state of this VRRPEndpoint has changed: ■ 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 VRRPEndpoint.	Enum: ■ RESPONSIVE ■ UNRESPONSIVE ■ UNKNOWN
SystemName	Name of the system hosting this VRRPEndpoint; for example: wpl01-07m01-gw01.isus.vmware.com	String
VirtualIP	Primary virtual IP address used by the VRRPGroup to which this VRRPEndpoint belongs. For example: 10.1.16.236 **Note** Virtual IP of VRRP is derived from vrrpAssoIpAddr, which is part of Indexes in vrrpAssoIpAddrTable. If the vrrpAssoIpAddrTable is not displayed in the MIB, then VRRPGroup will not be created.	String

Table 9-63. Attributes for VRRP Endpoints (Continued)

Attributes	Description	Allowed Values
VirtualMAC	Primary virtual MAC address used by the VRRPGroup to which this VRRPEndpoint belongs. The Virtual MAC is defined as xx-xx-xx-xx-xx-VRID.	String
VirtualRouterID	The Virtual Router Identifier (VRID) is the number that identifies the virtual router.	String

Root-cause problem for VRRPEndpoints

No root-cause problems are diagnosed for VRRPEndpoint.

Event for VRRPEndpoints

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

- SwitchOver: When a failure occurs or maintenance is required in an active router, a standby router must become active.

Note Separate events are generated for VRRPGroups. Event for VRRPEndpoints provides the list of events that are generated for VRRPGroups.

Logical link

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

- IPNetwork— A logical link that allows any two IPv4 addresses that are “ConnectedVia” the IPv4Network to communicate with one another.
- IPv6 Network — 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.

IPNetwork

A logical link that allows any two IPv4 addresses that are “ConnectedVia” the IPv4Network to communicate with one another.

Attributes for IPNetwork

Attributes for IPNetwork lists the attributes for IPNetwork.

Table 9-64. Attributes for IPNetwork

Attribute	Description	Allowed values
CIM_CreationClassName	CreationClassName attribute defined in CIM model.	String
CIM_Description	The Description property provides a textual description of the object.	String
CIM_Name	Name attribute defined in CIM model. It defines the label by which the object is known. When subclassed, the Name property can be overridden to be a Key property.	String
ConnectedSystemsUnresponsive		Boolean
CreationClassName	The name of the most-derived class of this instance.	String
Description	A textual description of the object.	String
DisplayClassName	The string shown in the GUI when this object's class is displayed.	String
DisplayName	The string shown in the GUI when this object's name is displayed.	String
IsManaged	The IsManaged attribute determines if an ICIM_ManagedSystemElement should be monitored by the management system. An unmanaged object will never have associated instrumentation. This attribute is readonly.	Boolean
IsShadow	TRUE, if this is a shadow IP object created to support backwards compatibility with the satellite servers of Availability Manager, when IP is tagged.	Boolean
KEYS	Types and Names of key attributes defined in CIM model.	String
MaximumNetworkSizeForCorrelation	The maximum number of systems that participate in this IPNetwork before stopping the exchange of MightBeDown symptoms.	Integer
Name	Name of the object.	String
Netmask	The IP network mask.	String
NetworkNumber	The IP network number.	String
ServiceName	Name of external server used for imported events and instrumented attributes.	String
SystemName	The scoping AdminDomain's Name.	String
Tag	The Tag configured by the user for this IPNetwork. Typically, all the IPs in one IPNetwork share the same tag.	String

Exceptions for IPNetwork

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

IPv6Network

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

Attributes for IPv6Network

Attributes for IPv6Network lists some key attributes for IPv6Network.

Table 9-65. Attributes for IPv6Network

Attribute	Description	Allowed values
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

Attributes for VLAN lists some key attributes for VLAN.

Table 9-66. 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 the VMware Smart Assurance IP Management Suite Configuration Guide.	Boolean: TRUE, 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
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 by Availability manager

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

Exceptions for VLAN by Performance manager

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

VLAN PerformanceException

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

Network adapter faults that result in a VLAN PerformanceException are described in Network adapter.

VLAN ErrorException

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

The network adapter fault (HighErrorRate) that results in a VLAN ErrorException is described in Network adapter.

OperationalException

Indicates that one or more operational faults exist on the ports/interfaces or cards that belong to members of the VLAN.

ConnectivityException

Indicates that one or more connectivity related faults exist for the ports/interfaces, cards, or switches that are members of the VLAN.

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.

However, some devices along the path 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. The VMware Smart Assurance IP Management Suite Configuration Guide provides more information about naming partitions.

Attributes for Partition

Attributes for Partition lists some key attributes for Partition.

Table 9-67. 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 problem for Partition

The following root-cause problem is diagnosed for Partition:

Down: Indicates that all systems in a Partition are unresponsive. This 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.

Attributes for Management agent lists some key attributes for management agent.

Table 9-68. Attributes for Management agent

Attribute	Description	Allowed values
AgentAddress	IP address used by the initial ICMP or ICMPv6 poll to contact this management agent; for example: 10.9.1.108 or 3FFE:80C0:22C:92:0:0:0:1	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
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 and ICMPv6 pings or SNMP polls. (FALSE if the host system is responding to ICMP and ICMPv6 pings and/or SNMP polls.)	Boolean: TRUE, 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

Table 9-68. Attributes for Management agent (Continued)

Attribute	Description	Allowed values
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, 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
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 and ICMPv6 pings. ■ UNREACHABLE indicates that the host system is not responding to ICMP and ICMPv6 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

Table 9-68. Attributes for Management agent (Continued)

Attribute	Description	Allowed values
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. **Note** 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, 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
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[]

Table 9-68. Attributes for Management agent (Continued)

Attribute	Description	Allowed values
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 and ICMPv6 pings. Typically, this situation is caused by the use of an incorrect community string (SNMPv1 or v2c), or the agent might be hung.

Note By default, the SNMP Agent NotResponding is generated after three polling cycles. It is not generated after one unsuccessful poll to avoid false alerts.

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

Events for Management agent

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

Table 9-69. 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 and ICMPv6 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. The VMware Smart Assurance IP Management Suite Configuration Guide provides information about these parameters.

Redundancy groups

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.
- VRRPGroup — Consists of two or more VRRP enabled routers. The VRRPGroup is created for each Virtual Router Identifier (VRID) and is composed of a logical element defined per interface per VRRPGroup on a VRRP router called VRRPEndpoint. VRRPEndpoints belonging to the same VRRPGroup (that is, having the same VRID) have a common virtual IP and a Virtual MAC. The Virtual MAC is defined as xx-xx-xx-xx-xx-VRID.

Attributes for redundancy groups

Attributes for redundancy groups lists some key attributes for CardRedundancyGroup, NetworkAdapterRedundancyGroup, NetworkConnectionRedundancyGroup, and SystemRedundancyGroup.

Table 9-70. Attributes for redundancy groups

Attribute	Description	Allowed values
AtRiskThreshold	Indicates the lower bound for number of redundancy group elements that must have normal status before a notification is generated. When the number of elements with a normal status falls below this threshold, an AtRisk notification is generated. By default, AtRiskThreshold is set to 1.	Integer
CIM_CreationClassName	CreationClassName attribute defined in CIM model.	String
CIM_Description	Displays a textual description of the objects.	String
CIM_Name	Displays the name by which the object is known. When subclassed, the Name property can be overridden by Key property.	String
CreationClassName	The name of the most-derived class of this instance.	String
Description	A textual description of the object.	String
DisplayClassName	The string shown in the GUI when this object's class is displayed.	String

Table 9-70. Attributes for redundancy groups (Continued)

Attribute	Description	Allowed values
DisplayName	The string shown in the GUI when this object's name is displayed.	String
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, FALSE
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, FALSE
IsGroupPartOfSingle-UnresponsiveSystem	TRUE - Indicates that the group is part of a single unresponsive system.	Boolean: TRUE, FALSE
IsManaged	The IsManaged attribute determines if an ICIM_ManagedSystemElement should be monitored by the management system. An unmanaged object will never have associated instrumentation. This attribute is readonly.	Boolean: TRUE, FALSE
KEYS	Types and names of key attributes defined in CIM model.	String
Name	Name of the object.	String
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
ServiceName	The name of external server used for imported events and instrumented attributes.	String
SystemName	The name of the ICIM_System containing this element.	String

Root-cause problems for redundancy groups

No root-cause problems are diagnosed for redundancy groups.

Events for redundancy groups

Events for redundancy groups lists the events detected for CardRedundancyGroup, NetworkAdapterRedundancyGroup, NetworkConnectionRedundancyGroup, and SystemRedundancyGroup. These events are exported to the Global Manager. None of the events are used as symptoms for root-cause analysis.

Table 9-71. Events for redundancy groups

Event	Description
AllComponentsDown	None of the member objects in the redundancy group are operational.
AtRisk	The number of 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 operational members is zero, an AllComponentsDown event occurs. For example, and assuming AtRiskThreshold = 1, the state of a three-member redundancy group having one operational member (and two non operational members) is AtRisk.
ReducedRedundancy	The number of 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 operational members (and one non operational member) is ReducedRedundancy.

As shown in Events for redundancy groups, 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

Attributes for HSRPGroup lists some key attributes for HSRPGroup.

Table 9-72. 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, 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, FALSE

Table 9-72. Attributes for HSRPGroup (Continued)

Attribute	Description	Allowed values
IsAnyHSRPEndpointActive	TRUE if at least one HSRPEndpoint in this HSRPGroup is active. (FALSE if no HSRPEndpoint in this HSRPGroup is active.)	Boolean: TRUE, 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, FALSE
IsEveryHSRPEndpointReady	TRUE if all HSRPEndpoints in this HSRPGroup have been polled.	Boolean: TRUE, FALSE
IsGroupPartOfSingle-UnresponsiveSystem	TRUE if all HSRPEndpoints in this HSRPGroup are part of a single, unresponsive system.	Boolean: TRUE, FALSE
IsVirtualIPUnresponsive		Boolean: TRUE, 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
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.
- AllComponentsDown: Indicates that all the components in the HSRPGroup are down.
- AtRisk: Indicates that the number of functioning components <= AtRisk threshold.

- ReducedRedundancy: Indicates that at least one component is not functioning but the total number of components > AtRisk threshold.

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

  The SwitchOver event is subscribed to by the Global Manager.

Attributes for VRRPGroup

Attributes for VRRPGroup lists the key attributes for VRRPGroup.

Table 9-73. Attributes for VRRPGroup

Attributes	Description	Allowed values
AtRiskThreshold	Set to a value representing the number of responsive or operational member VRRPEndpoints in this VRRPGroup. By default, AtRiskThreshold is set to 1.	String
DisplayName	Name, as shown in the Global Console, of this VRRPGroup; for example: VRRPGroup-10.1.16.254 [Group 16]	String
GroupNumber	Number assigned to this VRRPGroup; for example: 16	String
VrrpEpStateChanged	TRUE if one or more member VRRPEndpoints in this VRRPGroup are not operational. (FALSE if all member HSRPEndpoints in this VRRPGroup are operational.)	Boolean: TRUE, FALSE
IsAnyComponentDown	TRUE if at least one member VRRPEndpoint in this VRRPGroup is not operational. (FALSE if all member VRRPEndpoints in this VRRPGroup are operational.)	Boolean: TRUE, FALSE
IsAnyVRRPEndpointActive	TRUE if at least one VRRPEndpoint in this VRRPGroup is active. (FALSE if no VRRPEndpoint in this VRRPGroup is active.)	Boolean: TRUE, FALSE
IsEveryComponentDown	TRUE if all member VRRPEndpoints in this VRRPGroup are unresponsive or non-operational. (FALSE if at least one member VRRPEndpoint in this VRRPGroup is responsive or operational.)	Boolean: TRUE, FALSE
IsEveryVRRPEndpointReady	TRUE if all VRRPEndpoints in this VRRPGroup have been polled.	Boolean: TRUE, FALSE
IsGroupPartOfSingle-UnresponsiveSystem	TRUE if all VRRPEndpoints in this VRRPGroup are part of a single, unresponsive system.	Boolean: TRUE, FALSE
Name	Name, as known in the modeled topology, of this VRRPGroup; for example: VRRP-GROUP-10.1.16.254	String
NumberOfComponents	Number of member VRRPEndpoints in this VRRPGroup; for example: 2	Integer
NumberOfFaultyComponents	Number of member VRRPEndpoints in this VRRPGroup that are unresponsive or non-operational; for example: 0	Integer

Table 9-73. Attributes for VRRPGroup (Continued)

Attributes	Description	Allowed values
VirtualIP	Primary virtual IP address used by this VRRPGroup. For example: 10.1.16.254	String
VirtualMAC	Primary virtual MAC address used by this VRRPGroup.	String
VirtualRouterID	The Virtual Router Identifier (VRID) is the number that identifies the virtual router.	String

Root-cause problem for VRRPGroup

No root-cause problems are diagnosed for VRRPGroup.

Events for VRRPGroups

The following events are detected for VRRPGroup and exported to the Global Manager:

- SwitchOverFailed: Indicates that traffic fails to switch from an active interface to a standby interface in a VRRPGroup and that all interfaces in the VRRPGroup are inactive.
- AllComponentsDown: Indicates that all the components in the VRRPGroup are down.
- AtRisk: Indicates that the number of functioning components <= AtRisk threshold.
- ReducedRedundancy: Indicates that at least one component is not functioning, but the total number of components > AtRisk threshold.

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

  The SwitchOver event is subscribed to by the Global Manager.

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.

Processor

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

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

Attributes for Processor

Attributes for Processor lists some key attributes for Processor.

Table 9-74. Attributes for Processor

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

Faults for Processor

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

A HighUtilization fault indicates that the processor utilization exceeds the ProcessorUtilizationThreshold. The threshold for processor utilization is contained in the Processor and Memory setting. The VMware Smart Assurance IP Management Suite Configuration Guide provides more information.

Memory

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

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

Attributes for Memory

Attributes for Memory lists some key attributes for Memory.

Table 9-75. Attributes for Memory

Attribute	Description	Allowed values
BufferMissPct	Number of buffer misses for this Memory, expressed as a percentage of the total number of buffer requests; for example: 0.0	Numeric (float)
BufferUtilizationPct	Number of buffers used for this Memory, expressed as a percentage of the total number of buffers; for example: 0.0	Numeric (float)

Table 9-75. Attributes for Memory (Continued)

Attribute	Description	Allowed values
DeviceID	Address or other identifying information to uniquely name this Memory; for example: 3	String
DisplayName	Name, as shown in the Global Console, of this Memory; for example: MEM-10.9.1.108/3 [Virtual Memory]	String
FreeMemory	Amount of free memory in kilobytes available for this Memory; for example: 185024	Integer
FreeMemoryPct	The percentage of free memory of the total memory.	Numeric (float)
LargestFreeBuffer	Largest number of contiguous kilobytes that are currently unused for this Memory; for example: 93656	Integer
Name	Name, as known in the modeled topology, of this Memory; for example: MEM-10.9.1.108/3	String
SystemName	Name of the system containing this Memory; for example: 10.9.1.108	String
TotalBufferAllocationFailures	Number of buffer allocation failures due to lack of memory experienced in the last polling cycle for this Memory; for example: 0	Integer
TotalMemory	Amount of memory present in this Memory as reported by the instrumentation; for example: 2521984	Integer

Faults for Memory

Faults and related thresholds for Memory lists the faults detected for Memory.

Table 9-76. Faults and related thresholds for Memory

Memory Fault	Description	Threshold
ExcessiveFragmentation	Indicates that the system memory is highly fragmented and exceeds the Memory Fragmentation Threshold.	MemoryFragmentationThreshold
HighBufferMissRate	Indicates that the rate of buffer misses exceeds the Memory Buffer Miss Threshold. Drill down on this event notification in the Notification Log to view the percentage breakdown of buffer misses into the types of misses (such as small, medium, big, large, and huge buffer misses).	MemoryBufferMissThreshold

Table 9-76. Faults and related thresholds for Memory (Continued)

Memory Fault	Description	Threshold
HighBufferUtilization	Indicates that the number of buffers used exceeds the Memory Buffer Utilization Threshold. Drill down on this event notification in the Notification Log to view the percentage of small, medium, big, large, and huge buffers used.	MemoryBufferUtilizationThreshold
InsufficientFreeMemory	Indicates that the system is running out of memory resources and that the percentage of free memory falls below the Free Memory Threshold. This fault is also reported if there has been a failure to allocate a buffer due to lack of memory.	FreeMemoryThreshold

When a memory-related fault occurs, IP Performance Manager generates a system ResourceException for the affected system. The thresholds for memory faults are listed in the Processor and Memory setting. The VMware Smart Assurance IP Management Suite Configuration Guide provides more information.

Disk

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

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

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

Attributes for Disk

Attributes for Disk lists some key attributes for Disk.

Table 9-77. Attributes for Disk

Attribute	Description	Allowed values
Access	Indicates whether this Disk is readable and writable or only readable. ■ readWrite indicates that this Disk can be read and written. ■ readOnly indicates that this Disk can be read but not written.	Enum: ■ readOnly ■ readWrite
Capacity	Size in kilobytes for this Disk; for example: 3395069 If the media is removable and is currently removed, this value should be 0.	Integer
DeviceID	Address or other identifying information to uniquely name this Disk; for example: 5	String

Table 9-77. Attributes for Disk (Continued)

Attribute	Description	Allowed values
DisplayName	Name, as shown in the Global Console, of this Disk; for example: DISK-10.9.1.108/5 [Fixed Disk]	String
Media	Indication of the type of media used in this Disk. ■ other indicates that the media used in this Disk is of type other. ■ unknown_media indicates that the media type used in this Disk is not known. ■ hardDisk indicates that the media used in this Disk is a hard disk. ■ floppyDisk indicates that the media used in this Disk is a floppy disk. ■ opticalDiskrom indicates that the media used in this Disk is an optical disk ROM. ■ opticalDiskworm indicates that the media used in this Disk is an optical disk WORM. ■ opticalDiskrw indicates that the media used in this Disk is an optical disk RW. ■ ramDisk indicates that the media used in this Disk is a RAM disk.	Enum: ■ other ■ unknown_media ■ hardDisk ■ floppyDisk ■ opticalDiskrom ■ opticalDiskworm ■ opticalDiskrw ■ ramDisk
Name	Name, as known in the modeled topology, of this Disk; for example: DISK-10.9.1.108/5	String
Removable	TRUE if this Disk can be removed; for example, a floppy disk. (FALSE if this Disk cannot be removed; for example, a hard disk.)	Boolean: TRUE, FALSE
Status	Current status of this Disk as reported by the instrumentation.	Enum: ■ running
SystemName	Name of the system containing this Disk; for example: 10.9.1.108	String

Faults for Disk

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

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

File System

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

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

Attributes for File System

Attributes of File System lists some key attributes for File System.

Table 9-78. Attributes of File System

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

Celerra file system types

Celerra is a high performance IP storage platform. It delivers NAS (Network Attached Storage) and iSCSI capabilities to consolidate application storage and file servers in either an integrated configuration, or as a gateway connected to a CLARiiON or Symmetrix storage system.

Celerra allows file system access through NFS, CIFS and ISCSI protocols. The Celerra Server creates different file systems, as listed in Celerra File System types , depending on how they are used.

Table 9-79. Celerra File System types

File system	ID	Description
uxfs	1	Default file system
sfs		Shared file system
rawfs	5	Raw file system
mirrorfs	6	Mirrored file systems
ckpt	7	Checkpoint file system
mgfs	8	Migration file system
group	100	Stores members of a file system group
vpfs		Volume pool file system (multiple services sharing a single metavolume)
rvfs		Local configuration volume used to store replication specific internal information
nmfs	102	Nested mount file system

Faults for File System

IP Server Performance Manager detects the HighUtilization fault and LowAvailableSpace for File System. When a HighUtilization fault occurs, IP Server Performance Manager generates a system ResourceException for the affected host system.

A HighUtilization fault indicates that the File System utilization exceeds the MaxUtilizationPct threshold.

PowerSupply

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

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

Attributes for PowerSupply

Attributes for PowerSupply lists some key attributes for PowerSupply.

Table 9-80. Attributes for PowerSupply

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

Faults for PowerSupply

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

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

- NORMAL
- WARNING
- CRITICAL
- SHUTDOWN

VoltageSensor

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

Attributes for VoltageSensor

Attributes for VoltageSensor lists some key attributes for VoltageSensor.

Table 9-81. Attributes for VoltageSensor

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

Table 9-81. Attributes for VoltageSensor (Continued)

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

Faults for VoltageSensor

Faults and related thresholds for VoltageSensor lists the faults detected for VoltageSensor.

Table 9-82. Faults and related thresholds for VoltageSensor

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

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

TemperatureSensor

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

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

Attributes for TemperatureSensor

Attributes for TemperatureSensor lists some key attributes for TemperatureSensor.

Table 9-83. Attributes for TemperatureSensor

Attribute	Description	Allowed values
CurrentValue	Current value in degrees centigrade (C) of this TemperatureSensor as reported by the instrumentation; for example: 45 C	Integer
DeviceID	Address or other identifying information to uniquely name this TemperatureSensor; for example: 1	String
DisplayName	Name, as shown in the Global Console, of this TemperatureSensor; for example: TEMP-10.9.252.2/1 [Chassis Temperature Sensor]	String
HighThreshold	Current high threshold value in degrees C of this TemperatureSensor as reported by the instrumentation; for example: 85.5 C	Numeric (float)
Name	Name, as known in the modeled topology, of this TemperatureSensor; for example: TEMP-10.9.252.2/1	String
Status	Current state of this TemperatureSensor as reported by the instrumentation. ■ OK indicates that the observed temperature is acceptable. ■ WARNING indicates that the observed temperature is unacceptable but that the operation of the system can continue. ■ CRITICAL indicates that the observed temperature is unacceptable and that operation of the system might cease as a result. ■ SHUTDOWN indicates that the fan or Chassis has been shut down or that this TemperatureSensor has been shut down. ■ OTHER indicates that the state of this TemperatureSensor is not OK, WARNING, CRITICAL, or SHUTDOWN. ■ UNKNOWN indicates that this TemperatureSensor has yet to be polled. ■ MARGINAL indicates that the observed temperature is unacceptable, but that the operation of the system can continue.	Enum: ■ OK ■ WARNING ■ CRITICAL ■ SHUTDOWN ■ OTHER ■ UNKNOWN ■ MARGINAL
SystemName	Name of the system containing this TemperatureSensor; for example: qa-gw3.smarts.com	String

Faults for TemperatureSensor

Faults and related thresholds for TemperatureSensor lists the faults detected for TemperatureSensor.

Table 9-84. Faults and related thresholds for TemperatureSensor

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

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

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

Fan

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

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

Attributes for Fan

Attributes for Fan lists some key attributes for Fan.

Table 9-85. Attributes for Fan

Attribute	Description	Allowed values
DeviceID	Address or other identifying information to uniquely name this Fan; for example: 1	String
DisplayName	Name, as shown in the Global Console, of this Fan; for example: FAN-10.9.252.2/1 [Chassis Fan Tray 1]	String
Name	Name, as known in the modeled topology, of this Fan; for example: FAN-10.9.252.2/1	String

Table 9-85. Attributes for Fan (Continued)

Attribute	Description	Allowed values
Status	Current state of this Fan as reported by the instrumentation. ■ OK indicates that the fan is operating normally. ■ WARNING indicates that the fan is at warning status. ■ CRITICAL indicates that the fan is at critical status. ■ SHUTDOWN indicates that the fan has been shut down. ■ OTHER indicates that the state of the fan is not OK, WARNING, CRITICAL, or SHUTDOWN. ■ UNKNOWN indicates that the fan has yet to be polled.	Enum: ■ OK ■ WARNING ■ CRITICAL ■ SHUTDOWN ■ OTHER ■ UNKNOWN
SystemName	Name of the system containing this Fan; for example: 10.9.252.2	String

Faults for Fan

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

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

DuplicateIP

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

Attributes for DuplicateIP

Attributes for DuplicateIP lists some key attributes for DuplicateIP.

Table 9-86. Attributes for DuplicateIP

Attribute	Description	Allowed values
Address	IP address of this DuplicateIP; for example: 10.0.0.4	String
DisplayName	Name, as shown in the Global Console, of this DuplicateIP; for example: 10.0.0.4 [hagg-01-lo0-0.west.twtelecom.net]	String
DuplicatedBySystems	List of systems on which the IP address for this DuplicateIP is duplicated.; for example: hagg-01-lo0-0.west.twtelecom.net, cpe-66-66-65-1.rochester.res.rr.com,	String

Table 9-86. Attributes for DuplicateIP (Continued)

Attribute	Description	Allowed values
InterfaceAdminStatus	Reflects the current administrative status of the interface underlying this DuplicateIP. ■ UP indicates that the interface is administratively enabled. ■ DOWN indicates that the interface is administratively disabled. ■ TESTING indicates that the interface is in testing mode. ■ OTHER indicates that the interface is in an unknown state. ■ NOTPRESENT indicates that the MIB AdminStatus value for the interface is missing. ■ UNKNOWN indicates that the interface has yet to be polled. When the value of the interface's InterfaceAdminStatus is UP, the value of InterfaceOperStatus determines the state of the interface. Otherwise, the value of InterfaceAdminStatus determines the state of the interface.	Enum: ■ UP ■ DOWN ■ TESTING ■ OTHER ■ NOTPRESENT ■ UNKNOWN
InterfaceMode	Indicates the intended purpose of the interface underlying this DuplicateIP: normal, backup, or dial-on-demand.	Enum: ■ NORMAL ■ BACKUP ■ ONDEMAND
InterfaceName	Name, as shown in the Global Console, of the interface underlying this DuplicateIP; for example: IF-hagg-01-lo0-0.west.twtelecom.net/14 [fxp1.0] [10.0.0.4]	String
InterfaceOperStatus	Reflects the current operational status of the interface underlying this DuplicateIP. ■ UP indicates that the interface is operationally up. ■ DOWN indicates that the interface is operationally down. ■ TESTING indicates that the interface is in testing mode. ■ OTHER indicates that the interface is in an unknown state. ■ DORMANT indicates that the interface is waiting for an external action to occur before becoming active. ■ NOTPRESENT indicates that the MIB OperStatus value for the interface is missing. ■ UNKNOWN indicates that the interface has yet to be polled.	Enum: ■ UP ■ DOWN ■ TESTING ■ OTHER ■ DORMANT ■ NOTPRESENT ■ UNKNOWN

Table 9-86. Attributes for DuplicateIP (Continued)

Attribute	Description	Allowed values
InterfaceType	Type of interface underlying this DuplicateIP, distinguished according to the physical/link protocols immediately "below" the network layer in the protocol stack.	Enum: ATMFUNI ARCNET SONET HIPPI MODEM V36 IEEE1394 IFGSN ATMVIRTUAL **Note** The configuration file InterfaceType.conf has the exhaustive list of allowed values. The configuration file is located at:BASEDIR/smarts/conf/discovery

Table 9-86. Attributes for DuplicateIP (Continued)

Attribute	Description	Allowed values
IPStatus	Reflects the current state of this DuplicateIP as reported by the instrumentation. **Note** For a DuplicateIP, this attribute is set to UNKNOWN. ■ OK indicates that the IP interface is responding to ICMP pings. ■ NETUNREACHABLE indicates that the IP network is unreachable. ■ HOSTUNREACHABLE indicates that the host is unreachable. ■ PROTOCOLUNREACHABLE indicates that the ICMP protocol is unreachable. ■ PORTUNREACHABLE indicates that the port is unreachable. ■ NEEDFRAGUNREACHABLE indicates that the destination was unreachable because fragmentation was needed and do not fragment was set. ■ SRCFAILEDUNREACHABLE indicates that the source route failed. ■ DESTNETUNREACHABLE indicates that the destination network is unknown. ■ DESTHOSTUNREACHABLE indicates that the destination host is unknown. ■ ISOLATEDUNREACHABLE indicates that the source host is isolated. ■ AUTHNETUNREACHABLE indicates that communication with the destination network is administratively prohibited. ■ AUTHHOSTUNREACHABLE indicates that communication with the destination host is administratively prohibited. ■ NETSVCUNREACHABLE indicates that the destination network is unreachable for this type of service. ■ HOSTSVCUNREACHABLE indicates that the destination host is unreachable for this type of service. ■ TIMEXCEEDINTRANS indicates that the Time to Live (TTL) was exceeded in transit. ■ TIMEXCEEDREASS indicates that the fragment reassembly time was exceeded. ■ TIMEDOUT indicates that the last ICMP ping timed out. ■ OTHER indicates an unspecified error condition occurred. ■ UNKNOWN indicates an unspecified error condition occurred.	Enum: ■ OK ■ NETUNREACHABLE ■ HOSTUNREACHABLE ■ PROTOCOLUNREACHABLE ■ PORTUNREACHABLE ■ NEEDFRAGUNREACHABLE ■ SRCFAILEDUNREACHABLE ■ DESTNETUNREACHABLE ■ DESTHOSTUNREACHABLE ■ ISOLATEDUNREACHABLE ■ AUTHNETUNREACHABLE ■ AUTHHOSTUNREACHABLE ■ NETSVCUNREACHABLE ■ HOSTSVCUNREACHABLE ■ TIMEXCEEDINTRANS ■ TIMEXCEEDREASS ■ TIMEDOUT ■ OTHER ■ UNKNOWN
IsInterfaceInstrumented	TRUE if "IP LayeredOver Interface" is instrumented.	Boolean: TRUE, FALSE
Name	Name, as known in the modeled topology, of this DuplicateIP; for example: IP-10.0.0.4	String
Netmask	Network mask for this DuplicateIP; for example: 255.0.0.0	String

Table 9-86. Attributes for DuplicateIP (Continued)

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

Events for DuplicateIP

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

- Classifies the IP address as a DuplicateIP
- Suspends IP-related analysis for the address
- Generates a Duplicate notificationThe VMware Smart Assurance IP Management Suite Discovery Guide provides information about correcting Duplicate notifications.

NAS IP Elements

The Availability Manager builds a data model of the discovered NAS IP elements in the managed environment. The model represents the discovered elements as instances of the VMware Smart Assurance ICIM classes.

The NAS IP elements are represented by instances of the following ICIM classes:

- NASChassis
- FileServer

- Host (Celerra Control Station)

  During the discovery post-processing phase, the IP Manager creates the relationships and connections between the storage objects: Celerra Data Mover (FileServer object), NAS Network Server (NASChassis object), and Celerra Control Station (Host object).

  Note that, in addition, the Availability Manager discovers the Layer 2 and Layer 3 elements and relationships that are described in the VMware Smart Assurance IP Availability Manager User Guide; for example, Cable, Card, Interface.

  The VMware Smart Assurance IP Management Suite Discovery Guide provides more information about the VMware Smart Assurance ICIM classes and the discovery process.

NAS Chassis

A Chassis is a physical package that encloses other elements; in this case, the enclosed elements are the Celerra Data Movers and Control Station.

NASChassis is instantiated for each Celerra Network Server (NASChassis object) found during the discovery process.

The NASChassis is related to the FileServer and Host objects through the PackagesSystems relationship. The NASChassis is also related to remote Control Station Host objects through the ConnectedTo relationship. The ConnectedTo relationship reflects inter-Celerra device communication.

Events for NASChassis

Events for NASChassis lists the events detected for NASChassis.

Table 9-87. Events for NASChassis

Event	Description	Exported by IP Availability Manager
NASChassis Down	Indicates that a faulty Chassis is the root cause.	Yes

Attributes of NASChassis

Attributes of NASChassis lists the attributes of NASChassis.

Table 9-88. Attributes of NASChassis

Attributes	Descripition	Value
fsTable	A table holding entries to be added to the pending list	Struct
Tag	An arbitrary string that uniquely identifies the physical element and serves as the element's key. The Tag property can contain information such as an asset tag or serial number. The key for ICIM_PhysicalElement is placed very high in the object hierarchy in order to independently identify the hardware/entity, regardless of physical placement in or on cabinets, adapters, and so on. For example, a hot-swappable or removable component may be taken from its containing (scoping) package and be temporarily unused. The object still continues to exist and may even be inserted into a different scoping container. Therefore, the key for physical element is an arbitrary string and is defined independently of any placement or location-oriented hierarchy.	String

Attributes of NASManager

Table 9-89. Attributes of NASManager

Attributes	Description	Value
AddFsToPending	Determines whether the file server should be added to the pending list or discovered. The allowed values are: ■ TRUE — Adds the non-discovered FileServer to the pending list. ■ FALSE — Triggers discovery automatically for the newly found FileServer. Default value: TRUE **Note** Monitoring of FileSystem of FileServers and DataMovers are not supported. Only Discovery is supported.	Boolean: TRUE, FALSE
HttpsAdapterName	This is the name of the HTTPS java Adapter.	String
pdlTable	This is a table that holds entries to be added to the pending list	Struct

Attributes of NASManager lists the attributes of NASManager.

Host (Celerra Control Station)

A Host is a computer such as a workstation or server; in this case it represents the Celerra Control Station.

This class is used to instantiate the Celerra Control Station, which is the Celerra device management element. The Host class also exists in the Availability Manager.

A Host object is related to the NASChassis object through the PackagedIn relationship.

FileServer

A file server (Celerra Data Mover or NetApp Filer) is responsible for central storage and management of data files so that other computers can access the files. File server configurations can vary greatly, from a networked group of storage arrays that includes many disk drives to a virtual entity on a computer host. In a large Celerra network, however, a file server may be included in a Celerra Network Server that contains a Control Station, or it might be associated with a remote Control Station on the same IP network, or with a Control Station on a network not monitored by VMware Smart Assurance. There is no concept of Control Station with the NetApp Filer, which includes its own management software.

A FileServer object is related to the NASChassis object by the PackagedIn relationship, and to the IP network through the ConnectedVia relationship.

Attributes for FileServer

Attributes for FileServer lists key attributes for FileServer.

Table 9-90. Attributes for FileServer

Attribute	Description
InternalName	Unique name for this file server
InetAddr	IP address for accessing this file server
SoftwareVersion	Software version executing in this file server
Slot	Slot in the Chassis that packages this file server
Standby	Name of the file server backing up this file server

FibreChannelSwitchPort

The FibreChannelSwitchPort is created on the IP topology by probing the fcFxPortEntry MIB table during the discovery of fibre channel switches.

Table 88 on page 151 lists the attributes for FibreChannelSwitchPort. The MIB ObjectIDs listed in the table are used to probe the FibreChannelSwitchPort information.

Table 9-91. Attributes for FibreChannelSwitchPort

Attribute	Type	MIB ObjectID	Description
World Wide Name (WWN)	Octet String	fcFxPortName .1.3.6.1.2.1.75.1.1.5.1.2	World Wide Name Of the FibreChannelSwitchPort. This attribute is used as an identifier to establish a connection.
AdminStatus	Integer	fcFxPortPhysAdminStatus 1.3.6.1.2.1.75.1.2.2.1.1	This attribute provides the admininistration status of the FibreChannelSwitchPort. **Note** If the value of this attribute is offline, then IP does not create the class on the IP Topology.
OperStatus	Integer	fcFxPortPhysOperStatus 1.3.6.1.2.1.75.1.2.2.1.2	The current operational status of the FibreChannelSwitchPort which is used for event generation.

Note In case of the Cisco UCS FabricInterconnect switch, the relationship between Fabric Interconnect's card and the FibreChannelSwitchPort is not created due to insufficient data.

PortLink

The link between two FibreChannelSwitchPorts is called a PortLink. A PortLink is created by probing the fcFxPortEntry MIB table during the discovery on IP topology.

Connection between FibreChannelSwitchPorts

During the discovery, the MIB Object ID listed in MIB Object IDs of FibreChannelSwitchPort is probed to obtain the information on connection between the fibre channel switches. This information contains the WWN of the remote port which is connected to the local port of the local fibre channel switch.

Table 9-92. MIB Object IDs of FibreChannelSwitchPort

Attribute	Type	MIB ObjectID	Description
	Octet String	fcFxPortNxPortName 1.3.6.1.2.1.75.1.2.3.1.10	WWN of the attached corresponding Port

When the fibre channel switches are discovered, IP creates the FibreChannelSwitchPorts in the topology. Each FibreChannelSwitchPort is associated with a WWN. The WWN uniquely identifies the FibreChannelSwitchPort across the switches on the IP topology.

During post processing, IP uses the connection information to form the PortLink between the FibreChannelSwitchPorts.

Events for PortLink and FibreChannelSwitchPort

Events for PortLink and FibreChannelSwitchPort lists events for PortLink and FibreChannelSwitchPort.

Table 9-93. Events for PortLink and FibreChannelSwitchPort

Class	Event	Description
PortLink	Problem Down	Indicates FibreChannelSwitchPort DownOrFlapping
FibreChannelSwitchPort	DownOrFlapping	Indicates that FibreChannelSwitchPort's AdminStatus attribute is UP and the value of OperStatus is DOWN

External Polling Support for FibreChannelSwitchPort

The VMware Smart Assurance IP Manager User Guide provides information on how to enable external polling in the Polling and Thresholds tab.

SM_ElementManager

The SM_ElementManager class manages the life cycle of SM_SystemElement objects. It is a singleton class (the instance is SM_ElementManager::SM-ElementManager) and has attributes for configuring various aspects of the life cycle management. The key attributes for SM_ElementManager are listed in Key attributes for SM_ElementManager .

Table 9-94. Key attributes for SM_ElementManager

Attribute	Value	Description
FDLimit	Unsigned long integer This attribute is read-only.	Maximum number of file descriptors (socket numbers) that this application is allowed to use for client connections at any one time. For an application on a Solaris- or Linux-based host, the file-descriptor limit is imposed on the application by the OS *as long as that limit is 1024 or less*. If that limit is more than 1024, the foundation startup code sets the limit to 1024.
FDWarningHeadroom	Unsigned integer Default: 100	An integer in the following equation that determines when the number of file descriptors for this application increases to an unacceptable level: Number of file descriptors > FDLimit – FDWarningHeadroom For example, if FDLimit = 1024 and FDWarningHeadroom = 100, the number of file descriptors increases to an unacceptable level when that number is greater than 924.

Table 9-94. Key attributes for SM_ElementManager (Continued)

Attribute	Value	Description
ReapInterval	Unsigned long integer Default: 60 seconds	Interval, in seconds, between successive expiry scans of terminated client connections for this application. This attribute works in conjunction with two other attributes, ClientRetainTime and AbnormalClientRetainTime, to determine when an expiry scan deletes (reaps) the client objects and data for a terminated connection: ■ For any normally terminated connection, the expiry scan deletes the associated client objects and data when the time between the connection's termination timestamp and the current time exceeds the ClientRetainTime. ■ For any abnormally terminated connection, the expiry scan deletes the associated client objects and data when the time between the connection's termination timestamp and the current time exceeds the AbnormalClientRetainTime. The effective retain time for a normally terminated connectIon is 1/2 the ReapInterval plus the ClientRetainTime. The effective retain time for an abnormally terminated connectIon is 1/2 the ReapInterval plus the AbnormalClientRetainTime.
ClientRetainTime	Unsigned long integer Default: 60 seconds	The least amount of time, in seconds, between when a normally terminated connection ends and when the client objects and data that are associated with that connection are deleted from the repository.
AbnormalClientRetainTime	Unsigned long integer Default: 900 seconds(15 minutes)	The least amount of time, in seconds, between when an abnormally terminated connection ends and when the client objects and data that are associated with that connection are deleted from the repository.
RequestLogSize	Unsigned long integer Default: 25	Size of the request log for client connections for this application. By default, the 25 most recent requests and their responses are recorded. Setting RequestLogSize to 0 disables the collection of request information for client connections. Like the rest of the client data, the request information persists for a client connection until the associated SM_Client and its threads and queues are deleted.
LogClients	Boolean Default: TRUE	TRUE indicates that this application will log the client connects and disconnects in its log file.

Notifications for Network Objects

10

This chapter includes the following topics:

- Introduction
- Summary of root-cause problems, exceptions, and events
- Problems, events and Notification summary for IP Availability Manager
- Exception, Fault, Event, and Notification summary for IP Performance Manager

Introduction

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.

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

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), notifications (one event per notification), and IPv6Network exception notifications (one exception per notification) are displayed in the Global Console.

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

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

  The Global Manager imports all faults and events detected by IP Performance Manager. The fault notifications (one fault per notification) and the event notifications (one event per notification) are displayed in the Global Console.

Root cause problems summary

Root-cause problems diagnosed by IP Availability Manager 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 10-1. Root-cause problems diagnosed by IP Availability Manager

Managed object	Root cause	Condition	Events (displayed in Codebook Tab in the Global Console)
System	Down	None	System MightBeDown
			DownOrFlapping

Table 10-1. Root-cause problems diagnosed by IP Availability Manager (Continued)

Managed object	Root cause	Condition	Events (displayed in Codebook Tab in the Global Console)
	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	DownOrFlapping
			System MightBeDown (connected system)
	Unstable	When IsFlapping = TRUE	DownOrFlapping
			SystemMightBeDown
	Disabled	Port or interface is connected or is a physical interface with subinterfaces layered over it or is part of a NetworkAdapterRedundancyGroup	AdministrativelyDown
			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
Device connection	Down	Physical connection such as cable, serial, or point-to-point	NetworkAdapter Down
		IsLogicalConnectionDownEnabled = FALSE or IsLogicalConnection = FALSE	
	Unstable	Physical connection such as cable, serial, or point-to-point NetworkAdapterStatus= UNSTABLE	NetworkAdapterDown
		NetworkAdapterStatus= UNSTABLE IsLogicalConnectionDownEnabled = FALSE or IsLogicalConnection = FALSE	
Partition	Down	Is not a proxy	System Unresponsive (all systems are unresponsive)

Table 10-1. Root-cause problems diagnosed by IP Availability Manager (Continued)

Managed object	Root cause	Condition	Events (displayed in Codebook Tab in the Global Console)
		None	LayeredOver Partition Down
SNMPAgent	NotResponding	None	Management agent Unresponsive

Exceptions summary for IP Availability Manager

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

Table 10-2. 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)
	ResourceException	When there is a Memory, Processor or FileSystem Exception on the entities that has a ComposedOf/PartOf relationship with the system.
	PerformanceException	When there is a PerformanceException on the NetworkAdapters that has a ComposedOf/PartOf relationship with the system.
	OperationalException	When one or more operational related failures exist.
	ErrorException	When there is a Error Exception on the NetworkAdapters that has a ComposedOf/PartOf relationship with the system.
	PowerSupplyException	When one or more voltage or power supply faults exist for a particular system.
	TemperatureException	When one or more fan or temperature related faults exist for a particular system.
IPv6Network	Inaccessible	IPv6 Down (e)
IPNetwork	Inaccessible	Network Down

Table 10-2. Exceptions generated by IP Availability Manager (Continued)

Managed object	Exception	Cause (problem or event)
VLAN	ConnectivityException	System Down (p)
		Port Down (p)
		Port Unstable (p)
		Port Disabled (p)
	OperationalException	Port DownOrFlapping (e)
		Port BackupActivated (e)
		Port ExceededMaximumUptime (e)
	ErrorException	When there is an ErrorException on the NetworkAdapters that has a ComposedOf/PartOf relationship with VLAN.
	PerformanceException	When there is a PerformanceException on the NetworkAdapters that has a ComposedOf/PartOf relationship with VLAN.
Chassis	OperationalException	When there is one or more operaitonal related failures.
Physical Package	OperationalException	When the Card or its component is OperationallyDown.

Exceptions and faults summary for IP Performance Manager

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

Note Thresholds can be set in the Polling and Thresholds tab in Domain Manager Administration Console. The chapter "*Configuring Groups and Settings in the Polling and Thresholds Console*" in *VMware Smart Assurance IP Management Suite Version 8.1 Service Pack 1 Configuration Guide* provides more information on how to set thresholds.

Table 10-3. Exceptions generated by IP Performance Manager

Managed object	Exception	Component	Fault	Subscribed by Global Console	Threshold (setting)
System	Performance	Network adapter (Port or Interface)	HighBroadcastRate	Yes	BroadcastThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
			HighDiscardRate	Yes	DiscardThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)

Table 10-3. Exceptions generated by IP Performance Manager (Continued)

Managed object	Exception	Component	Fault	Subscribed by Global Console	Threshold (setting)
			HighQueueDropRate	Yes	QueueDropThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
			HighCollisionRate	Yes	CollisionThreshold (Ethernet Interface/Port Performance)
			HighUtilization	Yes	UtilizationThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
	Error	Network adapter (Port or Interface)	HighErrorRate	Yes	ErrorThreshold MinimumTrafficThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
	Resource	Memory	ExcessiveFragmentation	Yes	MemoryFragmentationThreshold (Processor and Memory)
			HighBufferMissRate	Yes	MemoryBufferMissThreshold (Processor and Memory)
			HighBufferUtilization	Yes	MemoryBufferUtilizationThreshold (Processor and Memory)
			InsufficientFreeMemory	Yes	FreeMemoryThreshold (Processor and Memory)
			InsufficientFreeMemory_MemoryPool		FreeMemoryThreshold
		Processor	HighUtilization	Yes	ProcessorUtilizationThreshold (Processor and Memory)
		FileSystem (Host only) (Available by IP Server Performance Manager only)	HighUtilization		MaxUtilizationPct (FileSystem)
System (continued)	Operational	Disk (Host only) (Available by IP Server Performance Manager only)	OperationallyDown	Yes	None

Table 10-3. Exceptions generated by IP Performance Manager (Continued)

Managed object	Exception	Component	Fault	Subscribed by Global Console	Threshold (setting)
	PowerSupply	PowerSupply	StateNotNormal	Yes	None
		VoltageSensor	OutOfRange	Yes	RelativeVoltageThreshold (Environment)
			StateNotNormal	Yes	None
	Temperature	TemperatureSensor	OutOfRange	Yes	RelativeTemperatureThreshold (Environment)
			StateNotNormal	Yes	None
		Fan	StateNotNormal	Yes	None
Chassis	OperationalException	Chassis	HighUtilization	Yes	UtilizationThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
VLAN	Performance	Network adapter (Port)	HighBroadcastRate	Yes	BroadcastThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
			HighDiscardRate	Yes	DiscardThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
			HighQueueDropRate	Yes	QueueDropThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
			HighCollisionRate	Yes	CollisionThreshold (Ethernet Interface/Port Performance)
			HighUtilization	Yes	UtilizationThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)
	Error	Network adapter (Port)	HighErrorRate	Yes	ErrorThreshold MinimumTrafficThreshold (Generic Interface/Port Performance and Ethernet Interface/Port Performance)

Events summary for IP Availability Manager

Events detected by IP Availability Managerlists the events detected by IP Availability Managerfor 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 by using the Polling and Thresholds Console, as described in the *VMware Ionix IP Management Suite Configuration Guide*.

Table 10-4. Events detected by IP Availability Manager

Managed object	Event (symptom)	Threshold (setting)	Subscribed to by the Global Manager
System	DiscoveryError	None	Yes
	MightBeDown	None	
	Unresponsive	None	Yes
	DiscoveryInProgress		
Physical Package	OperationallyDown	None	
Card	OperationallyDown	None	
	SwitchOver		Yes
Network adapter	BackupActivated	MaximumUptime (Backup Interface Support)	Yes
	ExceededMaximumUptime	MaximumUptime (Backup Interface Support or Dial-On-Demand Interface Support)	Yes
	AdministrativelyDown	None	
	DownOrFlapping	LinkTrapThreshold LinkTrapWindow (Interface/Port Flapping)	
	OperationallyDown	None	
Device connection	DownOrFlapping	See DownOrFlapping for network adapters	Yes
IP	Down	None	Yes
	Unresponsive		Yes
	SlowResponseTime		
DuplicateIP	Duplicate	None	Yes
IPv6	Down	None	Yes
	Unresponsive		Yes
DuplicateIPv6	Duplicate	None	
DuplicateVPNIP	Duplicate	None	
HSRPEndpoint	SwitchOver	None	Yes
HSRPGroup	SwitchOverFailed	None	
SNMPAgent	Unresponsive	None	

Table 10-4. Events detected by IP Availability Manager (Continued)

Managed object	Event (symptom)	Threshold (setting)	Subscribed to by the Global Manager
	RepeatedRestarts	RestartTrapThreshold RestartTrapWindow (Connectivity)	
Redundancy group	AllComponentsDown	AtRiskThreshold (set to 1 by default)	Yes
	AtRisk		Yes
	ReducedRedundancy		Yes
STPNode	stpPortStateChange	None	
VRRPGroup	SwitchOverFailed	None	
VRRPEndpoint	SwitchOver	None	
Chassis	HighBackplaneUtilization	Yes	Yes
Card	SwitchOver	None	Yes

Note *Problems, events and Notification summary for IP Availability Manager* provides a summary of the root-cause problems diagnosed by IP Availability Manager, the events correlated by IP Availability Managerto diagnose problems, and the notifications that are imported by the Global Managerfrom IP Availability Manager.

The *VMware Ionix 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.

SystemRestarted and ConfigChange events

SystemRestarted and ConfigChange events initiated by IP Availability Managerlists the events initiated by IP Availability Managerfor a managed system that has been restarted or reconfigured. When IP Availability Managerdetects a “system restarted” or “configuration change” condition, it creates and sends a SystemRestarted or ConfigChange trap to the VMware Smart Assurance 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 the *VMware Ionix IP Management Suite Configuration Guide*.

Table 10-5. SystemRestarted and ConfigChange events initiated by IP Availability Manager

Managed object	Event	Threshold (setting)	Received trap triggering the event
System	SystemRestarted **Note** Imported by the Global Manager through the Adapter Platform.	EnableGenericOIEvent MaxUpTimeThreshold (Connectivity)	coldStart or warmStart
	ConfigChange 1	None	ciscoConfigManEvent or sysConfigChangeTrap

Events summary for IP Performance Manager

Events detected by IP Performance Managerlists the events detected by IP Performance Manager. The events are imported by the

Table 10-6. Events detected by IP Performance Manager

Managed object	Event	Threshold (setting)
System	DiscoveryError	None
DuplicateIP	Duplicate	None
DuplicateIPv6	Duplicate	None

Global Console.

Note *Exception, Fault, Event, and Notification summary for IP Performance Manager* provides a summary of the exceptions generated by IP Performance Manager, the faults detected by IP Performance Managerto generate the exceptions, the events detected by IP Performance Manager, and the notifications imported by the Global Managerfrom IP Performance Manager.

Problems, events and Notification summary for IP Availability Manager

This section 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.

Problems and events

Problems and events diagnosed/detected by IP Availability Manager 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 10-7. 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)	
	MightBeDown (e)	
	DiscoveryInProgress (e)	
Chassis	Down (p)	Chassis
	HighBackplaneUtilization (e)	
	OperationallyDown (e)	
Card	Down (p)	Card
	OperationallyDown (e)	
	SwitchOver (e)	
Network adapter	Down (p)	NetworkAdapter
	Unstable (p)	
	Disabled (p)	
	LogicalConnectionDown (p)	
	DetectedProblem (p)	
	BackupActivated (e)	
	ExceededMaximumUptime (e)	
	AdministrativelyDown (e)	
	OperationallyDown (e)	
	DownOrFlapping (e)	
Device connection	Down (p)	ICIM_NetworkDeviceConnection
	Unstable (p)	
	Disabled (p)	
	DownOrFlapping (e)	
IP	Down (e)	IP
	Unresponsive (e)	
IPv6	Down (e)	IPv6
	Unresponsive (e)	
DuplicateIP	Duplicate (e)	DuplicateIP
HSRPEndpoint	SwitchOver (e)	HSRPEndPoint
VRRPEndpoint	SwitchOver (e)	VRRPEndpoint
Partition	Down (p)	Partition

Table 10-7. Problems and events diagnosed/detected by IP Availability Manager (Continued)

Managed object	Event	Class of origin
SNMPAgent	NotResponding (p)	SNMPAgent
	Unresponsive (e)	SNMPAgent_Fault (an instrumentation object)
	RepeatedRestarts (e)	
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)	
VRRPGroup	SwitchOverFailed (e	VRRPGroup
	AllComponentsDown (e)	
	AtRisk (e)	
	ReducedRedundancy (e)	
KEY (p) = Root-cause problem (e) = Event		

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

Notifications

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

Table 10-8. 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)	
	BackupActivated (e)	NetworkAdapter_Fault (an instrumentation object)
	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)	
NetworkConnection-RedundancyGroup	AllComponentsDown (e)	NetworkConnectionRedundancyGroup
	AtRisk (e)	

Table 10-8. IP Availability Manager notifications imported by the Global Manager (Continued)

Managed object	Event	Class of origin
	ReducedRedundancy (e)	
SystemRedundancyGroup	AllComponentsDown (e)	SystemRedundancyGroup
	AtRisk (e)	
	ReducedRedundancy (e)	
HSRPGroup	SwitchOverFailed (e)	HSRPGroup
	AllComponentsDown (e)	
	AtRisk (e)	
	ReducedRedundancy (e)	
VRRPGroup	SwitchOverFailed (e)	VRRPGroup
	AllComponentsDown (e)	
	AtRisk (e)	
	ReducedRedundancy (e)	
KEY (p) = Root-cause problem (e) = Event		

Note The Global Manager also imports the IPv6Network Inaccessible exception.

Exception, Fault, Event, and Notification summary for IP Performance Manager

This section summarizes the exceptions generated by IP Performance Manager, the faults detected by IP Performance Manager to generate the exceptions, the events detected by IP Performance Manager, and the notifications imported by the Global Manager.

Exceptions

Exceptions generated by IP Performance Manager lists, on a managed object basis, the exceptions generated by IP Performance Manager.

Table 10-9. Exceptions generated by IP Performance Manager

Managed object	Exception	Class of origin
System	Performance	UnitaryComputerSystem
	Error	
	Resource	
	Operational	
	PowerSupply	

Table 10-9. Exceptions generated by IP Performance Manager (Continued)

Managed object	Exception	Class of origin
	Temperature	
Chassis	BackplaneUtilization	Chassis
VLAN	Performance	VLAN
	Error	
	Operational	
	Connectivity	

Faults and events

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

Table 10-10. Faults and events detected by IP Performance Manager

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

Table 10-10. Faults and events detected by IP Performance Manager (Continued)

Managed object	Fault or event	Class of origin
	StateNotNormal (f)	
Temperature	OutOfRange (f)	TemperatureSensor_Fault
	StateNotNormal (f)	
Fan	StateNotNormal (f)	Fan_Fault
DuplicateIP	Duplicate (e)	DuplicateIP
KEY (f) = Fault (e) = Event		

Notifications

All of the faults and events listed in Notifications are imported by the Global Manager.

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

MIBs Polled and SNMP Traps Processed

11

This chapter includes the following topics:

- Standard SNMP MIBs polled by IP Availability Manager
- Standard SNMP MIBs polled by IP Performance Manager
- Enterprise MIBs polled by IP Availability Manager
- Enterprise MIBs polled by IP Performance Manager
- SNMP traps processed

Standard SNMP MIBs polled by IP Availability Manager

IP Availability Manager polls the following standard MIBs:

- LAG-MIB
- FIBRE-CHANNEL-FE-MIB
- ATM-MIB (RFC 2515)
- BRIDGE-MIB (RFC 1493)
- CISCO-STACK-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- 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)
- IEEE8023-LAG-MIB
- IF-MIB (RFC 1573)
- IP-MIB (RFC 2011)

- IPSEC-ISAKMP-IKE-DOI-TC SNMP MIB
- IPV6-MIB (RFC 2465)
- ISDN-MIB (RFC 2127)
- LLDP-MIB
- RFC1406-MIB (RFC 1406)
- RFC1286-MIB
- SNMP MIB-II (RFC 1213)
- VRRP-MIB (RFC2787)

Standard SNMP MIBs polled by IP Performance Manager

IP Performance Manager polls the following standard MIBs:

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

Enterprise MIBs polled by IP Availability Manager

IP Availability Manager polls the following vendor-specific MIBs:

- ciscoEthernetFabricExtenderMIB
- ciscoPagpMIB
- AIRESPACE-SWITCHING-MIB.my
- AIRESPACE-WIRELESS-MIB
- CISCO-DOT11-ASSOCIATION-MIB

- CISCO-DOT11-IF-MIB.my
- CISCO-LWAPP-AP-MIB
- CISCO-LWAPP-DOT11-CLIENT-MIB
- CISCO-LWAPP-WLAN-MIB
- WLSX-AUTH-MIB
- WLSX-SWITCH-MIB
- WLSX-WLAN-MIB
- AIRESPACE-SWITCHING-MIB
- AI194HUB-MIB
- AI198CLC-MIB
- ALTEON-CHEETAH-NETWORK-MIB
- ALTEON-TS-NETWORK-MIB
- ARROWPOINT-CHASSISMGREXT-MIB
- ATM-FORUM-TC-MIB
- BLADE-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
- 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
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-SYSTEM-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
- VMware-ATMOS-MIB

Note In this release, the host with sysoid .1.3.6.1.4.1.1139.16 is certified as Atmos host, ONLY if the VMware-ATMOS-MIB (1.3.6.1.4.1.1139.16.3) MIB is supported by the host.

Enterprise MIBs polled by IP Performance Manager

IP Performance Manager polls the following vendor-specific MIBs:

- ciscoEthernetFabricExtenderMIB
- ciscoPagpMIB
- AIRESPACE-SWITCHING-MIB.my
- AIRESPACE-WIRELESS-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-DOT11-IF-MIB.my
- CISCO-LWAPP-AP-MIB
- CISCO-LWAPP-DOT11-CLIENT-MIB
- CISCO-LWAPP-WLAN-MIB
- WLSX-AUTH-MIB
- WLSX-SWITCH-MIB
- WLSX-WLAN-MIB
- AIRESPACE-SWITCHING-MIB
- AI194HUB-MIB
- AI198CLC-MIB
- ALTEON-CHEETAH-SWITCH-MIB
- ARROWPOINT-CHASSISMGREXT-MIB
- ATM-FORUM-TC-MIB
- CENTILLION-BRIDGE-MIB
- CENTILLION-IF-EXTENSIONS-MIB
- CENTILLION-FDB-MIB
- CISCO-2900XL-MIB
- CISCO-CPU-MIB
- CISCO-CDP-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB

- CISCO-ENVMON-MIB
- CISCO-FRAME-RELAY-MIB
- CISCO-FRU-CONTROL-MIB
- CISCO-HSRP-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PAGP-MIB
- CISCO-PROCESS-MIB
- CISCO-RF-MIB
- CISCO-RHINO-MIB
- CISCO-STACK-MIB
- CISCO-SYSTEM-EXT-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- CNT21-MIB
- CNT241-MIB
- COSINE-ORION-MIB
- CT-CONTAINER-MIB
- CTRON-CHASSIS-MIB
- EXTREME-EDP-MIB
- EXTREME-FDB-MIB
- EXTREME-SYSTEM-MIB
- EXTREME-VLAN-MIB
- Fore-Common-MIB
- Fore-Switch-MIB
- FOUNDRY-SN-AGENT-MIB
- FOUNDRY-SN-SWITCH-GROUP-MIB
- GDCSCM-MIB
- GENERIC-3COM-TRUNK-MIB (A3Com)
- HP-ICF-OID (Hewlett Packard)
- HUAWEI-3COM-OID-MIB
- HUAWEI-LswDEVM-MIB
- JUNIPER-MIB

- LANPLEX-SYSTEM-MIB-1-1-1
- MP-DETOUR-MIB (NEC Corporation)
- OLD-CISCO-CPU-MIB
- OLD-CISCO-ENV-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-SYSTEM-MIB
- ONS15501-MIB (Cisco)
- RAPID CITY
- RBT-MIB (Riverbed)
- REPEATER-REV4-MIB (Cabletron)
- RND-MIB (RAD Network Devices)
- SSG-5000-CHASSIS-MIB (Shasta)
- STRATACOM-MIB
- SW-MIB (BCSI)
- SYNOPTICS-LS-ETHERNET-MIB
- TapeAlert-MIB (Hewlett Packard)
- UNISPHERE-DATA-ERX-SYSTEM-MIB
- Wellfleet-CCT-NAME-MIB
- Wellfleet-GAME-STATS-MIB
- Wellfleet-HARDWARE-MIB
- Wellfleet-IP-MIB
- XYLAN-BASE-MIB
- ciscoUnifiedComputingMIB
- ciscoVirtualNicMIB
- VMware-ATMOS-MIB

Note In this release, the host with sysoid .1.3.6.1.4.1.1139.16 is certified as Atmos device, ONLY if the VMware-ATMOS-MIB (1.3.6.1.4.1.1139.16.3) MIB is supported by the host.

SNMP traps processed

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

- Enterprise (the sysObjectID of the agent/object)

- Generic Trap Identifier
- Specific Trap Identifier
- Variable-Bindings
- IP address of the SNMPAgent

  IP Availability Manager and IP Performance Manager uses trap messages for two purposes:

- Discovery
- Analysis

SNMP traps processed for discovery

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

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

  SNMP traps processed by IP Availability Managerand IP Performance Managerfor discoverylists the SNMP traps that IP Availability Managerprocesses for discovery purposes.

Table 11-1. SNMP traps processed by IP Availability Manager and IP Performance Manager for discovery

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

Note IP Availability Managerand IP Performance Managerprocesses this trap, but takes no action.
IP Availability Managerand IP Performance Managerplaces the associated device for this trap on the Pending Devices list.

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

SNMP traps processed for analysis by IP Availability Manager

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.

SNMP traps that IP Availability Manager processes for analysis lists the SNMP traps that IP Availability Manager processes for analysis purposes.

Table 11-2. SNMP traps that IP Availability Manager processes 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 VMware Smart Assurance 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.

The VMware Smart Assurance IP Management Suite Configuration Guide provides more information about the SystemRestarted and ConfigChange traps, including procedures for enabling the generation of these traps.

SNMP traps processed for analysis by IP Performance Manager

SNMP traps processed by IP Performance Manager for analysis lists the SNMP traps processed by IP Performance Manager for analysis purposes.

Table 11-3. SNMP traps processed by IP Performance Manager for analysis

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

Network Topology Naming Conventions

12

This chapter includes the following topics:

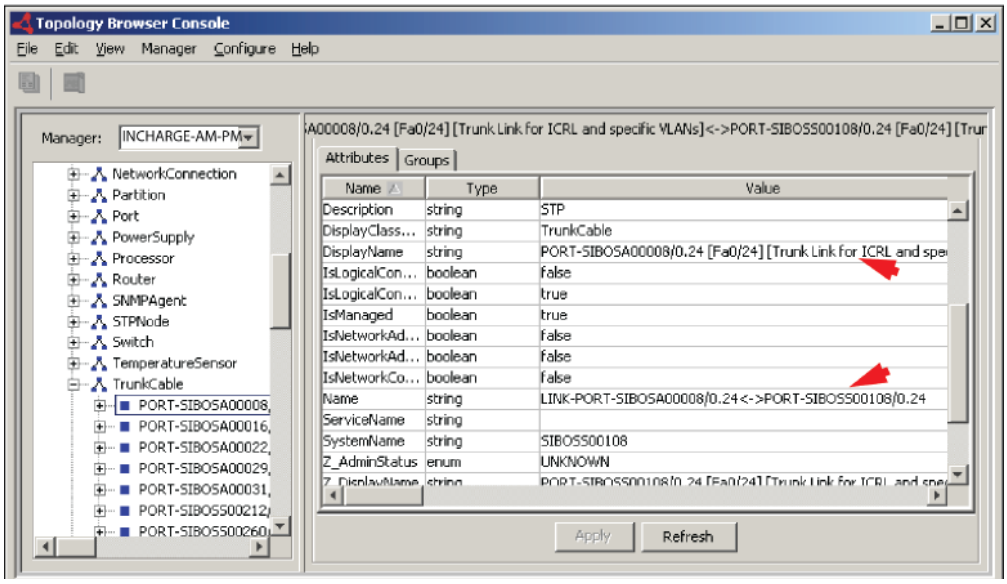
- DisplayName and Name attributes
- Naming convention for network objects

DisplayName and Name attributes

Each network object has a unique name, which is defined by the DisplayName and Name attributes for the object as shown in Figure 1 on page 184.

1 INCHARGE-AM-PM

Figure 12-1. 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.

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 and IP Performance Manager uses a consistent naming convention to assign the system and each of its components a unique name. The name assigned to a system is determined by the setting of the NameFormat parameter in the name-resolver.conf file, which is located in the BASEDIR/smarts/conf/discovery directory. The assigned name becomes the value of the system's Name attribute. The VMware Smart Assurance 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. The VMware Smart Assurance 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 and IP Performance Manager uses the appropriate naming format defined in Naming formats for discovered network objects 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 12-1. 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>*

Table 12-1. Naming formats for discovered network objects (Continued)

Class name	Naming format
LoadBalancer	Name:<*IP Address*>/<*FQDN*>
	Display Name:Name or <*MIBIISysName*>
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*>
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*>

Table 12-1. Naming formats for discovered network objects (Continued)

Class name	Naming format
	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*]
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]
VRRPEndpoint	Name:VRRP-*<IP Address>/<FQDN>/<VRRPEndpointKey>*
	Display Name:NAME [Group *<GroupNumber>*] [Interface NAME]
EVCEndPoint	Name:EVCEP-systemName [EVCEndPointId] [UNIId] [EVCId] Example:EVCEP-dev-7604.lss.vmware.com[3][PE2] [EVPL_EVC_2]
IP	Name:IP-*<IP Address>*
	Display Name:NAME [SystemName]
IPv6	Name:IPv6-*<IPv6 Address>*
	Display Name:*<IPv6 Address>* [*SystemName*]
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	

Table 12-1. Naming formats for discovered network objects (Continued)

Class name	Naming format
IPNetwork	Name:IPNET-<*NetworkNumber*> Example: IPNET-10.31.117.0
	Display Name:<*IP Address/ NetworkNumber*>
IPv6Network	Name:IPv6NET-<*NetworkNumber*> Example: IPv6NET-3FFE:80C0:22C:100:0:0:0:0
	Display Name:<*IPv6 Address*><*NetworkNumber*>
VLAN	Name:VLAN-<*VLANKey*>
	Display Name:NAME-[VLAN Description]
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
VRAgent	Name:VRA-<IP-Address>/<RouterID>
	DisplayName:VR Agent <IP-Address>/<RouterID>
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]

Table 12-1. Naming formats for discovered network objects (Continued)

Class name	Naming format
VoltageSensor	Name:VOLT-<*IP Address*>/<*FQDN*>/<*Index*>
	Display Name:NAME [VoltageSensor description]
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*>]
VRRPGroup	Name:VRRP-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	

Discovery

13

This chapter includes the following topics:

- Discovery probes
- Seed file format
- Device entry field descriptions
- Location, names, and content of discovery hook scripts
- ECIM-R hierarchies
- ECIM-R topology collection sets
- ECIM-R relationships

Discovery probes

The discovery process calls the discovery probes in the order that the probes are listed:

1. Name Resolution probe
2. Containment probe
3. VLAN probe
4. Bridge probe
5. HSRP probe
6. VRRP probe
7. IP Network probe
8. Virtual Router probe
9. Neighbor probe
10. Performance probe
11. Host Resources probe

VRRP probe

VRRP MIB data

vrrpAssoIpAddrRowStatusOID ".1.3.6.1.2.1.68.1.4.1.2"

– Key OID – If not present, any other VRRP data is not probed.

– The row status variable - Setting this object to active(1) or createAndGo(4) results in the addition of an associated address for a virtual router.

vrrpOperPriorityOid ".1.3.6.1.2.1.68.1.3.1.5"

– This object specifies the priority to be used for the virtual router master election process. Higher values imply a higher priority.

vrrpOperVirtualMacAddrOid ".1.3.6.1.2.1.68.1.3.1.2"

– The virtual MAC address of the virtual router.

vrrpOperState ".1.3.6.1.2.1.68.1.3.1.3"

– The current state of the virtual router. *Initialize*, *Backup* or *Master*.

– vrrpInfoVirtRtrState "1.3.6.1.4.1.1872.2.5.3.3.3.1.1.2“ or “1.3.6.1.4.1.1872.2.1.9.4.1.1.2” in Nortel

vrrpOperRowStatusOid ".1.3.6.1.2.1.68.1.3.1.15“

– The rowstatus of a currently active row in the vrrpOperTable is constrained by the operational state of the corresponding virtual router.

vrrpOperMasterIpAddrOID ".1.3.6.1.2.1.68.1.3.1.7“

– The master router's real (primary) IP address. This is the IP address listed as the source in a VRRP advertisement last received by this virtual router.

Seed file format

A seed file consists of one or more seed entries, each of which represents a discovery candidate system.

Seed-entry options

The allowed options for a seed entry are specified by using the keywords that are described in Keywords for seed file.

Table 13-1. Keywords for seed file

Keyword	Value	Definition
Global SNMP options		
ACCESSMODE=	ICMPONLY, SNMPONLY, or ICMPSNMP Default: ICMPSNMP	Protocols that are used to access the candidate system: ■ For ICMPSNMP, both ICMP and SNMP are used to discover and monitor the system. ■ For ICMPONLY, the system is not discovered or monitored. Instead, the system is added to the topology as a Host, which limits the IP Manager to only availability analysis by using ICMP. ■ For SNMPONLY, the system is discovered by using SNMP, but ICMP is not used to determine whether the system is reachable or to monitor the system's availability.
ADDRESSFORMAT=	AUTOADDRESS or LOOPBACKADDRESS Default: value in discovery.conf	Address that is used to access the candidate system for discovery and polling. If the value is omitted, the value that is specified in the AccessAddressFormat parameter (AUTOADDRESS by default) in the discovery.conf file is used. The *VMware Smart Assurance IP Management Suite Configuration Guide* provides information about the AccessAddressFormat parameter.
SNMPPORT=	0 to 65535 Default: port in discovery.conf	SNMP port that is used to access the SNMP agent of the candidate system. If the value is omitted or 0, the port that is specified in the defaultSNMPPort parameter (161 by default) in the discovery.conf file is used. The *VMware Smart Assurance IP Management Suite Configuration Guide* provides information about the defaultSNMPPort parameter.
SNMPVERSION=	V1, V2C, V3, or AUTODETECT Default: AUTODETECT	SNMP protocol version that is supported by the SNMP agent of the candidate system: ■ For AUTODETECT, send v2c request; if no response, send v1 request. ■ For V1, send v1 request only. ■ For V2C, send v2c request only. ■ For V3, send v3 request only. The SNMP protocol version is also the expected version of any trap message that is received from the candidate system after the system is discovered. For SNMPVersion=AUTODETECT, the expected trap message version is v2c or v1, which depends on the version of the first SNMP poll to successfully communicate with the SNMP agent of the candidate system.

Table 13-1. Keywords for seed file (Continued)

Keyword	Value	Definition
NAMEFORMAT=	TM_USEAUTONAME, TM_USELOOPBACK, TM_USESYSNAME, TM_USENONPRIVATEIP, TM_USEPRIVATEIP, TM_USEAGENTADDRESS, or TM_USESEEDNAME Default: null string (empty)	Naming source that is used to resolve the name of the candidate system. “How discovery names a system” on page 61 provides information on the NAMEFORMAT and SEEDNAME keywords.
SEEDNAME=	String of unspecified length Default: null string (empty)	User-specified name for the candidate system.
SNMPv1 and v2c options		
COMMUNITY=	String of unspecified length Default: read string or strings in Read Community Strings window 1	Read community string that is included in a request that is sent to the SNMPv1/v2c agent of the candidate system. This keyword is required if the first character of the string is #.
SNMPv3 options		
USER=	String that consists of 1 to 32 characters Default: null string (empty)	Name of the user that is included in a request that is sent to the SNMPv3 agent of the candidate system or received in an SNMPv3 trap message. Username is required.
ENGINEID=	An even-length string between 10 and 64 hex characters; e.g., 800002b804616263 Default: null string (empty)	Identifier, within an administrative domain, that uniquely identifies the SNMP engine of the SNMPv3 agent. Engine ID is required for communication to the SNMPv3 agent: ■ When specified, the IP Manager uses the specified value when attempting to communicate with the SNMP agent. ■ If empty, the IP Manager learns the engine ID through the engine ID discovery mechanism described in RFC 3414 and then uses the learned value when attempting to communicate with the SNMP agent. Engine ID is also required to authenticate and decrypt an SNMPv3 trap message.
AUTHPROTOCOL=	MD5, for Message Digest 5, SHA, for Secure Hash Algorithm, or NONE Default: NONE 2	For authentication: ■ Protocol that is used for authentication when sending a request to the SNMPv3 agent. ■ Authentication protocol is recommended but not required.
		For authenticating: ■ Protocol that is used for authenticating an SNMPv3 trap message. ■ Authentication protocol is required to authenticate an SNMPv3 trap message.

Table 13-1. Keywords for seed file (Continued)

Keyword	Value	Definition
AUTHPASS=	String that consists of 1 to 64 characters; using at least eight characters is recommended Default: null string (empty)	Password that is used as the basis for the following: the creation of the localized authentication key that is used with the selected authentication protocol and the SNMPv3 agent. The password is required if the authentication protocol is MD5 or SHA. Otherwise, the password is ignored. The password may be encrypted (recommended) or appear as plain text in the seed file. 3
PRIVPROTOCOL=	DES, for Data Encryption Standard, AES, for Advanced Encryption Standard, or NONE Default: NONE 4	For encryption: ■ Protocol that is used for encryption when sending a request to the SNMPv3 agent. ■ Privacy protocol is recommended but not required. For decrypting: ■ Protocol that is used for decrypting an SNMPv3 trap message. ■ Privacy protocol is required to decrypt an SNMPv3 trap message.
PRIVPASS=	String that consists of 1 to 64 characters; using at least eight characters is recommended Default: null string (empty)	Password that is used as the basis for the following: the creation of the localized encryption key that is used with the selected privacy protocol and the SNMPv3 agent. The password is required if the privacy protocol is DES or AES. Otherwise, the password is ignored. The password may be encrypted (recommended) or appear as plain text in the seed file. 3
CONTEXT=	String of no specific length Default: null string (empty)	Name that together with the username determines the access permissions of a request that is sent to the SNMPv3 agent. Context name is optional. The IP Manager must have permissions to access the standard and proprietary MIBs. that are identified in Appendix A of the VMware Smart Assurance IP Availability Manager User Guide.

1 Specified in the Topology tab of the Domain Manager Administration Console.

2 MD5 and SHA authentication are defined in RFC 3414.

3 Explained in “How to encrypt passwords in the seed file” on page 103.

4 DES privacy is defined in RFC 3414, and AES (AES-128) privacy is defined in RFC 3826.

Mandatory keyword options for SNMPv3

For a candidate system that has an SNMPv3 agent, two keyword options are mandatory:

- SNMPVERSION
- USER

  Required keyword options for various SNMPv3 seed entry scenarios identifies the required keyword options for various SNMPv3 seed entry scenarios.

Table 13-2. Required keyword options for various SNMPv3 seed entry scenarios

Seed entry scenario	Keyword options required
Seed entry 1: Send an authenticated message to an SNMPv3 agent:	■ SNMPVERSION=V3 ■ USER=<user name> ■ AUTHPROTOCOL=MD5 or SHA ■ AUTHPASS=<auth password>
Seed entry 2: Send an encrypted message to an SNMPv3 agent:	■ SNMPVERSION=V3 ■ USER=<user name> ■ PRIVPROTOCOL=DES or AES ■ PRIVPASS=<priv password>
Seed entry 3: Send an authenticated and encrypted message to an SNMPv3 agent:	■ SNMPVERSION=V3 ■ USER=<user name> ■ AUTHPROTOCOL=MD5 or SHA ■ AUTHPASS=<auth password> ■ PRIVPROTOCOL=DES or AES ■ PRIVPASS=<priv password>
Seed entry 4: Authenticate an SNMPv3 trap:	■ SNMPVERSION=V3 ■ USER=<user name> ■ ENGINEID=<engine id> ■ AUTHPROTOCOL=MD5 or SHA ■ AUTHPASS=<auth password>
Seed entry 5: Decrypt an SNMPv3 trap:	■ SNMPVERSION=V3 ■ USER=<user name> ■ ENGINEID=<engine id> ■ PRIVPROTOCOL=DES or AES ■ PRIVPASS=<priv password>
Seed entry 6: Authenticate and decrypt an SNMPv3 trap:	■ SNMPVERSION=V3 ■ USER=<user name> ■ ENGINEID=<engine id> ■ AUTHPROTOCOL=MD5 or SHA ■ AUTHPASS=<auth password> ■ PRIVPROTOCOL=DES or AES ■ PRIVPASS=<priv password>

Device entry field descriptions

Device entry field descriptions in oid2type_Field.conf describes the device entry fields for a field-based certification.

Table 13-3. Device entry field descriptions in oid2type_Field.conf

Field	Description
TYPE	Type of device. This value can be any unitary computer system class. This field is mandatory.
VENDOR	Manufacturer of the device. This value must be a single word. This field is mandatory.

Table 13-3. Device entry field descriptions in oid2type_Field.conf (Continued)

Field	Description
MODEL	Model name of the device. The field name, MODEL, is required. The value of MODEL is optional, and can be more than one word.
CERTIFICATION	Level of certification for the device. The value should always be CERTIFIED which means that the system is recognized by the IP Manager, but there is no knowledge about support for various MIBS used in the discovery process.
Discovery driver keywords	
ADNR	Parameter name of the autodiscovery name resolution driver that is to be used by the IP Manager to discover interface and IP (v4 and v6) address information for the device, for the purpose of determining if the device is a “match” to another device. The driver gathers the information from MIB-II-like tables in vendor-specific MIBs on the device. The full name of the autodiscovery name resolution driver is AD-MIB2-Data-<*param-name*>-Driver. Examples: AD-MIB2-Data-Unisphere-Access-Driver, AD-MIB2-Data-Tellabs-Access-Driver
DSCVDATA	Parameter name of the discovery data driver that is to be used by the IP Manager, in conjunction with the ADNR driver, to discover interface and IP (v4 and v6) address information for the device, for the purpose of determining if the device is a “match” to another device. The driver gathers the information from MIB-II-like tables in vendor-specific MIBs on the device. The full name of the discovery data driver is MIB2-Data-<*param-name*>-Driver. Examples: MIB2-Data-ERX-VR-Cont-Driver, MIB2-Data-Tellabs-Access-Driver
BRIDGE	Applicable to bridge or switch device only:Parameter name of the Bridge driver that is to be used by the IP Manager to collect bridge-forwarding tables and STP information for the bridge or switch device. The full name of the Bridge driver is Bridge-<*param-name*>-Driver. Examples: Bridge-Bay-C100-Driver, Bridge-Tut-MXL2300-BRIDGE-Driver
CONT	Parameter name of the Containment driver that is to be used by the IP Manager to discover the components of the device, including ports, interfaces, MAC endpoints, and any cards or modules. The full name of the Containment driver is Containment-<*param-name*>-Driver. Examples: Containment-Generic-MIB2-Driver, Containment-Cisco-Router-Driver
HEALTH	Parameter name of the Performance driver that is to be used by the IP Manager to collect performance-related information for the device’s components such as ports, interfaces, processors, memory, fans, power supplies, voltage sensors, and temperature sensors. The full name of the Performance driver is Performance-<*param-name*>-Driver. Examples: Performance-Max-TNT-Driver, Performance-AvayaVPNet-Driver
HOSTRESRCS	Applicable to host device only:Parameter name of the Host Resources driver that is to be used by the IP Manager to collect additional performance-related information for the host device’s components. The Host Resources driver collects metrics about host disks and file systems as well as additional information about host processors and memory. The full name of the Host Resources driver is HostResrcs-<*param-name*>-Driver. Examples: HostResrcs-MIB2-Driver, HostResrcs-HP-Driver

Table 13-3. Device entry field descriptions in oid2type_Field.conf (Continued)

Field	Description
IPNETWORK	Parameter name of the IP Network driver that is to be used by the IP Manager to examine the device's IP address table, to combine the IP (v4 and v6) addresses and the netmask for each interface on the device to create IPNetwork and IPv6Network objects, and to build the connected relationships between IP endpoints and IP networks and between IPv6 endpoints and IPv6 networks. The full name of the IP Network driver is IPNetwork-<*param-name*>-Driver. Examples: IPNetwork-Access-Driver, IPNetwork-3Com-CB9000L2-Driver
NEIGHBOR	Parameter name of the Neighbor driver that is to be used by the IP Manager to collect information about the device's neighbors by reading CDP, EDP, FDP, and other tables to discover remote addresses on the already discovered networks, and to discover ATM information. The full name of the Neighbor driver is Neighbor-<*param-name*>-Driver. Examples: Neighbor-ATM-Peer-Driver, Neighbor-Foundry-Fdp-Driver
RESOLVER	Parameter name of the Name Resolution driver that is to be used by the IP Manager to discover the IP (v4 and v6) addresses that are available for the device, and to provide a unique name for the device. The full name of the Name Resolution driver is Name-Resolver-<*param-name*>-Driver. Examples: Name-Resolver-Access-Driver, Name-Resolver-OnlyData-Driver
VLAN	Applicable to bridge or switch device only:Parameter name of the VLAN driver that is to be used by the IP Manager to collect VLAN information for the bridge or switch device, including VLAN identifiers, VLAN trunks, VLAN trunk ports, and VLAN port memberships. The full name of the VLAN driver is Vlan-<*param-name*>-Driver. Examples: Vlan-ERX-Driver, Vlan-Cisco-Membership-Driver
VROUTER	Applicable to router or switch device only:Parameter name of the Virtual Router driver that is to be used by the IP Manager to discover the virtual routers in the IPv4 physical router or switch device that contains virtual routers. The full name of the Virtual Router driver is VRouter-<*param-name*>-Driver. Examples: VRouter-ERX-Driver, VRouter-Cosine-Orion-Driver
VRRP	Applicable to router only:Parameter name of the VRRP driver that is to be used by the IP Manager to collect information from the router device about the redundancy group of routers that are involved in a VRRP group. The full name of the VRRP driver is VRRPGroup-<*param-name*>-Driver. Example: VRRPGroup-Unisphere-ERX-Driver
INSTRUMENTATION:	Introduces the instrumentation portion of a device entry.
Instrumentation keywords	
CPU/Memory	Name of the instrumentation set that is to be used by the IP Manager to monitor the performance of the device's CPU and memory. Examples: HostResources:DeviceID, CiscoSwitch:DeviceID, BluecoatRsc:DeviceID
Card-Fault	Name of the instrumentation set that is to be used by the IP Manager to monitor the status of the device's cards. Examples: Default, CiscoStack, AlcatelTimex
Disk-Fault	Name of the instrumentation set that is to be used by the IP Manager to monitor the status of the device's disks. Examples: HostResources:DeviceID, BluecoatRsc:DeviceID

Table 13-3. Device entry field descriptions in oid2type_Field.conf (Continued)

Field	Description
Chassis-Performance	Name of the instrumentation set that is to be used by the IP Manager to monitor the performance of the device's chassis. Example: = CiscoStack
FileSystem-Performance	Name of the instrumentation set that is to be used by the IP Manager to monitor the performance of the device's file systems. Examples: HostResources:DeviceID, HostResources_HP:DeviceID
Environment	Name of the instrumentation set that is to be used by the IP Manager to monitor the device's fans, memory, power supplies, temperature sensors, and voltage sensors. Examples: = CiscoStack, MrvEnvMon:DeviceID, DellEnvMon3248OID3:DeviceID
Interface-Fault	Name of the instrumentation set that is to be used by the IP Manager to monitor the status of the device's interfaces. Examples: MIB2, WellfleetRouter MIB2 means that the IP Manager polls ifAdminStatus and ifOperStatus for interface status.
Interface-Performance	Name of the instrumentation set that is to be used by the IP Manager to monitor the performance of the device's interfaces. Examples: MIB2, MIB2SNMP, CiscoRouter MIB2 means that the IP Manager polls ifInOctets, ifOutOctets, and other counters in the ifTable to report interface utilization and other statistics.
Interface-Ethernet-Performance	Name of the instrumentation set that is to be used by the IP Manager to monitor the performance of the device's Ethernet interfaces. Examples: MIB2, CiscoRouter_Ethernet
Port-Fault	Name of the instrumentation set that is to be used by the IP Manager to monitor the status of the device's ports. Examples: MIB2, AlcatelTimex:DeviceID, Brocade:PortKey
Port-Performance	Name of the instrumentation set that is to be used by the IP Manager to monitor the performance of the device's ports. This value is always MIB2.
Port-Ethernet-Performance	Name of the instrumentation set that is to be used by the IP Manager to monitor the performance of the device's Ethernet ports. Examples: MIB2, dot3_Ethernet

Location, names, and content of discovery hook scripts

The IP Manager provides five discovery hook scripts listed in Hook scripts, all of which are located in the BASEDIR/smarts/rules/discovery/custom directory in the IP Manager installation area

Table 13-4. Hook scripts

Hook script file name	Description
custom-start-fulldscv.asl	Is run by the IP Manager before a full discovery.
custom-start-system.asl	Is run by the IP Manager before initial system discovery.
custom-end-system.asl	Is run by the IP Manager after initial system discovery and before postprocessing.

Table 13-4. Hook scripts (Continued)

Hook script file name	Description
custom-start-post.asl	Is run by the IP Manager at the beginning of postprocessing.
custom-end-post.asl	Is run by the IP Manager at the end of postprocessing.

Examples of hook scripts

Two of the discovery hook scripts, custom-end-system.asl and custom-start-post.asl, as shipped with the IP Manager, are shown in *Figure on page* and *Figure on page*.

```
/*
.
.
.
 * RCS $Id: custom-end-system.asl,v 1.1 2003/03/06 17:39:37 ouc Exp $
 *
 * This asl file is used at the end of probing of each device.
 */
default AgentName  = "";
agentObj = object("SNMPAgent", AgentName);
if (agentObj->isNull()) {
    stop();
}
nodeObj = agentObj->getSystem();
if (nodeObj->isNull()) {
    stop();
}
factory = object(getInstances("ICIM_ObjectFactory")[0]);
topo_manager = object(getInstances("ICF_TopologyManager")[0]);
default DEBUG = topo_manager->DebugEnabled;
me = this->ReadsRulesFrom->fileName.": ";
blanks = "    ";
/*
 * Add additional initialization here.
 */
/*
 * Add convenience patterns here.
 */
/******************************************************************************/
START {
    /*
     * Add Parsing rules here.
     */
    .. eol
} do {
    /*
     * Add processing rules here.
     */
    stop();
}
/*
 * Addition EOF or DEFAULT here if necessary.
```

```
 */
/*********************************************************/
/*
 * Local Variables:
 * mode: C++
 * End:
 */
/*
.
.
.
 * RCS $Id: custom-start-post.asl,v 1.1.464.1 2009/02/04 21:36:47 tdemay Exp $
 *
 * This asl file is used at beginning of discovery post processing.
 */
factory = object(getInstances("ICIM_ObjectFactory")[0]);
topo_manager = object(getInstances("ICF_TopologyManager")[0]);
default DEBUG = topo_manager->DebugEnabled;
me = this->ReadsRulesFrom->fileName.": ";
blanks = "    ";
/*
 * Add additional initialization here.
 */
/*
 * Add convenience patterns here.
 */
/*****************************************************************************/
START {
    /*
     * Add Parsing rules here.
     */
    .. eol
} do {
    start = STARTTIMER() ;
    /*
     * Add processing rules here.
     */
    FINISHTIMER(start) ;
    stop();
}
STARTTIMER() do {
    msg = "Starting: ".this->Name ;
    TIMER(msg) ;
    return time() ;
}
FINISHTIMER(start) do {
    msg = "Finished: ".this->Name." (Running time: ".time()-start." seconds)" ;
    TIMER(msg) ;
}
TIMER(msg) do {
    print(msg." at ".time());
    topo_manager->probeStatusMessage = msg;
}
/*
 * Addition EOF or DEFAULT here if necessary.
```

```
 */
/*********************************************************/
/*
 * Local Variables:
 * mode: C++
 * End:
 */
```

ECIM-R hierarchies

ECIM-R depends upon class hierarchy and inheritance in order to pass attributes and other characteristics to other classes.

As an example of class hierarchy, here is the hierarchy of the ECIM-R Host class:

```
Host : UnitaryComputerSystem : ICIM_UnitaryComputerSystem : VMware_ComputerSystem :
ICIM_ComputerSystem : CIM_ComputerSystem : ICIM_ExtendedSystem : ICIM_System : CIM_System :
CIM_EnabledLogicalElement : ICIM_LogicalElement : CIM_LogicalElement : ICIM_ManagedSystemElement :
CIM_ManagedSystemElement : ICIM_ManagedElement : CIM_ManagedElement : ICF_CoreManagedElement :
CORE_ManagedObject : MR_ManagedObject : MR_Object
```

In this hierarchy, Host is a child class of UnitaryComputerSystem, which is a child class of ICIM_UnitaryComputerSystem, which is a child class of VMware_ComputerSystem, and so on.

An essential feature of ECIM-R is that it describes the managed network in terms of two parallel, but distinct, class hierarchies: physical and logical. Classes in both hierarchies are included in the IP data model.

The physical hierarchy describes the real-world components that make up your managed system; for example, a chassis. The logical hierarchy describes logical components that are created through the operation of hardware and software; for example, a host.

The physical hierarchy

The physical hierarchy consists of subclasses of the class ICIM_PhysicalElement, which describes any objects of a system that have distinct physical identities. All ECIM-R physical objects can contain or host other physical objects.

The most common class in the physical hierarchy is Card. Card is used to model any object that is capable of carrying signals or providing a mounting point for other physical components. Other classes that you will see include Chassis, which represents a physical object that encloses other objects and provide some definable functionality, and Rack, which represents an enclosure in which a Chassis is placed.

The most basic relationship in the physical hierarchy is ComposedOf, which relates a physical object to its component parts, which in turn are PartOf the enclosing object. A Chassis is ComposedOf the Cards that are placed in it. A Card that is used as a motherboard might in turn be ComposedOf Cards that are plugged in to it.

ComposedOf and other relationships are described in ECIM-R relationships.

Physical package classes instantiated by the IP Manager identifies the physical package classes that can be instantiated by the IP Manager.

Table 13-5. Physical package classes instantiated by the IP Manager

Class	Available to	Comment
Card	All IP Manager products	A type of physical container that can be plugged into another card or hosting board, or is itself a hosting board or motherboard in a Chassis.
Chassis	All IP Manager products	A physical element that encloses other elements and provides definable functionality, such as a desktop, processing node, Uninterruptible Power Supply (UPS), disk or tape storage, or a combination of these.
NASChassis	All IP Manager products	The chassis of a Celerra network-attached storage (NAS) gateway.
Rack	All IP Manager products	An enclosure in which chassis are placed. Typically, a rack is nothing more than the enclosure, and all the functioning component is packaged in the chassis that is loaded in the rack.

Note The indentations in the Class column indicate class hierarchy.

Hierarchy example for physical package classes:

Card : VMware_Card : CIM_Card : PhysicalPackage : ICIM_PhysicalPackage : CIM_PhysicalPackage : ICIM_PhysicalElement : CIM_PhysicalElement : ICIM_ManagedSystemElement : CIM_ManagedSystemElement : ICIM_ManagedElement : CIM_ManagedElement : ICF_CoreManagedElement : CORE_ManagedObject : MR_ManagedObject : MR_Object

Unitary computer systems

A unitary computer system, or just system, represents a computer-based network entity. Important classes of the computer system include Host and the following relay systems: Hub, Bridge, Switch, and Router. The relay systems forward packets at Layer 1 (a Hub), Layer 2 (a Bridge or Switch), or Layer 3 (a Router) in a network.

Unitary computer system classes instantiated by the IP Manager identifies the unitary computer system classes that can be instantiated by the IP Manager.

Table 13-6. Unitary computer system classes instantiated by the IP Manager

Class	Available to	Description
Bridge	All IP Manager products	A protocol-independent system that passes packets at the data-link layer between physically separate LANs.
Host	All IP Manager products	A general purpose computer, such as a workstation or a server.
CallServer	All IP Manager products	A system that hosts an application server that manages the setup or connection of telephone calls, such as a system that hosts the Call Manager application for a VoIP network.

Table 13-6. Unitary computer system classes instantiated by the IP Manager (Continued)

Class	Available to	Description
FileServer	All IP Manager products	A system that hosts file shares, such as a Data Mover component of a Celerra NAS gateway.
Hub	All IP Manager products	A system that connects multiple physical segments. A hub repeats signals that are received on any of its ports to all of its other ports.
Node	All IP Manager products	A system that has an unrecognized objectID. The IP Manager probes a Node for standard MIB-II data to monitor and analyze a Node object.
Probe	All IP Manager products	A system that monitors networks or other systems. An example is a remote monitoring (RMON) probe.
Router	All IP Manager products	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 towards its destination. A router might also be a virtual router, which is a software emulation of a router that is implemented within a physical router or switch.
Firewall	All IP Manager products	A system that controls the flow of traffic between networks.
LoadBalancer	All IP Manager products	A system that distributes client traffic across multiple web servers.
MSFC	All IP Manager products	A multilayer switch feature card in a Catalyst 6000/6500 switch that runs Cisco IOS router software and performs routing between virtual LANs (VLANs).
RSFC	All IP Manager products	A route switch feature card in a Catalyst 5000/5500 switch that runs Cisco IOS router software and performs routing between VLANs.
RSM	All IP Manager products	A route switch module (Card) in a Catalyst 5000 switch that runs Cisco IOS router software and performs routing between VLANs.
Switch	All IP Manager products	A system that switches packets, typically at wire speeds, between physically separate network segments.
MediaGateway	All IP Manager products	A system that hosts an application server that converts one media stream to another, such as a system that hosts the media server and gateway applications for a VoIP network.
TerminalServer	All IP Manager products	A specialized system that connects terminals to a network.
Uncertified	All IP Manager products	An uncertified object that identifies a system that has yet to be certified by VMware, Inc.. The IP Manager does not monitor Uncertified objects.

Note The indentations in the Class column indicate class hierarchy.

Hierarchy example for unitary computer system classes:

Bridge : RelayDevice : ICIM_RelayDevice : UnitaryComputerSystem : ICIM_UnitaryComputerSystem : VMware_ComputerSystem : ICIM_ComputerSystem : CIM_ComputerSystem : ICIM_ExtendedSystem : ICIM_System : CIM_System : CIM_EnabledLogicalElement : ICIM_LogicalElement : CIM_LogicalElement : ICIM_ManagedSystemElement : CIM_ManagedSystemElement : ICIM_ManagedElement : CIM_ManagedElement : ICF_CoreManagedElement : CORE_ManagedObject : MR_ManagedObject : MR_Object

Network adapters

A network adapter represents a Layer 2 connection point. Two classes are common: Interfaces, such as Ethernet interfaces that connect routers to an Ethernet; and Ports, which connect interfaces to Layer 2 systems. An Ethernet connection to an Ethernet switch is an example of a Port.

Network adapter classes instantiated by the IP Manager identifies the network adapter classes that can be instantiated by the IP Manager.

Table 13-7. Network adapter classes instantiated by the IP Manager

Class	Available to	Description
Interface	All IP Manager products	A logical connection to a network; for example, an Ethernet interface that connects a router to an Ethernet.
VRInterface	All IP Manager products	An interface of a virtual router.
Port	All IP Manager products	A port to which an interface connects and gains access to a network; for example, an Ethernet port on an Ethernet switch.

Hierarchy example for network adapter classes:

Interface : NetworkAdapter : ICIM_NetworkAdapter : VMware_NetworkPort : CIM_NetworkPort : CIM_LogicalPort : ICIM_LogicalDevice : CIM_LogicalDevice : CIM_EnabledLogicalElement : ICIM_LogicalElement : CIM_LogicalElement : ICIM_ManagedSystemElement : CIM_ManagedSystemElement : ICIM_ManagedElement : CIM_ManagedElement : ICF_CoreManagedElement : CORE_ManagedObject : MR_ManagedObject : MR_Object

Device connections

A device connection represents the path between a pair of network adapters. The most important examples are NetworkConnections, Cables, and TrunkCables.

The ConnectedVia relationship plays a role for device connections that is similar to its role for logical links. A Switch can be connected by a Cable to a Router, or by a TrunkCable to another Switch. Two Routers that are joined by a virtual circuit whose intermediate systems are not included in the topology are connected by a NetworkConnection.

Device connection classes instantiated by the IP Manager identifies the device connection classes that can be instantiated by the IP Manager.

Table 13-8. Device connection classes instantiated by the IP Manager

Class	Available to	Description
NetworkConnection	All IP Manager products	A network connection between two interfaces. A NetworkConnection can be a logical connection or a physical connection.
Cable	All IP Manager products	A connection between a network relay device, for example, a switch or hub, and a non-relay device, for example, a host or router.
TrunkCable	All IP Manager products	A connection between two network relay devices; switches are often “trunked” to provide redundant pathways through the network.

Hierarchy example for device connection classes:

NetworkConnection : ICIM_NetworkDeviceConnection : VMware_NetworkDeviceConnection : ICIM_DeviceConnection : VMware_DeviceConnection : VMware_ConnectivityCollection : CIM_ConnectivityCollection : CIM_SystemSpecificCollection : CIM_Collection : ICIM_Connection : CIM_EnabledLogicalElement : ICIM_LogicalElement : CIM_LogicalElement : ICIM_ManagedSystemElement : CIM_ManagedSystemElement : ICIM_ManagedElement : CIM_ManagedElement : ICF_CoreManagedElement : CORE_ManagedObject : MR_ManagedObject : MR_Object

Protocol endpoints

A protocol endpoint describes a logical endpoint that can be used to gain access to some network service. Important protocol endpoints are IP, which represents the point at which an IP address (Layer 3) can be reached, and Media Access Control (MAC), which similarly represents the point at which a MAC (Layer 2) address can be reached.

A protocol endpoint is related to some lower-level network object by the LayeredOver relationship. Thus, an IP address would be LayeredOver an Interface.

Protocol endpoint classes instantiated by the IP Manager identifies the protocol endpoint classes that can be instantiated by the IP Manager.

Table 13-9. Protocol endpoint classes instantiated by the IP Manager

Class	Available to	Description
DLCI	All IP Manager products	A Frame Relay data link connection identifier endpoint.
IP	All IP Manager products	An IPv4 address endpoint.
DuplicateIP	All IP Manager products	Two or more occurrences of the same IPv4 address.
IPv6	All IP Manager products	An IPv6 address endpoint.
DuplicateIPv6	All IP Manager products	Two or more occurrences of the same IPv6 address.
IPRoute	All IP Manager products	The start of the Default Route that is assigned to a system.
MAC	All IP Manager products	A media access control endpoint.
STPNode	All IP Manager products	Spanning Tree Protocol capabilities for a switch port.

Table 13-9. Protocol endpoint classes instantiated by the IP Manager (Continued)

Class	Available to	Description
TCP	All IP Manager products	A Transmission Control Protocol listening endpoint, as is used by network services such as HTTP servers.
VirtualTCP	All IP Manager products	A virtual TCP listening endpoint that has a mapping between virtual to real TCP endpoints, as is used by load balancers to map URLs to real HTTP servers.
HSRPEndpoint	All IP Manager products	A Hot Standby Router Protocol endpoint, which is a logical element that is defined per interface per HSRP group on the hosting router.
VRRPEndpoint	All IP Manager products	A Virtual Router Redundancy Protocol endpoint, which is a logical element that is defined per interface per VRRP group on the hosting router.

Hierarchy example for protocol endpoint classes:

DLCI : ProtocolEndpoint : ICIM_ProtocolEndpoint : CIM_ProtocolEndpoint : ICIM_ServiceAccessPoint : CIM_ServiceAccessPoint : CIM_EnabledLogicalElement : ICIM_LogicalElement : CIM_LogicalElement : ICIM_ManagedSystemElement : CIM_ManagedSystemElement : ICIM_ManagedElement : CIM_ManagedElement : ICF_CoreManagedElement : CORE_ManagedObject : MR_ManagedObject : MR_Object

Logical links

A logical link represents the path that connects protocol endpoints to each other. The most common logical link class is IPNetwork, which represents an IP (sub)network. ConnectedVia describes the relationship between a protocol endpoint and a logical link. Two IP addresses can communicate directly when they are ConnectedVia the same IPNetwork. A connection between two IP addresses that are not on the same IPNetwork must go through one or more Routers.

Logical link classes instantiated by the IP Manager identifies the logical link classes that can be instantiated by the IP Manager.

Table 13-10. Logical link classes instantiated by the IP Manager

Class	Available to	Description
IPNetwork	All IP Manager products	A Layer 3 logical link between IP objects.
IPv6Network	All IP Manager products	A Layer 3 logical link between IPv6 objects.
VLAN	All IP Manager products	A virtual LAN that is typically implemented in switched network environments.
VirtualCircuit	All IP Manager products	A virtual connection between network endpoints, typically traversing a WAN.
FrameRelayPVC	All IP Manager products	A circuit that is implemented over a Frame Relay network.

Hierarchy example for logical link classes:

IPNetwork : CIM_IPSubnet : LogicalNetwork : ICIM_LogicalNetwork : CIM_LogicalNetwork : CIM_CollectionOfMSEs : LogicalLink : ICIM_LogicalLink : CIM_Collection : ICIM_Connection : CIM_EnabledLogicalElement : ICIM_LogicalElement : CIM_LogicalElement : ICIM_ManagedSystemElement : CIM_ManagedSystemElement : ICIM_ManagedElement : CIM_ManagedElement : ICF_CoreManagedElement : CORE_ManagedObject : MR_ManagedObject : MR_Object

Collections

A collection represents a group of managed objects, such as an isolated region of inter-connected network devices.

Collection classes instantiated by the IP Manager identifies the collection classes that can be instantiated by the IP Manager.

Table 13-11. Collection classes instantiated by the IP Manager

Class	Available to	Description
Partition	All IP Manager products	A collection of managed elements.

Hierarchy example for collection classes:

Partition : ICIM_Collection : CORE_Collection : CORE_ManagedObject : MR_ManagedObject : MR_Object

Management agents

A management agent is a logical object that represents, configures, or manages some functionality that is provided by a system or software feature. Management agents include SNMP agents, which are applications that provide monitoring and other management functions for a computer system.

Management agent classes instantiated by the IP Manager identifies the management agent classes that can be instantiated by the IP Manager.

Table 13-12. Management agent classes instantiated by the IP Manager

Class	Available to	Description
SNMPAgent	All IP Manager products	An SNMP agent that is running in a system.
VRAgent	All IP Manager products	A refined SNMP agent that is running in a system.

Hierarchy example for management agent classes:

SNMPAgent : CIM_SNMPService : MgmtAgent : MgmtService : ApplicationService : ICIM_NetworkService : ICIM_Service : CIM_Service : CIM_EnabledLogicalElement : ICIM_LogicalElement : CIM_LogicalElement : ICIM_ManagedSystemElement : CIM_ManagedSystemElement : ICIM_ManagedElement : CIM_ManagedElement : ICF_CoreManagedElement : CORE_ManagedObject : MR_ManagedObject : MR_Object

Logical devices

A logical device is an emulation of a hardware entity that might or might not be realized in physical hardware. Logical devices include power supplies and processors; cooling devices such as fans; sensors that measure temperature or voltage characteristics of a computer system; and storage media that store data and allow data retrieval.

Logical device classes instantiated by the IP Manager identifies the logical device classes that can be instantiated by the IP Manager.

Table 13-13. Logical device classes instantiated by the IP Manager

Class	Available to	Description
Disk	IP Server Performance Manager	A disc logical device.
Fan	All but IP Availability Manager	A cooling-fan logical device.
FileSystem	IP Server Performance Manager	A file or dataset store that is local to a computer system or is remotely mounted from a file server.
Memory	All but IP Availability Manager	A memory logical device.
PowerSupply		A power-supply logical device.
Processor		A processor logical device.
TemperatureSensor		A temperature-sensor logical device.
VoltageSensor		A voltage-sensor logical device.

A feature license is required for IP Performance Manager. An additional feature license is required for IP Performance Manager to function as an IP Server Performance Manager.

Hierarchy example for logical device classes:

Disk : LogicalDisk : VMware_LogicalDisk : CIM_LogicalDisk : StorageExtent : CIM_StorageExtent : ICIM_LogicalDevice : CIM_LogicalDevice : CIM_EnabledLogicalElement : ICIM_LogicalElement : CIM_LogicalElement : ICIM_ManagedSystemElement : CIM_ManagedSystemElement : ICIM_ManagedElement : CIM_ManagedElement : ICF_CoreManagedElement : CORE_ManagedObject : MR_ManagedObject : MR_Object

Redundancy groups

A redundancy group is a logical object that contains two or more elements that participate in a redundant configuration. ECIM-R supports redundancy groups of systems, cards, network adapters, network connections, and protocol endpoints.

Redundancy group classes instantiated by the IP Manager identifies the redundancy group classes that can be instantiated by the IP Manager.

Table 13-14. Redundancy group classes instantiated by the IP Manager

Class	Available to	Description
CardRedundancyGroup	All IP Manager products	A specialized redundancy group that represents two or more cards.
NetworkAdapterRedundancyGroup	All IP Manager products	A specialized redundancy group that represents two or more network adapters.
NetworkConnectionRedundancyGroup	All IP Manager products	A specialized redundancy group that represents two or more NetworkConnections.
ProtocolEndpointRedundancyGroup	Not instantiated	
HSRPGroup	All IP Manager products	A specialized redundancy group that represents the HSRP standby group.
VRRPGroup	All IP Manager products	A specialized redundancy group that represents the VRRP standby group.
SystemRedundancyGroup	All IP Manager products	A specialized redundancy group that represents two or more systems.

Hierarchy example for redundancy group classes:

CardRedundancyGroup : RedundancyGroup : CIM_RedundancyGroup : ICIM_LogicalElement : CIM_LogicalElement : ICIM_ManagedSystemElement : CIM_ManagedSystemElement : ICIM_ManagedElement : CIM_ManagedElement : ICF_CoreManagedElement : CORE_ManagedObject : MR_ManagedObject : MR_Object

Joining two hierarchies

The physical and logical hierarchies are not independent: The objects of the physical hierarchy provide implementations for logical objects that implement features of interest in the network. The Realizes and PackagesSystems relationships joins a physical object to the logical objects for which the physical object acts as the physical embodiment or implementation.

ECIM-R topology collection sets

The IP Manager creates topology collection sets for the following satellite Domain Managers:

- MPLS Manager
- Multicast Manager
- Network Protocol Manager
- VoIP Availability Manager

  A topology collection set is represented as one or more instances of an ECIM-R topology collection class. Topology collection classes instantiated by the IP Manager identifies the topology collection classes that can be instantiated by the IP Manager.

Table 13-15. Topology collection classes instantiated by the IP Manager

Class	Available to	Description
MPLS_TopologyCollection	All IP Manager products	A collection of MPLS-related topology objects for an MPLS Manager.
MCAST_TopologyCollection	All IP Manager products	A collection of Multicast-related topology objects for a Multicast Manager.
BGP_TopologyCollection	All IP Manager products	A collection of BGP-related topology objects for a Network Protocol Manager for BGP.
EIGRP_TopologyCollection	All IP Manager products	A collection of EIGRP-related topology objects for a Network Protocol Manager for EIGRP.
ISIS_TopologyCollection	All IP Manager products	A collection of IS-IS-related topology objects for a Network Protocol Manager for IS-IS.
OSPF_TopologyCollection	All IP Manager products	A collection of OSPF-related topology objects for a Network Protocol Manager for OSPF.
VOIP_TopologyCollection	All IP Manager products	A collection of VoIP-related topology objects for a VoIP Availability Manager.
Global_TopologyCollection	All IP Manager products	A collection of related topology objects. Global_TopologyCollection is a general-purpose container for storing a set of related topology objects.

Hierarchy example for topology collection classes:

MPLS_TopologyCollection : TopologyCollection : ICIM_Collection : CORE_Collection : CORE_ManagedObject : MR_ManagedObject : MR_Object

Which topology collection instances are created depends on the particular topology collection set. For example, the IP Manager creates the following BGP_TopologyCollection instances for the Network Protocol Manager for BGP topology collection set:

- BGP-System
- BGP-Agent
- BGP-Card
- BGP-Interface
- BGP-IP
- BGP-IPNet

- BGP-NetworkConnection
- BGP-TrunkCable

  These instances consist of BGP-enabled Router and Switch objects, along with the SNMPAgent, Card, Interface, IP, IPNetwork, NetworkConnection, and TrunkCable objects that are associated with the Router and Switch objects.

  By default, the IP Manager does not create topology collection sets. The following configuration parameters in the BASEDIR/smarts/conf/discovery/tpmgr-param.conf file control whether a particular topology collection set is created:

- DisableMPLSDiscovery
- DisableMulticastDiscovery
- DisableProtocolDiscovery
- DisableVOIPDiscovery

  The VMware Smart Assurance IP Management Suite Configuration Guide describes these configuration parameters and provides instructions on modifying them.

  As explained in the configuration guide, To enable the creation of a particular topology collection set, you must set the appropriate configuration parameter to FALSE for each IP Manager.

ECIM-R relationships

ECIM-R defined relationships enable the IP Manager to associate the discovered network systems with each other, with their internal components, and with their connections. Because the relationships establish dependencies between the discovered objects, the IP Manager is able to correlate alarms from the managed objects to pinpoint the failed object, or root-cause problem, and to identify all managed objects that are affected by the failed object.

Network object relationships describes some of the relationships that can appear in the ECIM-R representation of IP network topology.

Table 13-16. Network object relationships

Relationship sets	Examples
ComposedOf/PartOf	Chassis CardCard Chassis Router InterfaceInterface Router Router MemoryMemory Router Switch PortPort Switch Switch InterfaceInterface Switch Switch CardCard Switch VLAN PortPort VLAN NetworkAdapterRedundancyGroup InterfaceInterface NetworkAdapterRedundancyGroup HSRPGroup HSRPEndpointHSRPEndpoint HSRPGroup VRRPGroup VRRPEndpointVRRPEndpoint VRRPGroup
ComposedOfVRs 1	Router Router Switch Router **Note** Identifies the virtual routers that are discovered within a physical router or switch.
ConnectedPorts 1	VLAN Port
ConnectedSystems/ConnectedVia	NetworkConnection RouterRouter NetworkConnection Cable SwitchSwitch Cable Cable RouterRouter Cable TrunkCable SwitchSwitch TrunkCable IPNetwork RouterRouter IPNetwork IPv6Network RouterRouter IPv6Network
ConnectedTo/ConnectedVia	NetworkConnection InterfaceInterface NetworkConnection Cable PortPort Cable Cable InterfaceInterface Cable TrunkCable PortPort TrunkCable IPNetwork IPIP IPNetwork IPv6Network IPv6IPv6 IPv6Network FrameRelayPVC DLCIDLCI FrameRelayPVC
ConsistsOf/MemberOf	Partition RouterRouter Partition BGP_TopologyCollection SNMPAgentSNMPAgent BGP_TopologyCollection
DuplicatedBy 1	DuplicateIP Router DuplicateIPv6 Router
HostedBy/HostsAccessPoints	MAC RouterRouter MAC IP RouterRouter IP IPv6 RouterRouter IPv6 DuplicateIP RouterRouter DuplicateIP DuplicateIPv6 RouterRouter DuplicateIPv6
HostedBy/HostsServices	SNMPAgent RouterRouter SNMPAgent HSRPEndpoint RouterRouter HSRPEndpoint VRRPEndpoint RouterRouter VRRPEndpoint

Table 13-16. Network object relationships (Continued)

Relationship sets	Examples
LayeredOver/Underlying	MAC PortPort MAC MAC InterfaceInterface MAC IP InterfaceInterface IP SNMPAgent IPIP SNMPAgent HSRPEndpoint InterfaceInterface HSRPEndpoint VRRPEndpoint InterfaceInterface VRRPEndpoint HSRPGroup RouterRouter HSRPGroup VRRPGroup RouterRouter VRRPGroup
RealizedBy/Realizes	Interface CardCard Interface Port CardCard Port
SystemPackagedIn/PackagesSystems	Router ChassisChassis Router Switch ChassisChassis Switch
1 Does not have an inverse relationship.	

The examples given here are just a few of the many relationships that can appear in the ECIM-R representation of IP network topology. Generally, as demonstrated in the examples, for every relationship, there is an inverse relationship. For example, PartOf is the reverse relationship of ComposedOf.

Configuration Settings

14

This chapter includes the following topics:

- Description of discovery.conf
- Description of tpmgr-param.conf
- Description of name-resolver.conf
- Description of partition.conf
- Description of tcat.conf
- Description of oidInfo.conf
- Description of user-defined-connections.conf
- Controlling the analysis of wide area networks
- Parameters for the SystemRestarted event
- Parameters for the ConfigChange event
- Interface-matching filters in the tpmgr-param.conf file
- Optimizing the discovery of ERX devices
- Problem Impact propagation policy over VLANs setting
- Default device access setting
- Default tagging filter groups and settings
- Possible adapter startup errors

Description of discovery.conf

The discovery.conf file contains configuration parameters that you edit to improve the performance of IP Manager discovery. The parameters are a subset of attributes that are defined for the ICF-TopologyManager object.

For parameters such as SNMPPort, you can override the value that is specified in the discovery.conf file by specifying an alternate value in a discovery filter, a seed file, or an Add Agent command.

Parameters in the discovery.conf file describes the parameters in the discovery.conf file. The parameters and their values are case-sensitive.

Table 14-1. Parameters in the discovery.conf file

Parameter	Value	Description
ipExcludeList	Regular expression Default: “” (empty string)	Use ipExcludeList to prevent certain system IP addresses from being added to the topology. By not adding the IP addresses to the topology, autodiscovery will not discover the systems that are associated with the IP addresses. A typical use of ipExcludeList is to identify IP addresses that are known to be unreachable from the management station, or are known to overlap with other systems. Use wildcards, which are described in *Appendix 15, “Wildcard Patterns,”* to specify matching patterns in the IP exclude patterns. Any IP address that matches an exclude pattern will *not* be added to the topology. The following example excludes IP addresses from the specified IP network: ipExcludeList += “10.10.9.*”
ShowPendingNONSNMP	TRUE,FALSE Default: FALSE	Controls whether non-SNMP systems that are found by autodiscovery are added to the IP Manager’s Pending Devices list or are discarded. A non-SNMP system is one that responds to ICMP polls but does not respond to SNMP polls: ■ A value of TRUE indicates that non-SNMP systems are added to the Pending Devices list. ■ A value of FALSE indicates that non-SNMP systems are discarded. **Note** Setting the value to TRUE and having autodiscovery enabled can result in adding many hosts, workstations, and other non-SNMP systems to the Pending Devices list.
LogDiscoveryProgress	TRUE,FALSE Default: FALSE	Controls whether verbose logging is used to log discovery-related messages to the IP Manager’s log file: ■ A value of TRUE enables verbose logging. ■ A value of FALSE disables verbose logging. **Note** This parameter is used mainly for debugging purposes.
defaultSNMPPort	0 to 65535 Default: 161	Specifies the default port used by the IP Manager for SNMP discovery and monitoring. You can override this value in a discovery filter, a seed file, or an Add Agent command. **Note** If 0 is specified, port 161 is used.
defaultRetries	Default: 5 retries	Number of SNMP retry polls to use during Phase 3 of discovery. Phase 3 of discovery is described in the VMware Smart Assurance IP Management Suite Discovery Guide. *“SNMP polling discovery settings” on page 56* provides recommendations about changing this value.
defaultTimeout	Default: 1000 milliseconds	Timeout for an SNMP poll during Phase 3 of discovery. Phase 3 of discovery is described in the VMware Smart Assurance IP Management Suite Discovery Guide. *“SNMP polling discovery settings” on page 56* provides recommendations about changing this value.

Table 14-1. Parameters in the discovery.conf file (Continued)

Parameter	Value	Description
defaultICMPAutoRetries	Default: 3 retries	Number of ICMP polls to try during Phase 1 of discovery. Phase 1 of discovery is described in the VMware Smart Assurance IP Management Suite Discovery Guide. *"ICMP polling discovery settings" on page 56* provides recommendations about changing this value.
defaultICMPAutoTimeout	Default: 500 milliseconds	Timeout for an ICMP poll during Phase 1 of discovery. Phase 1 of discovery is described in the VMware Smart Assurance IP Management Suite Discovery Guide. *"ICMP polling discovery settings" on page 56* provides recommendations about changing this value.
defaultICMPPacketSize	Default: 64 Bytes	The default ICMP packet size in Bytes (used during initial ICMP request. The smallest and the largest size of the ICMP packet set at the foundation level is 20 and 64 Bytes. Any value set below 20 will be reset back to a mininum of 20 Bytes and any value set above 64 will be reset back to a maximum of 64 bytes. **Note** For ICMPv4 ping packet, minimum size is 20 bytes and maximum size is 64 bytes. For ICMPv6 ping packet, minimum size is 32 bytes and maximum size is 64 bytes. By default, both ICMPv4 and ICMPv6 ping packet have 64 bytes set. The defaultICMPPacketSize variable controls ICMP ping packet size for both IPv4 and IPv6 ping packet. Needs Server restart.
defaultSNMPAutoRetries	Default: 3 retries	Number of SNMP polls to try during Phase 1 of discovery. Phase 1 of discovery is described in the VMware Smart Assurance IP Management Suite Discovery Guide. *"SNMP polling discovery settings" on page 56* provides recommendations about changing this value.
defaultSNMPAutoTimeout	Default: 1000 milliseconds	Timeout for an SNMP poll during Phase 1 of discovery. Phase 1 of discovery is described in the VMware Smart Assurance IP Management Suite Discovery Guide. *"SNMP polling discovery settings" on page 56* provides recommendations about changing this value.
numberProbeThreads	Default: 10 threads	Number of discovery threads that are used by the discovery process. If you are experiencing slow response SNMP discovery polling and your current CPU usage is relatively low (5 to 10 percent), consider increasing the number of discovery threads to improve your discovery performance. Increasing this number is one of the best and simplest methods for improving discovery. Increasing the number of discovery threads to 20, 30, or even 50 is acceptable, but remember that more threads might require additional or more capable CPUs, and that the requirements during discovery will increase. Increase discovery threads conservatively while monitoring SNMP Processing Statistics changes, as described in the VMware Smart Assurance IP Manager Deployment Guide.

Table 14-1. Parameters in the discovery.conf file (Continued)

Parameter	Value	Description
numberShortProbeThreads	Default: 7 threads	Number of discovery threads that are used by the short discovery process. If you increase the number of short discovery threads, use small increments and monitor your current CPU usage. Increasing the number of threads will increase the CPU usage. The short discovery process is independent of the main discovery process. Both may occur simultaneously. Short discovery handles SNMP MIB index changes, which typically occur during device restarts. In addition, SNMP MIB index changes occur for components that use fluid index values; for example, IPSec tunnel endpoints. Short discovery is described in the VMware Smart Assurance IP Management Suite Discovery Guide.
ICMPSleepTime	0 to 100 milliseconds Default: 0	Interval between successive ICMP poll requests. During the initial discovery phase, the IP Availability Manager sends large bursts of ICMP polls. If ICMP has a low priority, the network is congested, or the routers on the path are experiencing high processor utilization, a number of these ICMP packets may be dropped. As a result, the IP Manager receives a limited number of ICMP responses, which causes a number of systems that might otherwise be successfully discovered to be placed on the Pending Devices list as UNDISCOVERED. Other symptoms of packet loss include DiscoveryError notifications for systems that were previously discovered successfully and the full topology is not discovered after two full discoveries. Increasing the sleep time increases the amount of time between ICMP polls. You can specify a value between 0 and 100 milliseconds. A value of 100 milliseconds translates to 10 ICMP polls per second. Specifying a long sleep time can significantly prolong the discovery process. Estimate the total additional time by multiplying the sleep time by the number of IP addresses to be processed.
defaultReadCommunity	Default: public	Read-only community string used by the IP Manager when no community string is specified in the Community Strings field in the Topology tab of the Domain Manager Administration Console. The Community Strings field is described in the VMware Smart Assurance IP Management Suite Discovery Guide. If you do not want the IP Manager to use a default community string during discovery, you must remove "public" from the Community Strings field and from this parameter.
MaximumCommunities	Default: 4 strings	Number of read-only community strings that can be specified in the Community Strings field in the Topology tab of the Domain Manager Administration Console. The Community Strings field is described in the VMware Smart Assurance IP Management Suite Discovery Guide. Change this value to address networks with more than four different read-only community strings.

Table 14-1. Parameters in the discovery.conf file (Continued)

Parameter	Value	Description
MaximumSNMPV3Credentials	Default: 4	Number of SNMPV3 fallback credentials that can be specified in the SNMPV3 Credentials in the Topology tab of the Domain Manager Administration Console. This value can be changed to address networks which have more than 10 different SNMPV3 Credentials.
LicenseThresholdPercentage	Default: 90%	Determines the *LowOnSystemLicense* event. **Note** This attribute is common for System volume, WirelessAccessPoint, and WirelessClients. The default value is set at 90 %. The total number of systems that can be discovered with the available license blocks is calculated based on the value. For example, for four blocks of licenses and considering one block size = 50 devices, a total of 200 devices (50*4) can be discovered. Once the total number of systems reach 90 % of 200 devices, the *LowOnSystemLicense* event is generated.
MaximumHostBits	Default: 8 bits	Number of host bits in the netmask that is used by autodiscovery to find additional discovery candidate systems. The default value of 8 corresponds to a netmask of 255.255.255.0. If, for example, your network includes systems with a netmask of 255.255.254.0, these systems will not be found by autodiscovery. Modify the default value of the MaximumHostBits parameter with caution because as you increase the value, so do you increase the number of ICMP polls that are generated during every discovery. VMware recommends that you set the value only as high as needed. If necessary, modify the value during the initial topology discovery. Once the devices are discovered, lower the value so that subsequent pending and full discoveries do not attempt to look beyond the default netmask. This modification will not affect systems that have already been discovered. For example, the default value of 8 provides a maximum of 254 host IP addresses. A value of 16 provides a maximum of 65,534 host IP addresses. 192.168.1.1/24 = 8 host bits 192.168.1.1/18 = 14 host bits 192.168.1.1/16 = 16 host bits 192.168.1.1/8 = 24 host bits Valid values range from 2 to 24. If a value greater than 24 is specified, a value of 8 is used.

Table 14-1. Parameters in the discovery.conf file (Continued)

Parameter	Value	Description
AccessAddressFormat	AUTOADDRESS,LOOPBACKADDRESS Default: AUTOADDRESS	Determines how the discovery process obtains an IP address to communicate with discovered systems. This address is used for ICMP and SNMP polls during discovery and for monitoring and analysis. Valid values are AUTOADDRESS and LOOPBACKADDRESS. AUTOADDRESS means that all the IP addresses of a device are polled using ICMP. If a device has more than ten IP addresses, only ten of the IP addresses are polled using SNMP. The addresses to be polled by SNMP are chosen as follows: ■ IP address is managed and is not a duplicate ■ InterfaceMode of the IP, if any, is NORMAL ■ If the system has more than ten IP addresses, the first ten IP addresses are chosen in the following manner: IP addresses of type SOFTWARELOOPBACK, ETHERNET, TOKENRING, and GENERIC are chosen first in the order that the IP addresses appear in the IP address table (ipAddrTable). IP addresses of type GENERIC must not have a netmask of 255.255.255.252. The remaining IP addresses are chosen in the order that they appear in the IP address table. LOOPBACKADDRESS means that the discovery process uses the loopback address for both ICMP and SNMP for monitoring and discovery. (MIB-II ifType 24). Note that discovery cannot determine the loopback address until after the system has been discovered. **Note** If a qualified IP address is not found, the last known SNMP address is used and a DiscoveryError is notified. The DiscoveryError contains the message: Qualified access address not found.
DisplayNameFormat	AUTOASSIGNED,MIBIISYSNAME Default: AUTOASSIGNED	Determines how the discovery process populates the DisplayName attribute of a system. Valid values are AUTOASSIGNED and MIBIISYSNAME. AUTOASSIGNED means that the DisplayName of a system is set to the value of the Name attribute of the system. By using the NameFormat parameter, which is described in Table 127 on page 243, you can control how the value of the Name attribute is determined. Also, for AUTOASSIGNED, you can change the value of DisplayName by using dmctl or an Adapter Scripting Language (ASL) script. The value of DisplayName is not retained across subsequent discoveries. MIBIISYSNAME means that the DisplayName of a system is set to the value of the MIB-II sysName variable. Any change to the DisplayName by using dmctl or an ASL script is not retained across subsequent discoveries.

Table 14-1. Parameters in the discovery.conf file (Continued)

Parameter	Value	Description
HSRPEnabled	TRUE,FALSE Default: TRUE	Enables or disables Hot Standby Router Protocol (HSRP) discovery, monitoring, and analysis: ■ A value of TRUE enables HSRP discovery, monitoring, and analysis. ■ A value of FALSE disables HSRP discovery, monitoring, and analysis.
VRRPEnabled	TRUE,FALSE Default: TRUE	Enables or disables Virtual Router Redundancy Protocol (VRRP) discovery, monitoring, and analysis: ■ A value of TRUE enables VRRP discovery, monitoring, and analysis. ■ A value of FALSE disables VRRP discovery, monitoring, and analysis.
HostResourcesEnabled	TRUE,FALSE Default: TRUE	Enables or disables host resources discovery and monitoring: ■ A value of TRUE enables host resources discovery and monitoring. ■ A value of FALSE disables host resources discovery and monitoring.
VirtualRouterEnabled	TRUE,FALSE Default: TRUE	Enables or disables virtual router discovery and monitoring: ■ A value of TRUE enables virtual router discovery and monitoring. ■ A value of FALSE disables virtual router discovery and monitoring.
MinimumDemandGet	TRUE,FALSE Default: FALSE	Controls whether to allow only minimum Demand Get requests or to allow all Demand Get requests: ■ A value of TRUE allows only minimum Demand Get requests. ■ A value of FALSE allows all Demand Get requests. Setting this parameter to TRUE optimizes discovery performance by avoiding unnecessary Demand Get requests.

Table 14-1. Parameters in the discovery.conf file (Continued)

Parameter	Value	Description
DuplexAssumed	TRUE,FALSE Default: TRUE	Controls how to set the duplex mode for network adapters (ports or interfaces) in the topology. Valid values are TRUE and FALSE. ■ A value of TRUE indicates that duplex mode is assumed for all network adapters regardless of whether duplex mode can be determined by checking the MIBs. ■ A value of FALSE indicates that duplex mode is set only for the network adapters for which duplex mode can be determined by checking the MIBs. As further clarification, a value of TRUE means that the IP Manager will calculate current utilization for all ports and interfaces in the topology regardless of whether their duplex mode can be determined by checking the MIBs. For any port or interface whose duplex mode cannot be determined by checking the MIBs, the IP Manager sets the port's/interface's DuplexMode attribute to FULLDUPLEX and its DuplexSource attribute to ASSUMED. The one exception is the 10 megabit (Mb) Ethernet adapter, for which the IP Manager sets the adapter's DuplexMode attribute to HALFDUPLEX. A value of FALSE means that the IP Manager will calculate only current utilization for those ports or interfaces that can be determined as full-duplex or half-duplex by reading the Enterprise MIB, ETHERLIKE-MIB, and Neighbor MIB. Any port or interface having an unspecified duplex mode setting will be ignored. Be aware that calculating current utilization for all ports and interfaces (DuplexAssumed = TRUE) requires considerable system resources. Ensure that your server is sized properly to accommodate the size of your environment, as described in the VMware Smart Assurance IP Manager Deployment Guide. The VMware Smart Assurance IP Performance Manager and Server Performance Manager User Guide provides more information about duplex mode and current utilization calculations.
importExternalTagsConnections	TRUE,FALSE Default: FALSE	Controls whether MPLS tags and connections are imported by the IP Manager from MPLS Manager. ■ A value of TRUE indicates that the MPLS tags and connections are imported by the IP Manager. ■ A value of FALSE indicates that the MPLS tags and connections are not imported by the IP Manager. The VPN-Tagging Server is described in the VMware Smart Assurance MPLS Manager Discovery Guide Supplement.

Table 14-1. Parameters in the discovery.conf file (Continued)

Parameter	Value	Description
autoReprobe_short	TRUE,FALSE Default: FALSE	Enables or disables short discovery: ■ A value of TRUE enables short discovery. ■ A value of FALSE disables short discovery. The short discovery process is independent of the main discovery process. Both may occur simultaneously. Short discovery handles SNMP MIB index changes, which typically occur during device restarts. In addition, SNMP MIB index changes occur for components that use fluid index values; for example, IPSec tunnel endpoints.Short discovery is described in the VMware Smart Assurance IP Management Suite Discovery Guide.
reprobePeriod_short	60 or more seconds Default: 900 seconds	Interval between successive short discoveries. If you decrease the short discovery interval, use small decrements and monitor your current CPU usage. Decreasing the interval will increase the CPU usage. Short discovery is described in the VMware Smart Assurance IP Management Suite Discovery Guide.
WIFI_reprobePeriod_short	Default Value = 3600 seconds	Interval between successive WIFI short discoveries. If you decrease the short discovery interval, use small decrements and monitor your current CPU usage. Decreasing the interval will increase the CPU usage. Value should be more than 300, else 300 will be considered. Needs server restart.
DiscoveryAddrPref	IPV6FIRST_IPV4NEXT,IPV4FIRST_IPV6NEXT,IPV6_ADDRONLY, orIPV4_ADDRONLY Default: IPV6FIRST_IPV4NEXT	Controls the order of addresses in the list of IP addresses that are found on a discovered system, where the preferred addresses (IPv6 or IPv4) are first in the list. Valid values are: ■ IPV6FIRST_IPV4NEXT IPv6 addresses are first in the list, followed by IPv4 addresses. ■ IPV4FIRST_IPV6NEXT IPv4 addresses are first in the list, followed by IPv6 addresses. ■ IPV6_ADDRONLY Only IPv6 addresses are in the list. ■ IPV4_ADDRONLY Only IPv4 addresses are in the list. The DiscoveryAddrPref parameter influences how the discovery process names a discovered system, as explained in the VMware Smart Assurance IP Management Suite Discovery Guide. When IPv6 is the preferred address, the global unicast address and the addresses that begin with 3FFE:* take precedence.
SNMPGetBulkEnabled	TRUE,FALSE Default: TRUE	Enables or disables SNMP getBulk for device discovery: ■ A value of TRUE enables SNMP getBulk for device discovery ■ A value of FALSE disables SNMP getBulk for device discovery.

Table 14-1. Parameters in the discovery.conf file (Continued)

Parameter	Value	Description
STPVLANNamingEnabled	TRUE,FALSE Default: TRUE	STP based VLAN unique naming discovery is enabled by incorporating the root bride ID as part of the VLAN name. It is set to TRUE (by default) to enable VLAN unique naming by incorporating STP root bridge ID as part of the VLAN name during IP Manager discovery. If it is set to FALSE, the STP root bridge ID will not be included in the VLAN name.
WIFIEnabled	TRUE,FALSE Default: TRUE	Enables or disables wireless device discovery. To enable wireless device discovery, set the flag WIFIEnabled = TRUE. Disabling the Wifi discovery through the “WIFIEnabled” flag and doing a Discover All removes all the wireless components, for example, Wireless Access Points, Clients, and SSID, which were discovered earlier.
WIFI_autoReprobe_Short **Note** Server restart is required.	Default value: FALSE ■ TRUE — Enables WIFI related short discovery. ■ FALSE— Disables WIFI related short discovery.	Enables or disables WIFI related short discovery. Short discovery handles Wireless Topology changes, which typically occur during WirelessClient movement. In addition, dynamically detects Rogue Wireless APs.

Description of tpmgr-param.conf

The tpmgr-param.conf file contains configuration parameters that you edit to customize IP Manager discovery. The parameters are a subset of table entries that are defined for the ICF-TopologyManager object.

Use the parameters in this file to accomplish such tasks as disabling the discovery of certain interfaces or ports, enabling the discovery of topology collection sets for satellite Domain Managers, and changing the operation of the IP Manager to be backward compatible with earlier versions of satellite Domain Managers.

Parameters in the tpmgr-param.conf file describes the parameters in the tpmgr-param.conf file.

Note The parameters and their values are case-sensitive.

Table 14-2. Parameters in the tpmgr-param.conf file

Parameter	Value	Description
EnableShadowIP	TRUE,FALSE Default: TRUE	Controls whether shadow IP objects and shadow IPNetwork objects are created: ■ A value of TRUE indicates that shadow objects are created. ■ A value of FALSE indicates that shadow objects are not created. This parameter is used for backward compatibility so that the current version of the IP Manager is able to work with earlier versions of satellite Domain Managers.
Interface pattern filters	Not applicable	Filters that prevent the IP Manager from creating certain interfaces for certain discovered devices. Interface pattern filters are described in *Chapter 7, "Excluding Device-Access Interfaces."*
EnableTunnelHeuristic	TRUE,FALSE Default: FALSE	Controls whether the IP Manager uses a certain method, or heuristic, to create tunnel connections: ■ A value of TRUE indicates that the IP Manager uses the method to create tunnel connections. ■ A value of FALSE indicates that the IP Manager does not use the method to create tunnel connections. The EnableTunnelHeuristic parameter provides a method to create tunnel connections between tunnel endpoints by matching tunnel logical interfaces; for example, create a tunnel connection *between* tunnel endpoint A on Router A *and* tunnel endpoint B on Router B, where each tunnel endpoint has the same tunnel logical interface, say 1234. The EnableTunnelHeuristic parameter was introduced at a time when enterprise MIB support for the tunneling technologies, such as Internet Protocol Security (IPSec), Internet Key Exchange (IKE), and Generic Routing Encapsulation (GRE), was not available. Now that enterprise MIB support is available for the tunneling technologies, you should accept the default value for this parameter.
EnableClearByLinkUp	TRUE,FALSE Default: FALSE	Controls whether LinkUp traps set the OperStatus to UP: ■ A value of TRUE indicates that LinkUp traps set the OperStatus to UP. ■ A value of FALSE indicates that LinkUp traps do not set the OperStatus to UP.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
DisableProtocolDiscovery	TRUE,FALSE Default: TRUE	Controls whether the IP Manager identifies routing-protocol-enabled devices and creates routing-protocol topology collection sets for import by the VMware Smart Assurance Network Protocol Manager: ■ A value of TRUE indicates that the IP Manager does not identify routing-protocol-enabled devices and does not create network-protocol topology collection sets. ■ A value of FALSE indicates that the IP Manager identifies routing-protocol-enabled devices and creates network-protocol topology collection sets. For Network Protocol Manager for BGP, the IP Manager stores the BGP topology collection set in instances of the BGP_TopologyCollection class. For Network Protocol Manager for OSPF, the IP Manager stores the OSPF topology collection set in instances of the OSPF_TopologyCollection class. For Network Protocol Manager for EIGRP, the IP Manager stores the EIGRP topology collection set in instances of the EIGRP_TopologyCollection class. For Network Protocol Manager for IS-IS, the IP Manager stores the IS-IS topology collection set in instances of the ISIS_TopologyCollection class. By importing a routing-protocol topology collection set, Network Protocol Manager will probe only those devices that support the relevant routing protocol, which significantly reduces the discovery time for Network Protocol Manager. *“Enabling light discovery for satellite Domain Managers” on page 61* clarifies the use of the DisableProtocolDiscovery parameter.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
DisableMPLSDiscovery	TRUE,FALSE Default: TRUE	Controls whether the IP Manager identifies MPLS-enabled devices and creates an MPLS topology collection set for import by VMware Smart Assurance MPLS Manager: ■ A value of TRUE indicates that the IP Manager does not identify MPLS-enabled devices and does not create an MPLS topology collection set. ■ A value of FALSE indicates that the IP Manager identifies MPLS-enabled devices and creates an MPLS topology collection set. The IP Manager stores the MPLS topology collection set in instances of the MPLS_TopologyCollection class. By importing an MPLS topology collection set, MPLS Manager will probe only those devices that support MPLS, which significantly reduces the discovery time for MPLS Manager. *"Enabling light discovery for satellite Domain Managers" on page 61* clarifies the use of the DisableMPLSDiscovery parameter.
DisableOverlappingIP	TRUE,FALSE Default: TRUE	Controls whether the IP Manager discovers MPLS-related VPN routing and forwarding (VRF) IP addresses and performs IP tagging: ■ A value of TRUE indicates that the IP Manager does not discover VRF IP addresses and thus does not perform IP tagging. ■ A value of FALSE indicates that the IP Manager discover s VRF IP addresses and performs IP tagging. When DisableOverlappingIP = FALSE, all discovered VRF IP objects are subject to IP tagging.
PollableMPLSOids	.1.3.6.1.3.96.1.9.1.8|. 1.3.6.1.2.1.10.166.2.1.10. 1.9|. 1.3.6.1.4.1.2636.3.2.3.1.2| .1.3.6.1.3.118.1.2.1.1.2	List of MPLS OID's required to be polled in order to create a MPLS topology collection. Use the syntax below, separating each entry with a PIPE(|)] while adding new OID's in to below list. PollableMPLSOids .1.3.6.1.3.96.1.9.1.8|. 1.3.6.1.2.1.10.166.2.1.10.1.9|. 1.3.6.1.4.1.2636.3.2.3.1.2|.1.3.6.1.3.118.1.2.1.1.2
UseCDPEthernetConnection	TRUE,FALSE Default: TRUE	Controls whether the IP Manager creates interface-to-interface connections between two devices that are Cisco Discovery Protocol (CDP) neighbors across LAN segments: ■ A value of TRUE indicates that the IP Manager creates connections between the CDP-peer interfaces. ■ A value of FALSE indicates that the IP Manager does not create connections between the CDP-peer interfaces.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
UserDefinedConnectionsOverwrite	TRUE,FALSE Default: FALSE	Controls whether user-defined connections overwrite discovered connections: ■ A value of TRUE indicates that user-defined connections overwrite discovered connections. ■ A value of FALSE indicates that user-defined connections do not overwrite discovered connections.
masklistPattern	Default: {32,30,29,28,27,26,25,24,16,8}	Range of IPv4 subnetworks to try to find the best routing match.
EnableARPHeuristicForVPNIP	TRUE,FALSE Default: FALSE	Controls whether the IP Manager uses the ARP method, or heuristic, to find VPN-IPs (VRF IPs) that are not available in the IP address table (ipAddrTable): ■ A value of TRUE indicates that the IP Manager uses the ARP method to find VPN-IPs that are unavailable in the IP address table. ■ A value of FALSE indicates that the IP Manager does not use the ARP method to find VPN-IPs that are unavailable in the IP address table. For a Provider Edge (PE) or multi-VRF Customer Edge (CE) device, multiple instances of the *same* IP address might be bound to different VPN routing and forwarding (VRF) tables on the device. When the EnableARPHeuristicForVPNIP parameter is set to TRUE, the IP Manager accesses the device's Address Resolution Protocol (ARP) table MIB to find and instantiate multiple instances of that same IP address. Prerequisites for setting EnableARPHeuristicForVPNIP to TRUE: ■ Overlapping IP address discovery is enabled.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
IgnoreIPForPersistentMgmtState	TRUE,FALSE Default: FALSE	Controls whether the IP Manager compares the IP and MAC sets of newly discovered systems with the IP and MAC sets of existing systems, to determine whether a newly discovered system is a duplicate of an existing system (an already discovered system) or is in fact a new system: ■ A value of TRUE indicates that the IP Manager does not compare the IP and MAC sets of newly discovered systems with the IP and MAC sets of existing systems. ■ A value of FALSE indicates that the IP Manager compares the IP and MAC sets of newly discovered systems with the IP and MAC sets of existing systems. When the IgnoreIPForPersistentMgmtState parameter is set to TRUE, the IP Manager uses a method other than the comparison of IP and MAC sets to determine whether a newly discovered system is a duplicate system or a new system. The IP Manager discards any newly discovered system that is a duplicate. And, for a newly discovered system that is a duplicate but has a different resolved name because of a different DNS entry or a different sysName, the IP Manager uses that name to rename the existing device.
AllowNonPrivateIPAsName	TRUE,FALSE Default: TRUE	Controls whether a nonprivate IP address is to be used as the name for the NameFormat TM_USENONPRIVATEIP parameter in case nonprivate IPs cannot be resolved: ■ A value of TRUE indicates that a nonprivate IP address is to be used as the name for the NameFormat TM_USENONPRIVATEIP parameter in case nonprivate IPs cannot be resolved. ■ A value of FALSE indicates that a nonprivate IP address is not to be used as the name for the NameFormat TM_USENONPRIVATEIP parameter in case nonprivate IPs cannot be resolved. The NameFormat TM_USENONPRIVATEIP parameter is an AutoNameOrder parameter that is described in Description of tpmgr-param.conf. A nonprivate IP address is 10.x.x.x or 192.168.x.x.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
AllowPrivateIPAsName	TRUE,FALSE Default: FALSE	Controls whether a private IP address is to be used as the name for the NameFormat TM_USEPRIVATEIP parameter in case private IPs cannot be resolved: ■ A value of TRUE indicates that a private IP address is to be used as the name for the NameFormat TM_USEPRIVATEIP parameter in case private IPs cannot be resolved. ■ A value of FALSE indicates that a private IP address is not to be used as the name for the NameFormat TM_USEPRIVATEIP parameter in case private IPs cannot be resolved. The NameFormat TM_USEPRIVATEIP parameter is an AutoNameOrder parameter that is described in Description of tpmgr-param.conf.
AllowAllLocalInterfaceIPs	TRUE,FALSE Default: FALSE	Controls whether a local IP is to be discovered from the ipNetToMediaPhysAddress MIB: ■ A value of TRUE indicates that a local IP is to be discovered from the ipNetToMediaPhysAddress MIB. ■ A value of FALSE indicates that a local IP is not to be discovered from the ipNetToMediaPhysAddress MIB.
DiscoverCiscoTrunkPortVLANs	TRUE,FALSE Default: TRUE	Enables or disables the discovery of VLANs for which trunk ports on the discovered system are enabled: ■ A value of TRUE enables the discovery of VLANs for which trunk ports are enabled. ■ A value of FALSE disables the discovery of VLANs for which trunk ports are enabled. When the DiscoverCiscoTrunkPortVLANs parameter is set to TRUE, only *configured* VLANs for which trunk ports are enabled on the discovered system are discovered. Non-configured VLANs for which trunk ports are enabled are not discovered. Trunk ports are defined in Port Groups - Trunk Ports.
PropagateVRIfAlias	TRUE,FALSE Default: FALSE	Enables or disables the concatenation of the InterfaceAlias fields of the virtual routers on a Juniper ERX physical router into the InterfaceAlias field of the main router: ■ A value of TRUE enables the concatenation of the InterfaceAlias fields. ■ A value of FALSE disables the concatenation of the InterfaceAlias fields.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
LogDNSFailure	TRUE,FALSE Default: FALSE	Enables or disables the logging of error messages to the IP Manager's log file for a device (loopback) IP address that cannot be resolved to a name by the Domain Name System (DNS) during the initial phase of discovery: ■ A value of TRUE enables the logging of error messages for a device IP address that cannot be resolved to a name through DNS during autodiscovery. ■ A value of FALSE disables the logging of error messages for a device IP address that cannot be resolved to a name through DNS during autodiscovery.
ERXRtrUseDefaultComm	TRUE,FALSE Default: FALSE	Enables or disables the appending of '@default' to the community string that is used to query ERX physical routers: ■ A value of TRUE enables the appending of '@default' to the community string that is used to query ERX physical routers. ■ A value of FALSE disables the appending of '@default' to the community string that is used to query ERX physical routers.
EnableERXMainRouterIFDiscovery	TRUE,FALSE Default: TRUE	Enables or disables interface discovery for the main router of Juniper ERX physical routers: ■ A value of TRUE enables interface discovery for the ERX main router. ■ A value of FALSE disables interface discovery for the ERX main router.
OITrapAdapterHost	Default: localhost	The name or IP address of the host system where the SNMP Trap Adapter that is configured as a trap receiver is running. *"Enabling the SystemRestarted event" on page 65* and *"Enabling the ConfigChange event" on page 68* clarify the use of this parameter.
OITrapAdapterPort	Default: 162	The port on the host system where the SNMP Trap Adapter that is configured as a trap receiver is running. *"Enabling the SystemRestarted event" on page 65* and *"Enabling the ConfigChange event" on page 68* clarify the use of this parameter.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
EnableConfigChange	TRUE,FALSE Default: FALSE	Controls whether the IP Manager generates ConfigChange events: ■ A value of TRUE indicates that the IP Manager generates ConfigChange events. ■ A value of FALSE indicates that the IP Manager does not generate ConfigChange events. When the IP Manager generates a ConfigChange event, it adds the device that caused the event to the Pending Devices list. *“Enabling the ConfigChange event” on page 68* clarifies the use of this parameter.
EnableSystemRestart	TRUE,FALSE Default: FALSE	Controls whether the IP Manager generates SystemRestarted events: ■ A value of TRUE indicates that the IP Manager generates SystemRestarted events. ■ A value of FALSE indicates that the IP Manager does not generate SystemRestarted events. When the IP Manager generates a SystemRestarted event, it adds the device that caused the event to the Pending Devices list. *“Enabling the SystemRestarted event” on page 65* clarifies the use of this parameter.
EnableNonSlash30IPs	TRUE,FALSE Default: FALSE	Controls whether the IP Manager creates Layer 2 (L2) network connection when CidrRoute is used as the neighbor probe: ■ A value of TRUE indicates that the IP Manager creates an L2 network connection when CidrRoute is used as the neighbor probe. ■ A value of FALSE indicates that the IP Manager does not create an L2 network connection when CidrRoute is used as the neighbor probe.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
DisableMulticastDiscovery	TRUE,FALSE Default: TRUE	Controls whether the IP Manager identifies Multicast-enabled devices and creates a Multicast topology collection set for import by VMware Smart Assurance Multicast Manager: ■ A value of TRUE indicates that the IP Manager does not identify Multicast-enabled devices and does not create a Multicast topology collection set. ■ A value of FALSE indicates that the IP Manager identifies Multicast-enabled devices and creates a Multicast topology collection set. The IP Manager stores the Multicast topology collection set in instances of the MCAST_TopologyCollection class. By importing a Multicast topology collection set, Multicast Manager will probe only those devices that support the Multicast protocol, which significantly reduces the discovery time for Multicast Manager. *“Enabling light discovery for satellite Domain Managers” on page 61* clarifies the use of the DisableMulticastDiscovery parameter.
ProtocolInterfaceDisabledAlarm	TRUE,FALSE Default: FALSE	Controls whether the IP Manager generates NetworkDeviceConnection Disabled notifications: ■ A value of TRUE indicates that the IP Manager generates NetworkDeviceConnection Disabled notifications. ■ A value of FALSE indicates that the IP Manager does not generate NetworkDeviceConnection Disabled notifications.
EnableDNSLookupInReconfigure	TRUE,FALSE Default: FALSE	Controls the DNS lookup during a reconfiguration: ■ A value of TRUE indicates that DNS lookup is used during a reconfiguration. ■ A value of FALSE indicates that DNS lookup is not used during a reconfiguration. A value of FALSE improves discovery time. If you have frequent DNS changes and a full discovery takes a long time, you can set the value to TRUE to synchronize the AgentAddressList. A value of TRUE in combination with a misconfigured DNS can result in a long discovery time and possibly incorrect results.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
EnableIPSecDiscovery	TRUE,FALSE Default: FALSE	Enables or disables the discovery of IPSec tunnels: ■ A value of TRUE enables the discovery of IPSec tunnels. ■ A value of FALSE disables the discovery of IPSec tunnels. Discovery of IPSec tunnels is described in the VMware Smart Assurance IP Management Suite Discovery Guide.
EnableJapaneseCharacterEncode	TRUE FALSE Default: FALSE	Enables or disables the transcoding of SJIS encoded Japanese Characters to Unicode UTF-8 encoded characters: ■ A value of TRUE enables the transcoding of SJIS encoded Japanese Characters to Unicode UTF-8 encoded characters. ■ A value of FALSE disables the transcoding of SJIS encoded Japanese Characters to Unicode UTF-8 encoded characters.
FallbackInterfaceMonitoringToMIB2	TRUE FALSE Default: FALSE	Controls whether the IP Manager monitors interface performance for a device when the following two conditions are in effect: ■ Interfaces have maximum speed (MaxSpeed) greater than 20 megabits per second (Mbps). ■ No 64-bit counters are available in the device's MIB. Valid values are TRUE and FALSE: ■ A value of TRUE forces the IP Manager to use 32-bit counters to monitor greater-than-20-Mbps interfaces when 64-bit counters are not available in the MIB. ■ A value of FALSE allows the IP Manager to resort to its default behavior: Do not monitor greater-than-20-Mbps interfaces when 64-bit counters are not available in the MIB. When you set the value to TRUE, and no 64-bit counters are available in the MIB, the IP Manager will monitor interfaces within a MaxSpeed range of greater than 20 Mbps and less than 100 Mbps. **Note** When 64-bit counters (high-capacity octets) are present, MIB-II and MIB-II IF-MIB instrumentation is implemented. When 64-bit counters are not present, only MIB-II instrumentation is implemented.
MonitorHostGigaInterfaceByMIB2	TRUE FALSE Default: FALSE	If the MIB table (64 bit octet) counters are empty and the values for the FallbackInterfaceMonitoringToMIB2 and MonitorHostGigaInterfaceByMIB2 parameters are set to TRUE, then system will force all host GB interfaces to be instrumented by MIB2. This option work only for HOST interfaces.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
OmitIPPhonePort	TRUE FALSE Default: FALSE	Controls whether the IP Manager discovers Cisco switch ports that are connected to a Cisco IP phone: ■ A value of TRUE indicates that the IP Manager does not discover Cisco switch ports that are connected to a Cisco IP phone. ■ A value of FALSE indicates that the IP Manager discovers Cisco switch ports that are connected to a Cisco IP phone.
OmitEmptyPort	TRUE FALSE Default: FALSE	Controls whether the IP Manager discovers Cisco switch ports that have no connection or do not connect to anything: ■ A value of TRUE indicates that the IP Manager does not discover Cisco switch ports that have no connection. ■ A value of FALSE indicates that the IP Manager discovers Cisco switch ports that have no connection.
UseifLinkUpDownTrapEnable	TRUE FALSE Default: FALSE	Controls whether the IP Manager uses the value of ifLinkUpDownTrapEnable (.1.3.6.1.2.1.31.1.1.1.14) to manage or unmanage Cisco switch ports: ■ A value of TRUE indicates that the IP Manager uses the value of ifLinkUpDownTrapEnable to manage or unmanage Cisco switch ports. ■ A value of FALSE indicates that the IP Manager does not use the value of ifLinkUpDownTrapEnable to manage or unmanage Cisco switch ports.
DisablePerfProbeInDiscoveryMgrMode	TRUE FALSE Default: TRUE	Controls whether the IP Manager invokes performance probes at startup: ■ A value of TRUE indicates that the IP Manager does not invoke performance probes at startup. ■ A value of FALSE indicates that the IP Manager invokes performance probes at startup.
EnableEthernetBonding	TRUE FALSE Default: TRUE	Controls whether the IP Manager creates system-level connections, based on CDP and Bridge MIB data, for Linux bonded logical interfaces that are connected to multiple ports: ■ A value of TRUE indicates that the IP Manager creates system-level connections for the Linux bonded logical interfaces that are connected to multiple ports. ■ A value of FALSE indicates that the IP Manager does not create system-level connections for Linux bonded logical interfaces that are connected to multiple ports.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
DisableSystemLevelBackPlane-NetworkConnection	TRUE FALSE Default: TRUE	Controls whether the IP Manager creates system-level connections for backplane-connected cards: ■ A value of TRUE indicates that the IP Manager does not create system-level connections for backplane-connected cards. ■ A value of FALSE indicates that the IP Manager creates system-level connections for backplane-connected cards. The Global Manager includes the system-level connections in Physical Connectivity maps in order to show the relationship between backplane-connected cards and the physical packages that enclose the cards. For example, to show the relationship between a route switch module (RSM) card and the Cisco 6509 Catalyst switch that encloses the RSM.
EnableUnmanageAdminDown	TRUE FALSE Default: FALSE	Enables or disables the Unmanaged Administratively Down feature: ■ A value of TRUE enables the Unmanaged Administratively Down feature: the IP Manager does not discover IP objects that are layered over an administratively down interface. ■ A value of FALSE disables the Unmanaged Administratively Down feature: the IP Manager discovers IP objects that are layered over an administratively down interface. When the Unmanaged Administratively Down feature is enabled, the DisableOverlappingIP parameter in the tpmgr-param.conf file should be set to TRUE (default) to disable the IP tagging feature. The VMware Smart Assurance IP Management Suite Discovery Guide provides more information about the Unmanaged Administratively Down feature.
GroupLoopBackInterfaces	TRUE FALSE Default: FALSE	Controls whether the IP Manager creates loopback interface (iftype=24) groups: ■ A value of TRUE indicates that the IP Manager creates loopback interface groups. The IP Manager stores the loopback interface groups in instances of the LoopBack_InterfaceCollection class. ■ A value of FALSE indicates that the IP Manager does not create loopback interface groups.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
NetSNMPUseHostResourceForMemory	TRUE FALSE Default: FALSE	This flag applies to NetSNMP Agent discovery. It controls the memory instance creation for the host when the memory information is present in both NetSNMP MIB as well as Host Resources MIB. ■ A value of TRUE indicates that the Host Resource MIB is used to create the memory instance. ■ A value of FALSE indicates that the NetSNMP MIB is used to create the memory instance. The memory details in the vendor-specific MIB (compaq) takes precedence over Host Resources MIB. This flag is used to resolve the precedence between Host Resource MIB and NetSNMP MIB.
NoOfAccessPortBridgesMAC	Default: 1	If the number of *Bridges* (MAC) relationships for a port equals or exceeds the value of the NoOfAccessPortBridgesMAC parameter, the IP Manager identifies the port as a trunk port, as opposed to an access port. The purpose of this parameter is to enable the IP Manager to identify trunk ports more quickly. Trunk ports are defined in Port Groups - Trunk Ports. **Note** NoOfAccessPortBridgesMAC should remain 1 and should not be removed from the tpmgr-param.conf file.
DisableVOIPDiscovery	TRUE,FALSE Default: TRUE	Controls whether the IP Manager identifies VoIP-enabled devices and creates a VoIP topology collection set for import by VMware Smart Assurance VoIP Availability Manager: ■ A value of TRUE indicates that the IP Manager does not identify VoIP-enabled devices and does not create a VoIP topology collection set. ■ A value of FALSE indicates that the IP Manager identifies VoIP-enabled devices and creates a VoIP topology collection set. The IP Manager stores the VoIP topology collection set in instances of the VOIP_TopologyCollection class. By importing a VoIP topology collection set, VoIP Availability Manager will probe only those devices that support VoIP, which significantly reduces the discovery time for VoIP Availability Manager. *“Enabling light discovery for satellite Domain Managers” on page 61* clarifies the use of the DisableVOIPDiscovery parameter.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
EnableASNMPForMIB2	TRUE,FALSE Default: TRUE	By default, IP 8x versions allow for asynchronous SNMP (ASNMP) requests. Setting the value of this parameter to FALSE disables asynchronous requests for all the devices. If the user wants to enable synchronous SNMP requests for specific device models, only then configure the DoNotUseASNMPPattern paramerter. Currently only MIB2 is supported.
DoNotUseASNMPPattern	TRUE,FALSE Default: TRUE	Use the DoNotUseASNMPPattern parameter to enable synchronous SNMP requests for specific device models by specifying their system object ID (sysOID). To do this, uncomment the DoNotUseASNMPPattern parameter and add the list of sysOID entries, each separated by a pipe character (|). This is mostly used for slower SNMP agents which have problems with ASNMP. For example: #DoNotUseASNMPPattern: .1.3.6.1.4.1.9.5.50|. 1.3.6.1.4.9.5.44
maxOIDsPerPacketForASNMP	Integer Default: 19	This parameter is used to configure the maximum number of OIDs per packet that can be sent using ASNMP.
RigorousMACTest	TRUE,FALSE Default: FALSE	This parameter, if set to TRUE, will find out if All the MACs are shared between two systems (only if the two systems share the same sysName and sysOID). If so, the two systems are assumed to be the same and one is deleted. By default, it is set to FALSE, which means, if any one MAC is shared between two systems, (only if the two systems share the same sysName and sysOID), one of the systems is deleted, since they are assumed to be identical.
DefaultMaximumNetworkSizeForCorrelation	-1 and a positive integer Default: 10	The codebook for UnitaryComputerSystem's (Router, Switch, Host) Down problem include the MightBeDown symptom from the other UnitaryComputerSystems # that share a IPNetwork with it. Larger IPNetwork mean larger code book size and more system resources during correlation. And also, in this case, the MightBeDown symptom is not necessary to get proper correlation. Configuring the below flag customer can chose to exclude symptoms from IPNetwork. This is limit on the number of RelayDevices (Router, Switch) that are part of the IPNetwork. If the RelayDevice count is greater than this value then for that IPNetwork the symptoms from IPNetwork are not used in the UCS. Possible values for the flag are -1 and a positive integer. -1 is used to disable this functionality (In this case, irrespective of the IPNetwork size, the MightBeDown symptom is used). Default value suggested is 10.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
GetBulkPattern		This parameter allows you to enable or disable SNMP getBulk requests only for specific devices by sysOID. This setting overrides the value of SNMPGetBulkEnabled specified in the Discovery.conf The syntax for this parameter is GetBulkPattern-<SysOID> <TRUE/FALSE> For example: GetBulkPattern-.1.3.6.1.4.1.9.5.50 TRUE GetBulkPattern-.1.3.6.1.4.1.9.5.51 FALSE GetBulkPattern-.1.3.6.1.4.1.1872.1.15 TRUE
GetBulkTimeoutOverrideRatio		This parameter can be used to override the default value for SNMP getBulk timeouts during discovery. The format is SNMPGetBulkTimeoutOverride-<SysOID> <ratio>. The ratio is multiplied with defaultTimeout defined in the Discovery.conf For example: SNMPGetBulkTimeoutOverride-.1.3.6.1.4.1.9.5.50 2 This will set the timeout to 2 * 1000 for getBulk if the value for defaultTimeout is 1000 in Discovery.conf. GetBulkTimeoutOverrideRatio-.1.3.6.1.4.1.1872.1.15 2.5
GetBulkRetriesOverrideRatio		This parameter can be used to override the default value for SNMP getBulk retries during discovery. The ratio is multiplied with defaultRetries defined in discovery.conf The format is GetBulkRetriesOverrideRatio-<SysOID> <ratio> For example: GetBulkRetriesOverrideRatio-.1.3.6.1.4.1.9.5.50 2 This will set the no of retries to 2 * 5 for getBulk if the value for defaultRetries is 5 in discovery.conf. GetBulkRetriesOverrideRatio-.1.3.6.1.4.1.1872.1.15 1.5
ThresholdOfChangedUCSForIncReconfig	Integer Default: 10	This parameter controls the maximum number of UCS for which incremental reconfigure will run. For example, if the value is 10, then incremental reconfigure will run if the number of the last discovered UCS is less than or equal to 10, else BULK reconfigure will run, post discovery. This parameter is not used if reconfigure is invoked from the Console.
EnableTeamedNICDiscovery	TRUE, FALSE Default: TRUE	This parameter is used for enabling or disabling the NIC teaming functionality.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
DefaultMaximumNetworkSizeForCorrelation	Integer Default: 10	This parameter is used to prevent propagation of MightBeDown symptom between peer relay devices that are connected through the IPNetwork. These devices are not connected through a network connection or a cable or are not part of the same partition. If a count of relay devices on a network is greater than the value set in this attribute, then for that network the symptoms from IP Network are not used. Instead, symptoms from network, cable and partition connections are used.
VirtualMACPattern		This parameter is used to define the Virtual MAC patterns used in makeBridgedMAC call to populate the Port->VirtualBridges relationship. These include HSRP, VRRP virtual MAC and VMWare registered MAC pattern. For example: VirtualMACPattern 00-00-0C-07-AC-*|00-00-5E-00-01-*|00-05-69-*|00-0C-29-*|00-0C-14-*|00-50-56-*
IFNamePattern		This parameter is used to create interface and port based on the IFNamePattern.
CDFileSystemDirPattern	String value Default value: *CDROMFOO*	This parameter is used to prevent the creation of file system for the devices.
RetainStaleConnections	TRUE, FALSE Default: False	■ A value of TRUE indicates that, the existiing connections will be retained on rediscovery when the trunk ports are down. ■ A value of FALSE indicates that, the existiing connections will not be retained on rediscovery when the trunk ports are down.
LAPDL1activeConsideredUp	TRUE, FALSE Default: FALSE	A value of TRUE indicates that, for LAPD ISDN interfaces, Layer 1 active state will not be considered as DOWN.
UseLayer3SwitchPattern	TRUE FALSE Default: FALSE	This parameter is used to decide whether Layer3SwitchPattern must be used to identify the Layer3 switches or not.
PruneSystemlessMAC	TRUE FALSE Default: FALSE	This parameter is used to enable or disable pruning of Systemless MAC addresses.
WANLINK_PPP	TRUE FALSE Default: TRUE	This parameter is used to create WAN connections by ic-post-wan-link.asl file.
WANLINK_L3IPVLAN	TRUE FALSE Default: TRUE	This parameter is used to create WAN connections by ic-post-wan-link.asl file.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
WANLINK_RFC1483	TRUE FALSE Default: TRUE	This parameter is used to create WAN connections by ic-post-wan-link.asl file.
MAC2BridgedPortTable	TRUE FALSE Default: FALSE	This parameter is used to manage the VOIP handsets in VOIP Availability Manager. A value of TRUE indicates that, the user can manage the VOIP handsets in VOIP Availability manager.
EnableNonAccessIPPing	TRUE FALSE Default: FALSE	This parameter instruments all the IP addresses for ICMP ping.
EnableMIB2PortDiscovery	TRUE FALSE Default: FALSE	This parameter is used to manage the port discovery for Juniper EX series. ■ A value of TRUE indicates that, this parameter will trigger the port discovery for Juniper EX series based on ifTable. ■ A value of FALSE indicates that, ports for Juniper EX series will be discoverd from BRIDGE MIB, LAG MIB & LLDP MIB.
EnableNexus1KvVMautoDiscovery	TRUE FALSE Default: TRUE	Set the value of the parameter “EnableNexus1KvVMautoDiscovery” to TRUE. VMs attached to Nexus 1000V will be discovered automatically and placed in the IP pending list once the router and Nexus 1000V are discovered. You need to trigger the discovery manually from the Pending List. This feature also requires you to discover the Nexus 1000V and the connected adjacent Router or Layer 3 Switch. It does not require the option "Enable Auto Discovery" in the Topology tab to be enabled.
EnableWirelessClientDiscovery	TRUE FALSE Default: TRUE	Disabling this flag stops the discovery of the wireless client.
EnableWirelessClientShortDiscovery	TRUE FALSE Default: TRUE	Disabling this flag stops the short discovery of the wireless client.
EnableRogueAPShortDiscovery	TRUE FALSE Default: TRUE	Disabling this flag stops the short discovery of the Rogue AP.
EnableVPCDiscovery	TRUE FALSE Default: TRUE	Disabling this flag stops the VPC discovery of Nexus 5000 switches.

Table 14-2. Parameters in the tpmgr-param.conf file (Continued)

Parameter	Value	Description
WIFI_reprobePeriod_short	Default value:900 seconds **Note** Value should be positive and greater than 300.	Sets the interval between successive WIFI short discoveries. **Note** Decreasing the discovery interval will increase the CPU usage. If you decrease the short discovery interval, use small decrements and monitor your current CPU usage.
EnableVirtualDataContextDiscovery	TRUE FALSE Default: TRUE	Disabling this flag will stop the Virtual Data Context (VDC) discovery in Nexus 5000 switches. **Note** Provide the Read-only or Administrator VDC credentials under the CLI Access Group in Polling and Threshold > Device Access.

Parameters that can be added in tpmgr-param.conf lists the parameters that are provided by IP Manager. You can add these parameters in tpmgr-param.conf configuration file, to perform the operations as mentioned in the description column.

Note These parameters are not available in any configuration file.

Table 14-3. Parameters that can be added in tpmgr-param.conf

Parameter	Value	Description
UseVPNIP	TRUE FALSE Default: FALSE	This parameter is used to control the new tagged IP feature in 7.0. A value of TRUE indicates that VPNIP and VPNIPNetwork objects are created instead of tagged IP.
NameResolveUseSysname	TRUE FALSE Default: FALSE	A value of TRUE indicates that, the sysName is resolved to IP address. If one of the IP addresses is among the IP table, the IP address is resolved to a DNS name. If the DNS name is different from the nodeName, then the node is deleted and the device has to be rediscovered.
GetSeedNameFromAgent	TRUE FALSE Default: FALSE	A value of TRUE indicates that, the system name is taken from the SNMP agent's seed name.
EnableSTPMonitoring	TRUE FALSE Default: FALSE	A value of TRUE indicates that, monitoring of STP nodes are enabled.
DisableVirtualTCPDiscovery	TRUE FALSE Default value: TRUE	A value of FALSE indicates that, VirtualTCP objects are created.
DisplayNameIP	TRUE FALSE Default value: TRUE	A value of FALSE indicates that, the IP address is not added on the interface DisplayName.

Table 14-3. Parameters that can be added in tpmgr-param.conf (Continued)

Parameter	Value	Description
DisplayNameIPUnnumbered	TRUE FALSE Default value: FALSE	A value of TRUE indicates that, the word UNNUMBERED is added in the interface DisplayName if the interface does not have an IP address configured.
NoIPsConfigPhyRtrName	TRUE FALSE Default value: FALSE	A value of TRUE indicates that, IP Manager does not create IP objects for a router which has no IP addresses configured on it. **Note** If a router is not configured with an IP address, IP manager creates a default IP address for the router.
DSCV-UseOldPartitionName	TRUE FALSE Default value: FALSE	■ A value of TRUE indicates that, the naming convention used for partitions is Partition-<PartitionKey> ■ A value of FALSE indicates that, the naming convention used for partitions is Partition-<PartitionKey>/<IPDomainName>
EnableAVAYAServerPortnetworkConnection	TRUE FALSE Default value: FALSE	A value of TRUE indicates that, the AVAYA Server Port network connection is created.
PTOPSUBIF_ENABLED	TRUE FALSE Default value: FALSE	This parameter is used to validate if PTOP sub-interface is enabled or disabled. A value of TRUE indicates that, PTOP sub-interface is enabled.
CardRedundancyTypePattern	String Default value: 23|<38-42>|57|78|87|91|92|200|219|237|300|309|310|318|322|1002|1008|1010	This parameter is used to include the ModuleType while creating the Card Redundancy. MIB OID .1.3.6.1.4.1.9.5.1.3.1.1.2 indicates the ModuleType of the Card Redundancy obtained from CiscoStackMIB.
DeleteExtremeEDPTable	TRUE FALSE Default value: FALSE	A value of TRUE indicates that, the values in the table Neighbor-Pair-Extreme-Edp are cleared after the Extreme Networks devices post-processing.
JuniperIfOperStatusChecking	TRUE FALSE Default value: FALSE	This parameter is used to manage the interfaces. A value of TRUE indicates that, interfaces will be managed.
EnabletcpConnectionCloseTrap	TRUE FALSE Default: FALSE	A value of TRUE indicates that, IP Manager adds the device that generates the tcpConnectionClose trap.

Table 14-3. Parameters that can be added in tpmgr-param.conf (Continued)

Parameter	Value	Description
Usedot34Addresses	TRUE FALSE Default: TRUE	A value of TRUE indicates that, IP Manager selectively ignore the query to .34 table (ipAddressTable) and only rely on the .20 table (ipAddrTable) or to disable the query to .34 table across the topology.
dot34ExclusionPattern		This flag must be used in combination of the Usedot34Addresses, if the Usedot34Addresses is set to FALSE, then only the dot34ExclusionPattern is considered. And then add the device SysOIDs to the below attribute separated by "|" (pipe) symbol. For those SysOIDs which are part of this attribute, SMARTS InChargeServer do not poll the .34 table (i.e ipAddressTable) and query the .20 table (ipAddrTable) to identify the interface index that has an IP address configured.

Description of name-resolver.conf

The name-resolver.conf file contains configuration parameters that you edit to control how the IP Manager names discovered systems. The parameters are a subset of attributes that are defined for the ICF-TopologyManager object.

Parameters in the name-resolver.conf file describes the parameters in the name-resolver.conf file. The parameters and their values are case-sensitive.

Table 14-4. Parameters in the name-resolver.conf file

Parameter	Value	Description
NameFormat	TM_USEAUTONAME,TM_USESEEDNAME Default: TM_USEAUTONAME	Determines how the discovery process assigns a name to a discovered system. Valid values are: ■ TM_USEAUTONAME The discovery process uses the parameter values in the AutoNameOrder section of this file as the source for system names. ■ TM_USESEEDNAME The discovery process uses the seed name as the system name. How the discovery process names a system is described in the VMware Smart Assurance IP Management Suite Discovery Guide.
AutoNameOrder section		
TM_USELOOPBACK	0, 1, 2, 3, or 4 order priority Default: 0	Resolve loopback IP (v4 or v6) address: If a loopback interface IP address can be resolved to a name, that name will be used to name the system. By default, the default loopback interface type number is 24 (represents the “software loopback” interface type).
TM_USESYSNAME	0, 1, 2, 3, or 4 order priority Default: 1	Resolve MIB-II sysName: If the sysName can be resolved to at least one IP (v4 or v6) address and at least one of the resolved IP addresses resolves back to the sysName, the sysName will be used to name the system.

Table 14-4. Parameters in the name-resolver.conf file (Continued)

Parameter	Value	Description
TM_USENONPRIVATEIP	0, 1, 2, 3, or 4 order priority Default: 2	Resolve nonprivate IP (v4 or v6) address: If at least one of the IP addresses is not a private IP address, the nonprivate IP address is used to resolve the name. Once a name is resolved, the name is used to name the system.
TM_USEPRIVATEIP	0, 1, 2, 3, or 4 order priority Default: 3	For IPv4 protocol only, resolve private IP address: If at least one of the IP addresses is a private IP address, the private IP address will be used to resolve the name. Once a name is resolved, the name will be used to name the system. By default, the private IP address pattern is 10.*|192.168.*|172.<16-31>.*, which is defined as: ■ Any IP address with the value of 10 in the first octet (10.*.*.*). ■ Any IP address with a value of 172 in the first octet and a value between 16 and 31 in the second octet (172.<16-31>.*.*). ■ Any IP address with a value of 192 in the first octet and a value of 168 in the second octet (192.168.*.*).
TM_USEAGENTADDRESS	0, 1, 2, 3, or 4 order priority Default: 4	Resolve SNMP agent address: If an SNMP agent address can be resolved to a name, that name will be used to name the system. The VMware Smart Assurance IP Management Suite Discovery Guide provides details on how the SNMP Agent address is determined.

Description of partition.conf

You use the partition.conf file to assign display names to partitions that are formed by the IP Manager. When the topology is incomplete, the IP Managercreates partitions to allow analysis to proceed.

By default, the IP Managernames a partition by assigning it the name Partition-< *number*>, starting with 0, and incrementing this value by one for each new partition. The partition number is followed by the name of the Domain Manager that created the partition. For example, the name of the first partition created by the IP Availability Managernamed INCHARGE-AM is Partition-0/INCHARGE-AM, the second is Partition-1/INCHARGE-AM, and so on.

You can create a more descriptive name for a partition by using the partition.conf file to assign a DisplayName to the partition. The partition.conf file is shown in *Figure on page*.

```
# partition.conf
#
# Users can specify DisplayName for partitions.
# The first column is a hostname or IP Address. The rest is treated
# as the DisplayName for the partition.
# You could have multiple entries for one partition. The last one wins.
#
# The following line sets the DisplayName of the partition of which
# router1 is a member to "Routers in NYC"
# router1 Routers in NYC
#
# The following example shows how to set DisplayName of the partition # that consists of a network
device that hosts IP address 10.64.1.1
```

```
#
# 10.64.1.1 Servers in LA
#
# The following example shows how to set DisplayName of the partition
# that consists of a network device that hosts IPv6 address
# 3FFE:80C0:22C:101:219:56FF:FE3F:8A50
#
# 3FFE:80C0:22C:101:219:56FF:FE3F:8A50 NY IPv6 Network
```

To name a Partition object, the IP Manageruses the value of the Name attribute for the object to set the value of the DisplayName attribute for the object. The IP Managernames a partition by assigning it the name Partition-<number>, starting with 0, and incrementing this value by one for each new partition.

The partition number is followed by the name of the Domain Managerthat created the partition. For example, the name of the first partition created by and IP Availability Managernamed INCHARGE-AM is Partition-0/INCHARGE-AM, the second is Partition-1/INCHARGE-AM, and so on.

To set the DisplayName of a partition, specify the hostname or IP address of a partition member followed by its name. You should specify a name or IP address that is already known to the IP Manager. Specify one hostname or IP address and name combination on each line.

In the partition.conf file in *Figure on page*, the DisplayName, “Servers in LA,” is associated with partition member “10.64.1.1”:

```
10.64.1.1 Servers in LA
```

If you specify multiple names for a partition, which is done by providing separate entries, the last name listed is used.

You do not need to restart the IP Managerafter making a change to the partition.conf file. The IP Managerautomatically loads the partition.conf file each time that it performs post-processing.

Description of tcat.conf

The Topology Change Analysis Tool (TCAT) identifies the key topology differences between various versions of IP releases and provides logical explanations based on any feature changes or enhancements. TCAT helps you to identify changes to a set of objects, relationships, and attributes which are related to device certifications for IP Manager upgrades. TCAT is installed as “sm_tcat” while installing IP and is located in the <BASEDIR>\smarts\bin directory.

tcat.conf file contains TCAT configuration settings and is located under the <BASEDIR>smarts/conf/tcat directory.

Example

```
# Configuration Settings of Topology Comparison and Analysis Tool (TCAT)
# The flat file for the lists of Object/Relationship/Attribute to be compared
TopoDiffLists=TopoDiffLists.txt
# The flat file for the mapping of IP version info and Rule XML file
VersionMapSet=IPVersionMaps.txt
# The XML file for miscellaneous information
```

```
MiscInfoXML=misc.xml
# The suffix for the Excel report file (Excel 2007 or later recommended)
# (The earlier versions of Excel can't handle more than 65536 Rows.)
ExcelSuffix=xlsx
# The tag switch for MultiThreading
MultiThreading=on
# The tag switch for TCat developers
DevSwitch=off
```

The VMware Smart Assurance IP Manager User Guide provides more information on TCAT.

Description of oidInfo.conf

The OID Info tool is a utility, which when invoked against any discovered device, would gather a set of OIDs associated with it along with the corresponding drivers and instrumentation classes.

Before the tool is run, edit the *smarts/conf/discovery/oidInfo.conf* file in order to specify against which devices the tool needs to gather OID data and other particulars like the instrumentation class names and the probes names.

The VMware Smart Assurance IP Manager User Guide and the
VMware Smart Assurance IP Manager Concepts Guide provide more information on the OID Info tool.

Sample extract:

```
#==============================================================================#
#Configuration Paramters:
#------------------------------------------------------------------------------#
#Interval to poll for OID Values (in secs)
pollingInterval = 120
#Timeout to be used in sm_snmp get (in secs)
snmpTimeout = 500
#==============================================================================#
#==============================================================================#
#Devices Info:
#------------------------------------------------------------------------------#
#Router       Router1.VMware.com         Monitoring      Fan|Memory|SNMPAgent
#Switch       Switch1.VMware.com         Discovery       *
#Router       Router2.VMware.com         All             Card
#------------------------------------------------------------------------------#
#CLASS        INSTANCE                TYPE            ENTITY
#==============================================================================#
#==============================================================================#
#Note: White space is used as a delimeter while parsing this file.
#Please separate fields using whitespace and do not use whitespace within
#the fields
```

Description of user-defined-connections.conf

You use the user-defined-connections.conf file to add your own Layer 2 and Layer 3 connections to the managed topology. Doing so might be useful in cases where these connections are not discovered because of incomplete information in the MIB. If you know the necessary information, create these connections by specifying them in this file. The types of connections that are created include NetworkConnection, Cable, and TrunkCable.

The user-defined-connections.conf file is shown in *Figure on page*.

```
# This is a sample user-defined connections for the InCharge Server.
#
# A connection must contain FOUR fields separated by |
# - The first field is the local network device.
#   You can specify either a name or an IP address.
# - The second field is the network adapters on the local device.
#   It can be ifIndex or ifDescr or ifName as defined in MIB2.
#   It can also be n/m or n.m where n is the module number and m is
#   port number.
# - The third field is the remote network device.
#   You can specify either a name or an IP address.
# - The fourth field is the network adapters on the remote device.
#   It can be ifName or ifDescr or ifIndex as defined in MIB2.
#   It can also be n/m or n.m where n is the module number and m is
#   port number.
#
# The search for network adapter is performed in the order of
# ifName, ifDescr, ifIndex. If it fails to return a network adapter
# object, the specified string is used as interfaceKey/PortKey to
# find interface/port objects.
#
# To make your file more readable, you can
# include blank and comment lines.
# A comment line is one whose first character is "#".
#
# Following are a few examples. NOTE - the lines are commented, so the
# discovery won't really try to make these connections.
#
# 192.168.1.200|Serial0|router2.smarts.com|5|
# 10.64.1.1|2.4|Core-switch.smarts.com|2/4|
#
```

As indicated in *Figure on page* , a user-defined connection contains the following four fields, each separated by a pipe character (|):

- The first field is the local network. You can specify the local network by name or IP address.
- The second field is the network adapter on the local device. You can specify the network adapter by its ifIndex, ifDescr, or ifName, as defined in RFC 1213. You can also use the < *n*>/< *m*>or < *n*>.< *m*>syntax, where < *n*>is the module number, and < *m*>is the port number.

- The third field is the remote network device. You can specify the remote network device by name or IP address.
- The fourth field is the network adapter on the remote device. You can specify the network adapter by its ifIndex, ifDescr, or ifName, as defined in RFC 1213. You can also use the < *n*>/< *m*>or < *n*>.< *m*>syntax, where < *n*>is the module number, and < *m*>is the port number.

  Any object that is specified in these four fields must be in the managed topology.

  The IP Managersearches for the network adapter in the order of ifName, ifDescr, and ifIndex. If a network adapter is not found, the specified string is used as InterfaceKey/PortKey to find the network adapter.

  The following are two examples of user-defined connections:

  ```
  192.168.1.200|Serial0|router2.smarts.com|5|
  10.64.1.1|2.4|Core-switch.smarts.com|2/4|
  ```

  The network adapter field for the remote device must end with a pipe character (|). As with changes to the partition.conf file, you do not need to restart the IP Managerafter making a change to the user-defined-connections.conf file. The IP Managerautomatically loads the user-defined-connections.conf file each time that it performs post-processing.

Controlling the analysis of wide area networks

In a wide area network (WAN), where multiple logical connections emanate from a single physical interface, the IP Manager performs WAN analysis by default and diagnoses one of the following problems listed in Problems diagnosed by IP Manager in a WAN.

Table 14-5. Problems diagnosed by IP Manager in a WAN

Problem	Description
Interface::Down	If the physical interface is operationally down, which explains why all of the subinterfaces that are layered over the physical interface have failed, along with any peer interfaces of those subinterfaces. “Interface” in “Interface::Down” represents the physical interface.
Interface::LogicalConnectionDown	■ If two or more network connections at the subinterface level have failed and the physical interface is operationally up. “Interface” in “Interface::LogicalConnectionDown” represents the physical interface. Network connections at the subinterface level represent WAN circuits. ■ Indicates a probable failure in the WAN network that does not cause a physical failure. The premise for the diagnosis is that a common but unobservable condition is causing all of the network connection failures.
NetworkConnection::Down	If a single network connection at the subinterface level has failed.

Whether or not the IP Manager performs WAN analysis is controlled by the SM_LOGICALCONNECTIONDOWN environment variable.

SM_LOGICALCONNECTIONDOWN environment variable

Valid values for the SM_LOGICALCONNECTIONDOWN environment variable are:

- ENABLED (default)

  The IP Manager performs WAN analysis, and generates an Interface::LogicalConnectionDown problem when two or more network connection failures occur at the subinterface level and the physical interface is operationally up.

- DISABLED

  The IP Manager does not perform WAN analysis and therefore does not generate an Interface::LogicalConnectionDown problem. Instead, when the physical interface is operationally up, the IP Manager generates a NetworkConnection::Down problem for each network connection failure that occurs at the subinterface level.

  Values ENABLED and DISABLED are not case-sensitive.

Parameters for the SystemRestarted event

The parameters in Parameters for the SystemRestarted event enable and control the SystemRestarted event.

Table 14-6. Parameters for the SystemRestarted event

Parameter name	Allowed values	Description
EnableGenericOIEvent	ENABLED,DISABLED Default: DISABLED Controls whether a SystemRestarted trap for a system is sent to the Adapter Platform, through the SNMP Trap Adapter that is configured as a trap receiver.	Belongs to Connectivity setting and is described in *"Connectivity threshold setting" on page 181*.
MaxUpTimeThreshold	1 to 1436 minutes Default: 60 minutes Amount of system up time at which a system is considered to have restarted.	
OITrapAdapterHost	String Default: localhost Name or IP address of the host system where the SNMP Trap Adapter that is configured as a trap receiver is running.	Belongs to tpmgr-param.conf file and is described in *"Description of tpmgr-param.conf" on page 40*.
OITrapAdapterPort	Integer Default: 162 Trap listening port on the host system where the SNMP Trap Adapter that is configured as a trap receiver is running.	
EnableSystemRestart	TRUE,FALSE Default: FALSE	

As shown in *Figure 7 on page 65*, The polled system uptime value for a managed system is compared to the MaxUpTimeThreshold value. Whenever the system uptime value for a system equals or exceeds the MaxUpTimeThreshold value, the IP Availability Manager considers the system to have been restarted.

Trap parsing rules for the SystemRestarted event

The SNMP Trap Adapter that is configured as a trap receiver uses the rules that are specified in the trap_mgr.conf file to map a SystemRestarted trap into the data fields of a SystemRestarted notification. The Adapter Platform, in turn, creates the SystemRestarted notification (object) from the data fields and exports the notification to the Global Manager.

The parsing rules for the SystemRestarted trap are defined in the “System restart traps” section of the trap_mgr.conf file. The trap_mgr.conf file is located in the BASEDIR/smarts/conf/icoi directory of the Service Assurance Manager installation area.

Parameters for the ConfigChange event

The parameters in Parameters for the ConfigChange event enable and control the ConfigChange event.

Table 14-7. Parameters for the ConfigChange event

Parameter name	Allowed values	Description
OITrapAdapterHost	String Default: localhost Name or IP address of the host system where the SNMP Trap Adapter that is configured as a trap receiver is running.	Belongs to tpmgr-param.conf file and is described in *“Description of tpmgr-param.conf” on page 40*.
OITrapAdapterPort	Integer Default: 162 Trap listening port on the host system where the SNMP Trap Adapter that is configured as a trap receiver is running.	
EnableConfigChange	TRUE,FALSE Default: FALSE	

Trap parsing rules for the ConfigChange event

The SNMP Trap Adapter that is configured as a trap receiver uses the rules that are specified in the trap_mgr.conf file to map a ConfigChange trap into the data fields of a ConfigChange notification. The Adapter Platform, in turn, creates the ConfigChange notification (object) from the data fields and exports the notification to the Global Manager.

The parsing rules for the ConfigChange trap are defined in the “Cisco Configuration Management Traps” and “Cisco Configuration change Traps” sections of the trap_mgr.conf file. The trap_mgr.conf file is located in the BASEDIR/smarts/conf/icoi directory of the Service Assurance Manager installation area.

Interface-matching filters in the tpmgr-param.conf file

Use the interface-matching filters in the tpmgr-param.conf configuration file as a starting point to configure interface-matching filters for access devices. The tpmgr-param.conf file contains the IFTypePattern and IFDescrPattern interface-matching filters that are listed in IFTypePattern and IFDescrPattern interface-matching filters. Modify any of these filters or add your own filters to the file.

Note Currently, the tpmgr-param.conf file does not contain any IFIndexPattern interface-matching filters; thus, by default, those filters are set to ~*.

Table 14-8. IFTypePattern and IFDescrPattern interface-matching filters

Device	Interface pattern type and device	Interface-matching pattern
Ascend Max-1800 Switch	IFTypePattern-.1.3.6.1.4.1.529.1.2.2	~1 Interface type definitions: 1 = other (generic) **Note** For any discovered device that matches the sysObjectID of this filter, any interface that has an ifType value other than 1 will match this filter and therefore be created.
Ascend Max-2000 Switch	IFTypePattern-.1.3.6.1.4.1.529.1.2.3	
Ascend Max-3000 Switch	IFTypePattern-.1.3.6.1.4.1.529.1.2.9	
Cisco 861W Router	IFDescrPattern-.1.3.6.1.4.1.9.1.834	SSLVPN*|wlan*|Vlan* **Note** For any discovered device that matches the sysObjectID of this filter, any interface that has an ifDescr description that contains SSLVPN, wlan, or Vlan will match this filter and therefore be created.
Cisco IOS 6509 NEB Router	IFTypePattern-.1.3.6.1.4.1.9.1.310	~51 Interface type definitions: 51 => sonetVT
Paradyne 3160 Probe	IFTypePattern-. 1.3.6.1.4.1.1795.1.14.2.2.1	~*
	IFDescrPattern-. 1.3.6.1.4.1.1795.1.14.2.2.1	~COM*|~Modem*|~DTE*|~AUX* **Note** For any discovered device that matches the sysObjectID of this filter, any interface that has an ifDescr description that does not contain COM, Modem, DTE, or AUX will match this filter and therefore be created.
Paradyne T1 SLV Model 9124 Probe	IFTypePattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.5	~*
	IFDescrPattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.5	~RMON*|~DSX-1*
Paradyne DDS SLV Model 9626 Probe	IFTypePattern-. 1.3.6.1.4.1.1795.1.14.2.4.1.6	~*
	IFDescrPattern-. 1.3.6.1.4.1.1795.1.14.2.4.1.6	~RMON*|~COM*|~Modem*

Table 14-8. IFTypePattern and IFDescrPattern interface-matching filters (Continued)

Device	Interface pattern type and device	Interface-matching pattern
Paradyne DDS SLV Model 9624-OS Probe	IFTypePattern-. 1.3.6.1.4.1.1795.1.14.2.4.1.8	~*
	IFDescrPattern-. 1.3.6.1.4.1.1795.1.14.2.4.1.8	~RMON*|~COM*
Paradyne T1 SLV Model 9126-IISLV Probe	IFTypePattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.7	~*
	IFDescrPattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.7	~RMON*|~Modem*|~DSX-1*|~Ethernet*
Paradyne T1 SLV Model 9128-II Probe	IFTypePattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.8	~*
	IFDescrPattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.8	~RMON*|~DSX-1*|~COM*|~Modem*
Paradyne T1 SLV Model 9124-II Probe	IFTypePattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.9	~*
	IFDescrPattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.9	~RMON*|~DSX-1*
Paradyne T1 FLEX Model 9123-C Probe	IFTypePattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.11.1	~*
	IFDescrPattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.11.1	~COM*
Paradyne T1 FLEX Model 9123-SLV Probe	IFTypePattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.11.2	~*
	IFDescrPattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.11.2	~RMON*|~COM*
Paradyne T1 SLV Model 9124-OS Probe	IFTypePattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.12	~*
	IFDescrPattern-. 1.3.6.1.4.1.1795.1.14.2.4.4.12	~RMON*|~DSX-1*
Paradyne T3 DSU/CSU Model 9520-II Probe	IFTypePattern-. 1.3.6.1.4.1.1795.1.14.2.4.5.3	~*
	IFDescrPattern-. 1.3.6.1.4.1.1795.1.14.2.4.5.3	~RMON*|~COM*|~Modem*
Paradyne T1 DSU/CSU Model 7123 Probe	IFTypePattern-. 1.3.6.1.4.1.1795.1.14.2.4.12.1.1	~*
	IFDescrPattern-. 1.3.6.1.4.1.1795.1.14.2.4.12.1.1	~COM*
Radware IP-mux1 Router	IFTypePattern-.1.3.6.1.4.1.164.6.1.3.82	~80~81~82 Interface type definitions:

Table 14-8. IFTypePattern and IFDescrPattern interface-matching filters (Continued)

Device	Interface pattern type and device	Interface-matching pattern
Radware IP-mux16 Router	IFTypePattern-.1.3.6.1.4.1.164.6.1.3.83	80 => atmLogical81 => ds082 => ds0Bundle **Note** For any discovered device that matches the sysObjectID of this filter, any interface that has an ifType value other than 80, 81, or 82 will match this filter and therefore be created.
Redback SMS 1800 Router	IFTypePattern-.1.3.6.1.4.1.2352.1.3	~23~53~0 Interface type definitions: 23 => ppp 53 => propVirtual0 => invalid value (ignored) **Note** For any discovered device that matches the sysObjectID of this filter, any interface that has an ifType value other than 23 or 53 will match this filter and therefore be created.
	IFDescrPattern-.1.3.6.1.4.1.2352.1.3	~LOGICAL INTERFACE~PPP LAYER~0 **Note** For any discovered device that matches the sysObjectID of this filter, any interface that has an ifDescr description that does not contain LOGICAL INTERFACE, PPP LAYER, or 0 will match this filter and therefore be created.
Redback SMS 10000 Router	IFTypePattern-.1.3.6.1.4.1.2352.1.4	~23~53~0 Interface type definitions: 23 => ppp 53 => propVirtual0 => invalid value (ignored)
	IFDescrPattern-.1.3.6.1.4.1.2352.1.4	~LOGICAL INTERFACE~PPP LAYER~0
Unisphere ERX-1440 Router	#IFTypePattern-. 1.3.6.1.4.1.4874.1.1.1.1.1 (Commented out)	* (Described in *“Optimizing the discovery of ERX devices” on page 133*.)
	#IFDescrPattern-. 1.3.6.1.4.1.4874.1.1.1.1.1 (Commented out)	~* (Described in *“Optimizing the discovery of ERX devices” on page 133*.)
RAD IPmux-16 Router	IFTypePattern-.1.3.6.1.4.1.164.6.1.3.83	~80~81~82 **Note** For any discovered device that matches the sysObjectID of this filter, any interface that has an ifType value other than 80, 81, 82 will match this filter and therefore be created.
RAD IPmux-1 Router	IFTypePattern-.1.3.6.1.4.1.164.6.1.3.82	~80~81~82 **Note** For any discovered device that matches the sysObjectID of this filter, any interface that has an ifType value other than 80, 81, 82 will match this filter and therefore be created.

Other interface-limiting parameter types in the tpmgr-param.conf file

The tpmgr-param.conf file also contains other interface-limiting parameter types, most of which are listed in Other interface-limiting parameter types. The table includes an example, the default value, and the definition of each parameter type. Several parameter types in Other interface-limiting parameter types are interface-matching filters that are also based on the ifIndex, ifDescr, and ifType objects. However, they have slightly different interface-matching pattern names and employ slightly different syntax than the standard interface-matching filters previously discussed.

Table 14-9. Other interface-limiting parameter types

Parameter type	Default value	Definition
IFTypePatternIFExt<*sysObjectID*> <*interface type pattern*> Example (in tpmgr-param.conf file): ■ IFTypePatternIFExt.1.3.6.1.4.1.119.1.3.13.4 39|53|1 where: sysObjectID is the NEC Bluefire 5003 Switch; and Interface types are 39 => sonet, 53 => ds3, and 1 => other (generic). For any discovered device that matches the sysObjectID, the filter will override the 30|37|134 default interface type pattern with 39|53|1. Only the interfaces that have an ifType value of 39, 53, or 1 will be created.	30|37|134	A filter that restricts the creation of interfaces (ports) for a specific device based on a specific interface type pattern. The IFTypePatternIFExt filter, as well as the IFDescrPatternIFExt and IFIndexPatternIFExt filters, apply to some of the first Cisco, Fore, Huawei, NEC, and Riverstone devices that were certified for the IP Manager. The default values for these filters are: ■ IFIndexPatternIFExt defaults to ~* ■ IFDescrPatternIFExt defaults to ~* ■ IFTypePatternIFExt defaults to 30|37|134
IFTypePattern-SwitchPort[sysObjectID] <*interface type pattern*> Example (in tpmgr-param.conf file): ■ IFTypePattern-SwitchPort.1.3.6.1.4.1.119.1.14.8 37 where: sysObjectID is the NEC Bluefire 8000 series 2.5G ATM Switch; and Interface type is 37 => atm. For any discovered device that matches the sysObjectID, the filter will override the 6|26|62|69|117 default interface type pattern: Only the interfaces that have an ifType value of 37 will be created.	6|26|62|69|117	A filter that restricts the creation of interfaces (ports) for a specific device based on a specific interface type pattern. The IFTypePattern-SwitchPort filter, as well as the IFDescrPattern-SwitchPort and the IFIndexPattern-SwitchPort filters, apply to some of the first Cisco, NEC, and Lucent devices that were certified for the IP Manager. The default values for these filters are: ■ IFIndexPattern-SwitchPort defaults to ~* ■ IFDescrPattern-SwitchPort defaults to ~* ■ IFTypePattern-SwitchPort defaults to 6|26|62|69|117

Table 14-9. Other interface-limiting parameter types (Continued)

Parameter type	Default value	Definition
IFDescrPattern-SwitchPort[sysObjectID] <*interface description pattern*> Example (commented out in tpmgr-param.conf file): ■ #IFDescrPattern-SwitchPort.1.3.6.1.4.1.9.1.501 Vlan888 where: sysObjectID is the Cisco C4507-with-Sup Switch. For any discovered device that matches the sysObjectID, the filter will override the ~* default interface description pattern: Only the interfaces that contain Vlan888 in their ifDescr descriptions will be created.	~*	A filter that restricts the creation of interfaces (ports) for a specific device based on a specific interface description pattern. When this filter is used, the associated IFTypePattern-SwitchPort filter is typically set to "~*".
CiscoStackWithATM-Pattern <*sysObjectID1*>| <*sysObjectID2*>| <*sysObjectIDn*> Example (in tpmgr-param.conf file): ■ CiscoStackWithATM-Pattern .1.3.6.1.4.1.9.5.7|.1.3.6.1.4.1.9.5.17|.1.3.6.1.4.1.9.5.34 where: sysObjectID1 is the Cisco Catalyst WS-C5000 Switch; sysObjectID2 is the Cisco 5500 Switch; and sysObjectID3 is the Cisco Catalyst 5505 Switch. For any discovered ATM switch that matches any of these sysObjectIDs, ATM peer connections will be created between the ATM switch ports and the ports on the neighboring ATM switches.	.1.3.6.1.4.1.9.5.7, .1.3.6.1.4.1.9.5.17, .1.3.6.1.4.1.9.5.34	Identifies which devices are ATM switches so that ATM peer connections are created between the ATM switch ports and the ports on the neighboring ATM switches.
Layer3SwitchPattern <*sysObjectID1*>| <*sysObjectID2*>| <*sysObjectID3*>|<*sysObjectIDn*> Example (in tpmgr-param.conf file): ■ Layer3SwitchPattern .1.3.6.1.4.1.9.1.400|.1.3.6.1.4.1.9.5.44| .1.3.6.1.4.1.4641.1.*|.1.3.6.1.4.1.5567.1.1.* where: sysObjectID1 is the Cisco 6513 IOS Switch; sysObjectID2 is the Cisco 6509 Switch; sysObjectID3 is the Tellabs 8820 or 8860 Switch; and sysObjectID4 is the Riverstone Networks Procut Line of Multi Layer Switch Router. For any discovered Layer 3 device that matches any of these sysObjectIDs, WAN network connections will be created between the Layer 3 switch ports and the ports on the neighboring routers.	.1.3.6.1.4.1.9.1.400, .1.3.6.1.4.1.9.5.44	Identifies which devices are Layer 3 switches so that WAN network connections are created between the Layer 3 switch ports and the ports on the neighboring routers. If you comment out the default line for this parameter in the tpmgr-param.conf file, the IP Manager consults the rule set in the following file to determine how to create WAN network connections during the postprocessing phase of the discovery process: BASEDIR/smarts/rules/discovery/ic-post-wan-link.asl

Table 14-9. Other interface-limiting parameter types (Continued)

Parameter type	Default value	Definition
DisplayNameByIfDescr-<*sysObjectID*> TRUE|FALSE Example (in tpmgr-param.conf file): ■ DisplayNameByIfDescr-.1.3.6.1.4.1.800.3.1.1.9 TRUE where: sysObjectID is the Alcatel OmniStack 6024 Switch. For any discovered device that matches the sysObjectID, any interface discovered without an ifName string will have its ifDescr description included in its display name.	FALSE	Controls how to name the interface of a specific device when no ifName string is discovered for the interface: ■ A value of TRUE indicates that the ifDescr description for the interface will be included in the display name for the interface. ■ A value of FALSE indicates that the DeviceID for the interface will be included in the display name for the interface. If the DeviceID is empty, the ifDescr description will be included in the display name. **Note** ifName is a text string that contains the name that is used by the device to represent the interface. DeviceID refers to the device to which this interface belongs.
ERXIfExcludeSysPattern <*name pattern*> Example (in tpmgr-param.conf file): ■ ERXIfExcludeSysPattern * Any discovered Juniper ERX device whose Name attribute string matches * (all discovered ERX devices will match this filter) will be subjected to the following two filters: ERXIfExcludeTypePattern ERXIfExcludeDescrPattern	*	Identifies through a name pattern filter which Juniper ERX devices are to be subjected to the following two filters: ■ ERXIfExcludeTypePattern ■ ERXIfExcludeDescrPattern *“Optimizing the discovery of ERX devices” on page 133* clarifies the use of this parameter. **Note** The term “Juniper ERX device” or just “ERX device,” as used here, represents an instance of any discovered Juniper ERX main or virtual router.
ERXIfExcludeTypePattern <*interface type pattern*> Example (in tpmgr-param.conf file): ■ ERXIfExcludeTypePattern 1|23|126|134 where: Interface types are 1 => other (generic), 23 => ppp, 126 => ip, and 134 => atmSubInterface. For any discovered Juniper ERX device that matches the ERXIfExcludeSysPattern filter, any interface that has an ifType value other than 1, 23, 126, or 134 will be created.	1|23|126|134	A filter that restricts the creation of interfaces (ports) for the Juniper ERX devices that match the ERXIfExcludeSysPattern filter. The filtering is based on a specific interface type pattern. Any interface type that matches the ERXIfExcludeTypePattern filter is excluded from the discovered topology, and any interface type that does not match the filter is included in the discovered topology. *“Optimizing the discovery of ERX devices” on page 133* clarifies the use of this parameter.
# ERXIfExcludeTypePattern 1|23|134 This modified pattern of the existing ERXIfExcludeTypePattern parameter enables the VRRP probe to discover IP interfaces on Juniper ERX devices that belong to a VRRP group. In cases where a VRRPGroup is configured as a member of a VRF, the ifType 126 should not be excluded. Use this pattern instead # ERXIfExcludeTypePattern 1|23|134	1|23|134	A filter that enables the VRRP probe to discover IP interfaces on Juniper ERX devices that belong to a VRRP group.

Table 14-9. Other interface-limiting parameter types (Continued)

Parameter type	Default value	Definition
ERXIfExcludeDescrPattern <*interface description pattern*> Example (commented out in tpmgr-param.conf file): ■ #ERXIfExcludeDescrPattern *ATM*<0-20>/<0-20>.<1800-900000>| *LOOPBACK<200-10000>|*PPPOE* For any discovered Juniper ERX device that matches the ERXIfExcludeSysPattern filter, any interface that has an ifDescr description that matches any of these patterns will *not* be created, and any interface that has an ifDescr description that does *not* match any of these patterns will be created.	~*	A filter that restricts the creation of interfaces (ports) for the Juniper ERX devices that match the ERXIfExcludeSysPattern filter. The filtering is based on a specific interface description pattern. Any interface description that matches the ERXIfExcludeDescrPattern filter is excluded from the discovered topology, and any interface description that does not match the filter is included in the discovered topology. *“Optimizing the discovery of ERX devices” on page 133* clarifies the use of this parameter.
ERXVRNonIfIPExcludeSysPattern <*name pattern*> Example (commented out in tpmgr-param.conf file): ■ #ERXVRNonIfIPExcludeSysPattern * For any discovered Juniper ERX device whose Name attribute string matches * (all discovered ERX devices will match this filter), any IP address (discovered on the device) that is not related to interfaces will be excluded from the discovered topology.	~*	Identifies through a name pattern filter which Juniper ERX devices are to have all discovered IP addresses *that are not related to interfaces* excluded from the discovered topology.
IfVirtualTypePattern-<*sysObjectID*> <*interface type pattern*> Example (commented out in tpmgr-param.conf file): ■ #ifVirtualTypePattern-.1.3.6.1.4.1.9.1.452 135|136 where: sysObjectID is the Cisco WS-C3550-24Dc Switch; and Interface types are 135 => l2vlan and 136 => l3ipvlan. For any discovered device that matches the sysObjectID, the IP Manager will *not* create a “LayeredOver/Underlying” relationship *between* a virtual interface associated with ifType 135 or 136 *and* the underlying MAC address. Thus, only the “LayeredOver/Underlying” relationship between the underlying MAC address and the layered-over physical interface will exist for the MAC address. Accordingly, during the postprocessing phase of the discovery process, the IP Manager will create the network connection for the physical interface.	~*	For a specific device, enables the creation of a network connection for a physical interface that shares a physical MAC address with one or more virtual interfaces. This parameter can be used for any device that has multiple interfaces (one physical and the others virtual) that share the same MAC address. *“Enabling the creation of a physical connection for a shared MAC address” on page 136* clarifies the use of this parameter.

Table 14-9. Other interface-limiting parameter types (Continued)

Parameter type	Default value	Definition
ForceAgentAddressInListSysPattern <*name pattern*> Example (in tpmgr-param.conf file): ■ ForceAgentAddressInListSysPattern * For any discovered device whose Name attribute string matches * (all discovered devices will match this filter), the IP address held in its SNMP agent's AgentAddress attribute will be added to the list of IP addresses held in its SNMP agent's AgentAddressList attribute.	*	Identifies through a name pattern filter which devices should have the IP address held in their SNMP agent's AgentAddress attribute added to the list of IP addresses that are held in their SNMP agent's AgentAddressList attribute. The AgentAddress attribute holds the IP address that is used by the initial ICMP poll to reach the device, and the AgentAddressList attribute holds a list of IP addresses discovered on the device. In general (but not always), rules are already in place that result in the AgentAddress IP being added to the AgentAddressList. The ForceAgentAddressInListSysPattern parameter provides a means to specify which devices should be forced to have their AgentAddress IP address added to their AgentAddressList.
CDPDeviceOIDs <*sysObjectID1*>|<*sysObjectID2*>|<*sysObjectIDn*> Example (in tpmgr-param.conf file): ■ CDPDeviceOIDs ~.1.3.6.1.4.1.2467.4.*|~.1.3.6.1.4.1.9.9.368.4.* where: sysObjectID1 and sysObjectID2 together represent the Cisco CSS 11000 and 11500 Series Content Services Switches. For a Cisco CSS 11000 or 15000 Series Content Services Switch, no CDP connections are created for the interfaces on the switch. Conversely, for any discovered device other than a Cisco CSS 11000 or 15000 Series Content Services Switch, CDP connections are created for the interfaces on the switch.	(Identified in example)	Identifies which Cisco devices to which Cisco Discovery Protocol (CDP) connections should *not* be made. This parameter is used to exclude network connections to Cisco devices (such as CSS 11000 and 11500 Series Content Services Switches) with a management interface. Because CDP is used for some network management functions, any person on a directly connected segment to a Cisco CSS 11000 or 11500 series switch (for example) is able to perform CDP actions, actions that might include the gathering of sensitive information about the switch. This information could be used to design attacks against the switch. For this reason, do not make CDP connections to Cisco devices that have a management interface.
CiscoIPPhonePattern	Cisco?IP?Phone*	Pattern to be used for omitting IP phone ports.
LinuxBondingInterfacePattern	bond*	Pattern to be used for including Linux bonded logical interfaces. The EnableEthernetBonding parameter in the tpmgr-param.conf file must be TRUE (default) for this pattern to be used.

Table 14-9. Other interface-limiting parameter types (Continued)

Parameter type	Default value	Definition
ERX-VRF-VRRPCommunities-Pattern	*brmgt*|*orfe*	This parameter limits the discovery of VRF interfaces on Juniper ERX devices that belong to a VRRP group to just the VRF interfaces on the ERX devices that have a community string that matches the specified pattern.
ShortDiscoveryInstrPattern	Card_Fault_CiscoONSCPU|Card_Fault_CiscoEntityFRU	Instrumentation class pattern to be included in short discovery. For cards, the pattern that is specified by “ShortDiscoveryInstrPattern” will be checked against the instrument class name of the card that is operationally down before proceeding with short discovery. The autoReprobe_short parameter in the discovery.conf file must be TRUE for this pattern to be used.

Optimizing the discovery of ERX devices

Parameters for optimizing the discovery of ERX devices lists the parameters for optimizing the discovery of ERX devices.

Table 14-10. Parameters for optimizing the discovery of ERX devices

Parameter name	Filter type	Default value	Description
ERXIfExcludeSysPattern <*name pattern*> Example: ■ ERXIfExcludeSysPattern *network* Any discovered Juniper ERX device whose Name attribute string matches “network” (not case-sensitive) will be subjected to the following two filters: ERXIfExcludeTypePattern ERXIfExcludeDescrPattern	Inclusive	* (By default, all discovered Juniper ERX devices will match this filter.)	Identifies through a name pattern filter which Juniper ERX devices are to be subjected to the following two filters: ■ ERXIfExcludeTypePattern ■ ERXIfExcludeDescrPattern Any discovered ERX device whose Name attribute string matches the name pattern that is specified for this parameter will be subjected to these two filters.
ERXIfExcludeTypePattern <*interface type pattern*> Example: ■ ERXIfExcludeSysPattern *network* ■ ERXIfExcludeTypePattern 1|23|126|134 where: Interface types are 1 => other (generic), 23 => ppp, 126 => ip, and 134 => atmSubInterface. For any discovered Juniper ERX device whose Name attribute string matches “network” (not case-sensitive), any interface that has an ifType value other than 1, 23, 126, or 134 will be created.	Exclusive	1|23|126|134	A filter that restricts the creation of interfaces (ports) for the Juniper ERX devices that match the ERXIfExcludeSysPattern filter. The filtering is based on a specific interface type pattern. The ERXIfExcludeTypePattern filter is an exclusive-type filter: Any interface type that matches the filter is excluded, and any interface type that does not match the filter is included.
ERXIfExcludeDescrPattern <*interface description pattern*> Example: ■ ERXIfExcludeSysPattern *network* ■ #ERXIfExcludeDescrPattern *ATM*<0-20>/<0-20>.<1800-900000>| *LOOPBACK<200-10000>|*PPPOE* (commented out in the tpmgr-param.conf file) For any discovered Juniper ERX device whose Name attribute string matches “network” (not case-sensitive), any interface that has an ifDescr description that matches any of these patterns will *not* be created, and any interface that has an ifDescr description that does *not* match any of these patterns will be created.	Exclusive	~*	A filter that restricts the creation of interfaces (ports) for the Juniper ERX devices that match the ERXIfExcludeSysPattern filter. The filtering is based on a specific interface description pattern. Like the ERXIfExcludeTypePattern filter, the ERXIfExcludeDescrPattern filter is an exclusive-type filter: Any interface description that matches the filter is excluded, and any interface description that does not match the filter is included.

Table 14-10. Parameters for optimizing the discovery of ERX devices (Continued)

Parameter name	Filter type	Default value	Description
IFTypePattern-<*ERX sysObjectID*> <*interface type pattern*> Example: ■ IFTypePattern-.1.3.6.1.4.1.4874.1.1.1.1.1 ~80 where: sysObjectID is the Unisphere ERX-1440 Router; and Interface type is 80 => atmLogical. **Note** In this example, all ifType values will match ~80 except ifType 80.	Inclusive	*	A filter (standard filter) that further restricts the creation of interfaces (ports) for a Juniper ERX device based on a specific interface type pattern. Any interface type that matches the filter is included, and any interface type that does not match the filter is excluded. **Note** In the case of an ifType exclude/include conflict, the ERXIfExcludeTypePattern filter has higher priority than the IFTypePattern filter.
IFDescrPattern-<*ERX sysObjectID*> <*interface description pattern*> Example: ■ IFDescrPattern-.1.3.6.1.4.1.4874.1.1.1.1.1 ~*Logical Interface* where: sysObjectID is the Unisphere ERX-1440 Router. **Note** In this example, all ifDescr descriptions will match ~*Logical Interface* except those that contain a “Logical Interface” string.	Inclusive	~*	A filter (standard filter) that further restricts the creation of interfaces (ports) for a Juniper ERX device based on a specific interface description pattern. Any interface description that matches the filter is included, and any interface description that does not match the filter is excluded. When this filter is used, the associated IFTypePattern filter is typically set to “~*”. **Note** In the case of an ifDescr exclude/include conflict, the ERXIfExcludeDescrPattern filter has higher priority than the IFDescrPattern filter.

Problem Impact propagation policy over VLANs setting

Default values for the Problem Impact propagation policy over VLANs setting lists the Problem Impact propagation policy over VLANs setting parameters.

Table 14-11. Default values for the Problem Impact propagation policy over VLANs setting

Parameter	Default Value	Description
ImpactPropagation	ENABLED	Determines whether to allow problems on devices in a VLAN to propagate impacts on other devices in the same VLAN. The value can be ENABLED or DISABLED. ■ ENABLED allows impact propagation for the VLANs that belong to the VLAN impact propagation group. ■ DISABLED prevents impact propagation for the VLANs that belong to the VLAN impact propagation group. **Note** If a VLAN is not a member of any VLAN impact propagation group, impact propagation is allowed for the VLAN. Discovery is required for any change to take effect.

To use the “Problem Impact propagation policy over VLANs” setting to create a VLAN impact propagation group, you need to change the setting’s ImpactPropagation parameter to DISABLED. Accessing the Polling and Thresholds Console and modifying the parameters in a setting are described in *“Introduction to the Polling and Thresholds Console” on page 138* and *“Working with groups and settings” on page 144*.

When a VLAN becomes a member of a VLAN impact propagation group that has ImpactPropagation = DISABLED, the IP Manager sets the following attribute of the VLAN to FALSE:

```
isImpactPropOverVLANEnabled
```

For a VLAN that has isImpactPropOverVLANEnabled = FALSE, impact propagation for the VLAN is prevented.

For a VLAN that has isImpactPropOverVLANEnabled = TRUE (the default), impact propagation for the VLAN is allowed.

Default device access setting

The Device Access tab of the Polling and Thresholds Console provides a single default device access setting named CLI Access Setting. Default values for the CLI Access Setting lists the CLI Access Setting parameters.

Table 14-12. Default values for the CLI Access Setting

Parameter	Default Value	Description
AccessProtocol	TELNETSSH1SSH2 Default: TELNET	Determines the remote-access application to use to establish connections to the managed routing devices that belong to this group. **Note** Selecting SSH1 or SSH2 requires configuring an SSH client on the Network Protocol Manager host.
Enable	A structure having the following default value: {NULL String,ENCRYPTED}	Specifies the enable password for the managed devices that belong to this group. Type the enable password value twice to confirm the password value. There must be an entry for this parameter. **Note** IP Availability Manager uses the site key to encrypt the entered password value. As explained in VMware Smart Assurance System Administration Guide, The site key is created during the installation of VMware Smart Assurance applications.
LoginID	String of unspecified length Default: null string (empty)	Specifies the username (user ID) for the managed routing devices that belong to this group. There must be an entry for this parameter. If no username is configured on the devices that belong to this group, type any value; for example, cisco.
Password	String of unspecified length Default: null string (empty)	Specifies the password for the managed Cisco devices that belong to this group. Type the password value twice to confirm the password value. There must be an entry for this parameter unless the access protocol for this group is SSH1 or SSH2 and passwordless authentication is in effect. **Note** IP Availability Manager uses the site key to encrypt the entered password value. As explained in VMware Smart Assurance System Administration Guide, the site key is created during the installation of VMware Smart Assurance applications.
Timeout	1 to 496 seconds Default: 10 seconds	Sets the amount of time to wait for a Telnet/SSH response before the Telnet /SSH session request times out.

Default tagging filter groups and settings

Using the default tagging filter groups for the IP Manager, you create IP tag filter groups to control the naming of the IP addresses gathered from the systems in the managed network environment.

Default tagging groups

The IP Manager provides two default tagging groups:

- IP Tag Filter-1

- Other Filters

  Default tagging groups lists the default tagging groups, their matching criteria, and their settings. The matching-criteria target class for tagging groups is UnitaryComputerSystem.

Table 14-13. Default tagging groups

Tagging group	Matching criteria	Default settings
IP Tag Filter-1	UnitaryComputerSystem attributes: ■ Name = *	IP Tagging Policy
Other Filters	UnitaryComputerSystem attributes: ■ No attributes	IP Tagging Policy

The Other Filters tag group does not contain any matching-criteria attributes and has the lowest priority. Systems that do not match the criteria for the IP Tag Filter-1 tag group become members of the Other Filters tag group.

Default tagging settings

A single default tagging setting named IP Tagging Policy is provided by the IP Availability Manager. The IP Tagging Policy setting configures the IP tagging for a system. Default values for the IP Tagging Policy setting lists the IP Tagging Policy setting parameters, and Parameters of default setting IP Tagging Policy shown in a single view shows all of the parameters in a single view.

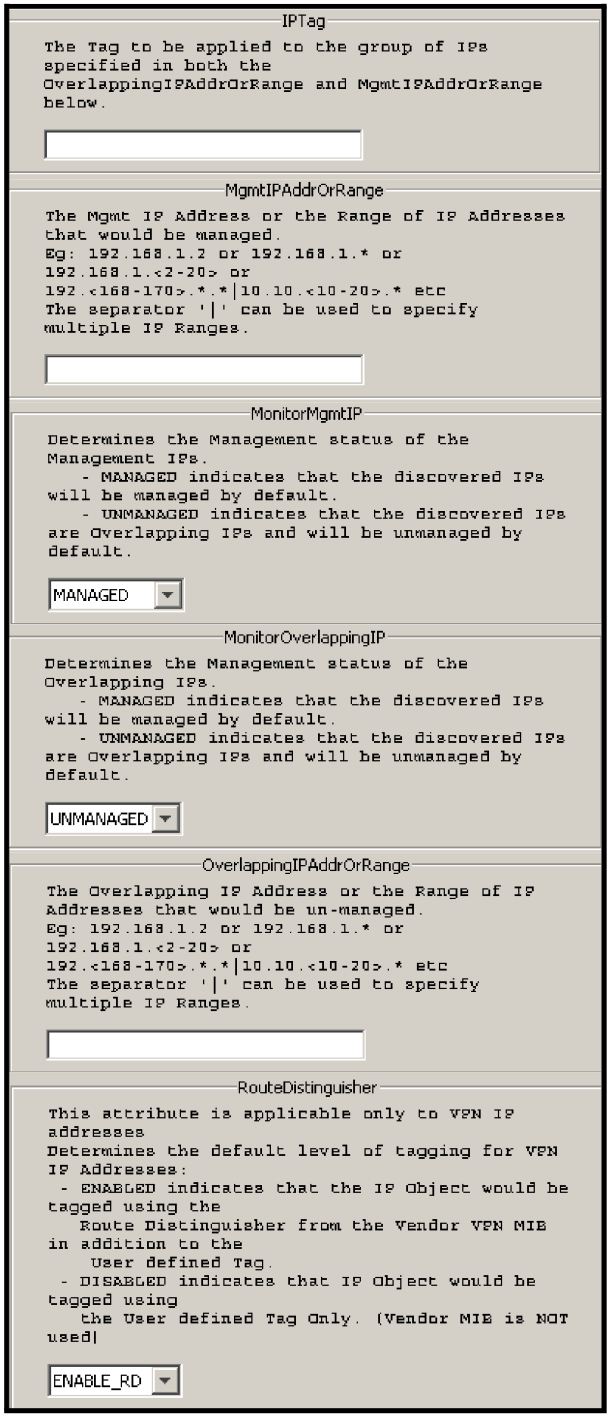
Table 14-14. Default values for the IP Tagging Policy setting

Parameter	Value	Description
IPTag	String of unspecified length Default: Null string (empty)	Specifies the name to be assigned to this tag. This tag will be applied to the IP addresses falling within the ranges that are specified for the OverlappingIPAddrOrRange and MgmtIPAddrOrRange parameters.
MgmtIPAddrOrRange	String of unspecified length Default: Null string (empty)	Specifies the IP address or range of IP addresses to be managed by default. Use the pattern matching criteria in Chapter 17 Wildcard Patterns For example: ■ 192.168.1.2 or 192.168.1.* ■ 192.168.1.<2-20> ■ 192.<168-170>.*.*|10.10.<10-20>.* The pipe (|) separator can be used to specify multiple IP ranges.
MonitorMgmtIP	MANAGED,UNMANAGED Default: MANAGED	Determines the management status to be assigned to the IP addresses falling within the range of the MgmtIPAddrOrRange parameter: ■ MANAGED Indicates that the discovered IP addresses are to be managed. ■ UNMANAGED Indicates that the discovered IP addresses are to be unmanaged.

Table 14-14. Default values for the IP Tagging Policy setting (Continued)

Parameter	Value	Description
MonitorOverlappingIP	MANAGED,UNMANAGED Default: UNMANAGED	Determines the management status to be assigned to the IP addresses falling within the range of the OverlappingIPAddrOrRange parameter: ■ MANAGED Indicates that the discovered IP addresses are to be managed. ■ UNMANAGED Indicates that the discovered IP addresses are to be unmanaged.
OverlappingIPAddrOrRange	String of unspecified length Default: Null string (empty)	Specifies the IP address or range of IP addresses to be unmanaged by default. Use the pattern matching criteria in Chapter 17 Wildcard Patterns For example: ■ 192.168.1.2 or 192.168.1.* ■ 192.168.1.<2-20> ■ 192.<168-170>.*.*|10.10.<10-20>.* The pipe (|) separator can be used to specify multiple IP ranges.
RouteDistinguisher	ENABLE_RD,DISABLE_RD Default: ENABLE_RD	Determines the level of tagging for VPN-IP (VRF IP) addresses: ■ ENABLE_RD Indicates that the IP objects created for the VRF IP addresses falling within the range that is specified for the OverlappingIPAddrOrRange parameter are to be tagged by using the route distinguisher from the vendor VPN MIB, in addition to the user-defined tag that is specified in the IPTag parameter. ■ DISABLE_RDIndicates that the IP objects created for the VRF IP addresses falling within the range that is specified for the OverlappingIPAddrOrRange parameter are *not* to be tagged by using the route distinguisher from the vendor VPN MIB; only the user-defined tag that is specified in the IPTag parameter is to be used to tag these IP objects.

Figure 14-1. Parameters of default setting IP Tagging Policy shown in a single view



Possible adapter startup errors

This section describes possible errors which could occur in the startup of the adapter.

1 Could not find correct *<adapter_name>.conf*

The adapter could not find the *<adapter_name>.conf* file in the *BASEDIR /SAM/smarts/*local/conf/audit_parse directory. In this case, the following error is written to the *<adapter_name>.log* file.

```
ERROR: Could not find adapter conf file named: audit_parse/IC-SAM-AUDIT.conf
```

2 Could not find an existing *<server_name>_audit.log*

The name of this file is specified in *<adapter_name>.conf*. If there is a misspelling in the configuration file, or the raw audit log file does not exist, the following error will be written to the *<adapter_name>.log* file:

```
ASL-W-ERROR_RULE_SOURCE-While executing rule set
'/work/clv/citigroup/62branch/smarts/install/solaris2.8-sparc/debug/local/
    rules/audit_parse/init.asl'
 ASL-ERROR_ACTION-While executing action at:
 ASL-CALL_STACK_RULE-   RuleName: START_AUDIT_PARSE, Line: 55
 ASL-CALL_STACK_RULE-   RuleName: EOF, Line: 37
 ASL-ERROR_INVOKE-While attempting to invoke operation 'startWithParameters'
    of object 'GA_Driver::PARSE_AUDIT_LOG_DRIVER'
 ASL-ERROR_INIT_FRONTEND-While initializing front-end
 ASL-ERROR_FILEFE_OPEN-Could not open input file
    '/opt/InCharge6/SAM/smarts/local/logs/IC-SAM_audit.log'
 CI-ESPEC-While attempting to locate file with primary
    "/opt/InCharge6/SAM/smarts/local/logs/IC-SAM_audit.log", default "??2?", and related "?3?"
 <SYS>-ENOENT-No such file or directory
```

Polling and Threshold Settings

15

This chapter includes the following topics:

- Default polling groups
- Polling settings
- Default threshold groups
- Threshold settings

Default polling groups

The IP Manager provides a polling category named “Polling Groups,” which contains the following default polling groups:

- ComputeFabric
- MediaGateways
- 5620 SAM Managed Systems
- Proxy Devices
- Switches
- WirelessControllers
- WirelessAccessPoints
- WirelessClients
- Routers
- Hubs and Bridges
- Other Systems

  Default polling groups for the IP Manager shows the default polling groups, their target classes and matching criteria, and their default settings. The target class for all polling groups is UnitaryComputerSystem.

Table 15-1. Default polling groups for the IP Manager

Polling group	Target class and matching criteria	Default polling settings
ComputeFabric	Description = *Version*\(1.4*\)* SystemObjectID = .1.3.6.1.4.1.9.12.3.1.3.847 | .1.3.6.1.4.1.9.12.3.1.3.899	Cleanup Unused Monitoring Instances Connectivity Polling Environment Polling Performance Polling - Processor and Memory
MediaGateways	Type = MEDIAGATEWAY	Cleanup Unused Monitoring Instances Connectivity Polling Connectivity Polling for IPv6 Addresses Environment Polling Performance Polling - Ports and Interfaces Performance Polling - Processor and Memory
5620 SAM Managed Systems	UnitaryComputerSystem with attributes: ■ IsManaged = TRUE ■ ServiceName = [-~]* ■ Type = SWITCH|ROUTER ■ Vendor = Alcatel*	Connectivity Polling - External Poller Environment Polling - External Poller
Proxy Devices	UnitaryComputerSystem with attributes: ■ IsProxy = TRUE	Connectivity Polling - External Poller
Switches	UnitaryComputerSystem with attributes: ■ IsManaged = TRUE ■ Type = SWITCH |VIRTUALSWITCH	Cleanup Unused Monitoring Instances Connectivity Polling Connectivity Polling for IPv6 Addresses Environment Polling Performance Polling - Ports and Interfaces Performance Polling - Processor and Memory
WirelessControllers	CreationClassName = WirelessController	GarbageCollection_Setting Connectivity_Polling_Setting Connectivity_Polling_IPv6_Setting Processor_PerformancePolling_Setting System_EnvironmentPolling_Setting NetworkAdapter_PerformancePolling_Setting Wireless_PerformancePolling_Setting
WirelessAccessPoints	CreationClassName = WirelessAccessPoint	GarbageCollection_Setting Connectivity_Polling_Setting Connectivity_Polling_IPv6_Setting Processor_PerformancePolling_Setting System_EnvironmentPolling_Setting NetworkAdapter_PerformancePolling_Setting Wireless_PerformancePolling_Setting
WirelessClients	Type = WIRELESSCLIENT	GarbageCollection_Setting **Note** By default, WirelessClient monitoring is disabled. Add Connectivity setting to WirelessClient group to enable it.

Table 15-1. Default polling groups for the IP Manager (Continued)

Polling group	Target class and matching criteria	Default polling settings
Routers	UnitaryComputerSystem with attributes: ■ IsManaged = TRUE ■ Type = ROUTER	Cleanup Unused Monitoring Instances Connectivity Polling Connectivity Polling for IPv6 Addresses Default IP_Route Connectivity Polling Environment Polling Performance Polling - Ports and Interfaces Performance Polling - Processor and Memory
Hubs and Bridges	UnitaryComputerSystem with attributes: ■ IsManaged = TRUE ■ Type = HUB|BRIDGE	Cleanup Unused Monitoring Instances Connectivity Polling Connectivity Polling for IPv6 Addresses
Other Systems	UnitaryComputerSystem with attribute: ■ IsManaged = TRUE	Cleanup Unused Monitoring Instances Connectivity Polling Connectivity Polling for IPv6 Addresses FileSystem Polling Performance Polling - Processor and Memory

Three points to note about Default polling groups for the IP Manager:

- The “Other Systems” polling group has the lowest priority. Managed systems that do not match the criteria for the other polling groups become members of the Other Systems polling group. For example, managed host systems become members of the Other Systems polling group.
- Only discovered objects that match the type and attribute values in the “Target class and matching criteria” column for a particular group can become members of that group.
- By default, all discovered objects that match the type and attribute values in the "Target class and matching criteria" column for a particular group become members of that group.

  You can specify matching criteria for a polling group to limit its membership, as explained in *“Editing matching criteria” on page 146.*.

Polling settings

The IP Manager polling settings are shown in Polling settings for the IP Manager.

Table 15-2. Polling settings for the IP Manager

Polling setting	Type
Cleanup Unused Monitoring Instances	Optimization Described in *“Polling setting for optimization” on page 156.*
Connectivity Polling	Availability monitoring Described in *“” on page 156.*
Connectivity Polling - External Poller	
Connectivity Polling for IPv6 Addresses	
Connectivity Polling for IPv6 Addresses - External Poller	
Default IP_Route Connectivity Polling	

Table 15-2. Polling settings for the IP Manager (Continued)

Polling setting	Type
Environment Polling	Performance monitoring Described in *"Polling settings for IP performance monitoring" on page 162.*
Environment Polling - External Poller	
FileSystem Polling	
Performance Polling - Ports and Interfaces	
Performance Polling - Processor and Memory	

In general, a group category, such as "Polling Groups," has a set of settings that are available to any group in the group category. Thus, all polling settings are available to each of the default polling groups.

But even though you can apply any polling setting to any default polling group, not all group-to-setting mappings are valid. The default group-to-setting mappings in Polling settings are the mappings that users would typically use.

Polling settings for IP availability monitoring

Through the polling settings for IP availability monitoring, you control the ICMP and SNMP connectivity polling of the managed network objects in your network. The polled information serves as input to IP Availability Manager's availability analysis of switches, routers, hubs, bridges, and other systems.

Connectivity polling setting parameters

Default values for the Connectivity Polling setting lists the Connectivity Polling setting parameters.

Table 15-3. Default values for the Connectivity Polling setting

Parameter	Default value	Description
AnalysisMode	ENABLED,DISABLED Default: ENABLED	Enables or disables connectivity polling and the subsequent availability analysis of the polled data.
MaximumLatency	0 to 3600 milliseconds Default: 0 milliseconds	Applicable to ICMP polling:Maximum round-trip time between an ICMP request and the subsequent ICMP response. MaximumLatency = 0 disables the ICMP latency feature, and MaximumLatency = <non-zero value> enables the ICMP latency feature.
PingControl	ENABLED,DISABLED Default: DISABLED	Applicable to ICMP polling:Enables or disables PingInterval and PingRetries. When PingControl is enabled, you can use PingInterval and PingRetries to control ICMP polling.
PingInterval	20 to 3600 seconds Default: 20 seconds	Applicable to ICMP polling:Time between successive ICMP polls.
PingRetries	0 to 10 retries Default: 3	Applicable to ICMP polling:Number of retry polls to perform when the initial ICMP poll fails.
PollingInterval	30 to 3600 seconds Default: 240 seconds	Applicable to SNMP polling:Time between successive SNMP polls.

Table 15-3. Default values for the Connectivity Polling setting (Continued)

Parameter	Default value	Description
Retries	0 to 10 retries Default: 3	Applicable to SNMP polling:Number of retry polls to perform when the initial SNMP poll fails.
Timeout	10 to 10000 milliseconds Default: 700 milliseconds	Applicable to both ICMP and SNMP polling:Amount of time to wait for the poll response before the first poll request times out. The timeout value doubles for each successive retry. For Timeout=700 msec (0.7 sec) and Retries=3: ■ 0.7 seconds for first retry ■ 1.4 seconds for second retry ■ 2.8 seconds for third retry

Default values for the Connectivity Polling for IPv6 Addresses setting lists the Connectivity Polling for IPv6 Addresses setting parameters.

Table 15-4. Default values for the Connectivity Polling for IPv6 Addresses setting

Parameter	Default value	Description
AnalysisMode	ENABLED,DISABLED Default: ENABLED	Enables or disables connectivity polling and the subsequent availability analysis of the polled data.
PollingInterval	30 to 3600 seconds Default: 240 seconds	Applicable to both ICMP and SNMP polling:Time between successive connectivity polls.
Retries	0 to 10 retries Default: 3	Applicable to both ICMP and SNMP polling:Number of retry polls to perform when the initial poll fails.
Timeout	10 to 10000 milliseconds Default: 700 milliseconds	Applicable to both ICMP and SNMP polling:Amount of time to wait for the poll response before the first poll request times out. The timeout value doubles for each successive retry. For Timeout=700 msec (0.7 sec) and Retries=3: ■ 0.7 seconds for first retry ■ 1.4 seconds for second retry ■ 2.8 seconds for third retry

External poller settings

The following are external poller settings:

- Connectivity Polling—External Poller
- Connectivity Polling for IPv6 Addresses—External Poller

The settings serve three purposes:

- Provide a means of testing the system (v4 or v6) instrumentation of the IP Availability Manager.
- Provide a means of testing the system (v4 or v6) analysis functionality of the IP Availability Manager.

- Provide a means for the IP Availability Manager to import system (v4 or v6) status updates from an VMware Smart Assurance adapter, such as the VMware Smart Assurance Adapter for Alcatel-Lucent 5620 SAM EMS.

  Default values for the Connectivity Polling—External Poller setting lists the Connectivity Polling—External Poller setting parameters.

Table 15-5. Default values for the Connectivity Polling—External Poller setting

Parameter	Default value	Description
AnalysisMode	ENABLED,DISABLED Default: ENABLED	Enables or disables the collection and analysis of data from an external source.
InitialStatus	UP,UNKNOWN Default: UNKNOWN	Determines the desired initial state for the stored instrumentation objects. Initial status value can be UP or UNKNOWN.
InstrumentCards	TRUE,FALSE Default: FALSE	Determines whether stored instrumentation objects are created for Card objects. If TRUE, stored instrumentation objects are created for Card objects. If FALSE, no stored instrumentation objects are created for Card objects.
InstrumentIPs	TRUE,FALSE Default: TRUE	Determines whether stored instrumentation objects are created for IP objects. If TRUE, stored instrumentation objects are created for IP objects. If FALSE, no stored instrumentation objects are created for IP objects.
InstrumentNetwork-Adapters	TRUE,FALSE Default: TRUE	Determines whether stored instrumentation objects are created for interface and port objects. If TRUE, stored instrumentation objects are created for interface and port objects. If FALSE, no stored instrumentation objects are created for interface and port objects.
InstrumentSNMP-Agents	TRUE,FALSE Default: TRUE	Determines whether stored instrumentation objects are created for SNMP agent objects. If TRUE, stored instrumentation objects are created for SNMP agent objects. If FALSE, no stored instrumentation objects are created for SNMP agent objects.

Default values for the Connectivity Polling for IPv6 Addresses—External Poller setting lists the Connectivity Polling for IPv6 Addresses—External Poller setting parameters.

Table 15-6. Default values for the Connectivity Polling for IPv6 Addresses—External Poller setting

Parameter	Default value	Description
AnalysisMode	ENABLED,DISABLED Default: ENABLED	Enables or disables the collection and analysis of data from an external source.
InitialStatus	UP,UNKNOWN Default: UNKNOWN	Determines the desired initial state for the stored instrumentation objects. Initial status value can be UP or UNKNOWN.
InstrumentIPv6s	TRUE,FALSE Default: TRUE	Determines whether stored instrumentation objects are created for IPv6 objects. If TRUE, stored instrumentation objects are created for IPv6 objects. If FALSE, no stored instrumentation objects are created for IPv6 objects.

Default IP_Route Connectivity Polling setting

The Default IP_Route Connectivity Polling setting determines the polling intervals that are used by the IP Availability Manager to monitor default routes. The IP Availability Manager monitors the default routes by probing the SNMP ipRouteTable (.1.3.6.1.2.1.4.21.0.0.0.0) on certain router devices.

Default values for the Default IP_Route Connectivity Polling setting lists the Default IP_Route Connectivity Polling setting parameters.

Table 15-7. Default values for the Default IP_Route Connectivity Polling setting

Parameter	Default value	Description
AnalysisMode	ENABLED,DISABLED Default: ENABLED	Enables or disables default-route polling and the subsequent availability analysis of the polled data.
PollingInterval	30 to 3600 seconds Default: 240 seconds	Time between successive polls for default-route data.
Retries	0 to 10 retries Default: 3	Number of retry polls to perform when the initial poll fails.
Timeout	10 to 10000 milliseconds Default: 700 milliseconds	Amount of time to wait for the poll response before the first poll request times out. The timeout value doubles for each successive retry. For Timeout=700 msec (0.7 sec) and Retries=3: ■ 0.7 seconds for first retry ■ 1.4 seconds for second retry ■ 2.8 seconds for third retry

Polling settings for IP performance monitoring

Through the polling settings for IP performance monitoring, you control the ICMP and SNMP performance polling of the managed network objects in your network. The polled information serves as input to IP Performance Manager‘s fault and performance analysis of interfaces and ports, processors and memory, disks and filesystems, fans and power supplies, and voltage and temperature sensors.

Environment Polling setting

The Environment Polling setting configures the polling intervals that are used to monitor system components such as the fan, memory, power supply, temperature sensor, and voltage sensor objects.

Default values for the Environment Polling setting lists the Environment Polling setting parameters.

Table 15-8. Default values for the Environment Polling setting

Parameter	Default value	Description
AnalysisMode	ENABLED,DISABLED Default: ENABLED	Enables or disables environment polling and the subsequent performance analysis of the polled data.
PollingInterval	30 to 3600 seconds Default: 240 seconds	Time between successive polls for environment data.
Retries	0 to 10 retries Default: 3	Number of retry polls to perform when the initial poll fails.
Timeout	10 to 10000 milliseconds Default: 700 milliseconds	Amount of time to wait for the poll response before the first poll request times out. The timeout value doubles for each successive retry. For Timeout=700 msec (0.7 sec) and Retries=3: ■ 0.7 seconds for first retry ■ 1.4 seconds for second retry ■ 2.8 seconds for third retry

Environment Polling - External Poller

The Environment Polling - External Poller setting serves two purposes:

- Provides a means of testing the system-component instrumentation and analysis functionality of the IP Performance Manager.
- Provides a means for the IP Performance Manager to import system-component status updates from an VMware Smart Assurance adapter, such as the VMware Smart Assurance Adapter for Alcatel-Lucent 5620 SAM EMS.

  Default values for the Environment Polling - External Poller setting lists the Environment Polling - External Poller setting parameters.

Table 15-9. Default values for the Environment Polling - External Poller setting

Parameter	Default value	Description
AnalysisMode	ENABLED,DISABLED Default: ENABLED	Enables or disables the collection and analysis of system-component data from an external source.
InitialStatus	UP,UNKNOWN Default: UNKNOWN	Determines the desired initial state for the stored instrumentation objects. Initial status value can be UP or UNKNOWN.

Table 15-9. Default values for the Environment Polling - External Poller setting (Continued)

Parameter	Default value	Description
InstrumentFans	TRUE,FALSE Default: TRUE	Determines whether stored instrumentation objects are created for fan objects. If TRUE, stored instrumentation objects are created for fan objects. If FALSE, no stored instrumentation objects are created for fan objects.
InstrumentMemory	TRUE,FALSE Default: TRUE	Determines whether stored instrumentation objects are created for memory objects. If TRUE, stored instrumentation objects are created for memory objects. If FALSE, no stored instrumentation objects are created for memory objects.
InstrumentPowerSupply	TRUE,FALSE Default: TRUE	Determines whether stored instrumentation objects are created for power supply objects. If TRUE, stored instrumentation objects are created for power supply objects. If FALSE, no stored instrumentation objects are created for power supply objects.
InstrumentSNMP-Agents	TRUE,FALSE Default: TRUE	Determines whether stored instrumentation objects are created for SNMP agent objects. If TRUE, stored instrumentation objects are created for SNMP agent objects. If FALSE, no stored instrumentation objects are created for SNMP agent objects.
InstrumentTemperatur-Sensors	TRUE,FALSE Default: TRUE	Determines whether stored instrumentation objects are created for temperature sensor objects. If TRUE, stored instrumentation objects are created for temperature sensor objects. If FALSE, no stored instrumentation objects are created for temperature sensor objects.
InstrumentVoltage-Sensors	TRUE,FALSE Default: TRUE	Determines whether stored instrumentation objects are created for voltage sensor objects. If TRUE, stored instrumentation objects are created for voltage sensor objects. If FALSE, no stored instrumentation objects are created for voltage sensor objects.

FileSystem Polling setting

The FileSystem Polling setting configures the polling intervals that are used to monitor a host system's filesystem. This setting is a valid choice only for the Other Systems polling group.

Table 147 on page 278 lists the FileSystem Polling setting parameters.

Table 15-10. Default values for the FileSystem Polling setting

Parameter	Default value	Description
AnalysisMode	ENABLED,DISABLED Default: ENABLED	Enables or disables filesystem polling and the subsequent performance analysis of the polled data.
PollingInterval	30 to 3600 seconds Default: 240 seconds	Time between successive polls for filesystem data.

Table 15-10. Default values for the FileSystem Polling setting (Continued)

Parameter	Default value	Description
Retries	0 to 10 retries Default: 3	Number of retry polls to perform when the initial poll fails.
Timeout	10 to 10000 milliseconds Default: 700 milliseconds	Amount of time to wait for the poll response before the first poll request times out. The timeout value doubles for each successive retry. For Timeout=700 msec (0.7 sec) and Retries=3: ■ 0.7 seconds for first retry ■ 1.4 seconds for second retry ■ 2.8 seconds for third retry

Performance Polling - Ports and Interfaces setting

The Performance Polling - Ports and Interfaces setting configures the polling intervals that are used to monitor the performance of managed ports and interfaces.

Default values for the Performance Polling - Ports and Interfaces setting lists the Performance Polling - Ports and Interfaces setting parameters.

Table 15-11. Default values for the Performance Polling - Ports and Interfaces setting

Parameter	Default value	Description
AnalysisMode	ENABLED,DISABLED Default: ENABLED	Enables or disables port and interface polling and the subsequent performance analysis of the polled data.
PollingInterval	30 to 3600 seconds Default: 240 seconds	Time between successive polls for interface and trunk port data.
PollingInterval_Access-Ports	30 to 3600 seconds 1200 seconds	Time between successive polls for access port data.
Retries	0 to 10 retries Default: 3	Number of retry polls to perform when the initial poll fails.
Timeout	10 to 10000 milliseconds Default: 700 milliseconds	Amount of time to wait for the poll response before the first poll request times out. The timeout value doubles for each successive retry. For Timeout=700 msec (0.7 sec) and Retries=3: ■ 0.7 seconds for first retry ■ 1.4 seconds for second retry ■ 2.8 seconds for third retry

Performance Polling - Processor and Memory setting

The Performance Polling - Processor and Memory setting configures the polling intervals that are used to monitor a system's processor and associated memory objects.

Default values for the Performance Polling - Processor and Memory setting lists the Performance Polling - Processor and Memory setting parameters.

Table 15-12. Default values for the Performance Polling - Processor and Memory setting

Parameter	Default value	Description
AnalysisMode	ENABLED,DISABLED Default: ENABLED	Enables or disables processor and memory polling and the subsequent performance analysis of the polled data.
PollingInterval	30 to 3600 seconds Default: 240 seconds	Time between successive polls for processor and memory data.
Retries	0 to 10 retries Default: 3	Number of retry polls to perform when the initial poll fails.
Timeout	10 to 10000 milliseconds Default: 700 milliseconds	Amount of time to wait for the poll response before the first poll request times out. The timeout value doubles for each successive retry. For Timeout=700 msec (0.7 sec) and Retries=3: ■ 0.7 seconds for first retry ■ 1.4 seconds for second retry ■ 2.8 seconds for third retry

Default threshold groups

The IP Manager provides the following categories of threshold groups, each of which contains default threshold groups:

- AggregatePortGroup
  - AggregatePort
- File systems
  - FileSystems
- Interface Groups
  - 1 GB Ethernet
  - 10/100 MB Ethernet
  - ATM
  - Token Ring
  - ISDN Physical Interface
  - ISDN B Channel
  - ISDN D Channel
  - Serial
  - FDDI
  - Backup
  - Dial-on-Demand
  - Other Interfaces

- Port Groups - Access Ports
  - 1 GB Ethernet
  - 10/100 MB Ethernet
  - ATM
  - Other Ports
- Port Groups - Trunk Ports
  - 1 GB Ethernet
  - 10/100 MB Ethernet
  - ATM
  - Other Ports
- System Resource Groups
  - ComputeFabric
  - Switches
  - WirelessControllers
  - WirelessAccessPoints
  - Routers
  - Hubs and Bridges
  - MediaGateway
  - Other Systems
- System VLAN Tag Groups
  - Systems
  - Other systems
- TemperatureSensor
  - TemperatureSensor
- VoltageSensor
  - VoltageSensor
- VLAN Impact Propagation Groups

  The “VLAN Impact Propagation Groups” category does not automatically appear. As explained in *“Creating VLAN impact propagation group objects” on page 200*, You must issue a certain command for the VLAN Impact Propagation Groups category to appear.

AggregatePortGroup

Default Threshold group

Default threshold group and matching criteria for AggregatePortGroup lists the default threshold group and matching criteria for AggregatePortGroup.

Table 15-13. Default threshold group and matching criteria for AggregatePortGroup

Threshold Group	Matching criteria	Default Settings
AggregatePort	CreationClassName=AggregatePort	DiscrepancyThreshold

Default Threshold setting

Threshold setting for Discrepancy Threshold lists the parameters for the setting Discrepancy Threshold.

Table 15-14. Threshold setting for Discrepancy Threshold

Parameter	Default value	Description
UtilizationDiscrepancyThreshold	25	This is the discrepancy value of the individual link usage in percentage, which should not exceed. When this value exceeds the default value, the *UnbalancedAdapterUtilization* event is generated.

File systems

File System Management functionality allows you to define and configure thresholds for file system space utilization.

Events and thresholds for File systems

Events and thresholds for File systems provides the events and thresholds along with their description.

Table 15-15. Events and thresholds for File systems

Events	Utilization threshold	Description of threshold	Default value	Condition
HighUtilization **Note** Severity level: Major	MaxUtilizationPct	The percentage of total size currently in use.	95% **Note** User can change this value for each file system instance.	This event is generated when the utilization threshold exceeds the configured threshold value. **Note** This threshold has greater priority over the ModerateUtilization event.
ModerateUtilization **Note** Severity level: Minor	ModerateUtilization Pct	Moderate threshold for percentage of total size currently in use.	80% **Note** User can change this value for each file system instance.	This event is generated when the utilization threshold exceeds the configured threshold value.
LowAvailableSpace **Note** Severity level: Minor	MinAvailableSpace	The available space is less than the minimum available space.	1024 **Note** User can change this value for each file system instance.	This event is generated when the utilization threshold exceeds the configured threshold value.

Sample File system groups and matching criteria

Sample File system groups and matching criteria lists sample file system groups along with their matching criteria. You can use these as a guide to create file system groups manually.

Table 15-16. Sample File system groups and matching criteria

File system group	Description	Matching Criteria
OS Only File Systems	Configures all Linux file system instances that match the criteria.	The default matching criteria is the Filesystem attribute "Root" to match the value /. All file system instances with the "Root" attribute value as "/" (single forward slash) will fall in this group.
Writable File Systems	Configures all Linux file system instances that match the criteria.	The default matching criteria is the Filesystem attribute "Root" to match the value "/var". All file system instances with the "Root" attribute value as "/var" will fall under this group.
Temporary File Systems	Configures all Linux file system instances that match the criteria.	The default matching criteria is the Filesystem attribute "Root" to match the value "/temp". All file system instances with the "Root" attribute value as "/temp" will fall under this group.
Non Critical File Systems	Configures all Linux file system instances that match the criteria.	No default matching criteria provided, and will match all the file system instances.
Unclassified File Systems	Configures all Linux file system instances that match the criteria.	No default matching criteria provided, and will match all the file system instances.

Attribute of File system management describes the attribute for a file system instance.

Table 15-17. Attribute of File system management

Attribute	Description	Allowed values
IsManaged	Determines if a file system instance should be monitored by the management system. An unmanaged object does not have any associated instrumentation. This attribute is read-only.	Boolean: TRUE, FALSE Default: TRUE

Interface Groups

Threshold groups for interfaces are used to configure parameters for interface analysis. Thresholds are determined by the interface's media type (for example, Ethernet or ATM) and its role (primary, backup, or dial-on-demand).

Default interface threshold groups for the IP Manager shows the default interface threshold groups, their target classes and matching criteria, and their default settings. The target class for all interface threshold groups is Interface.

Table 15-18. Default interface threshold groups for the IP Manager

Interface groups	Target class and matching criteria	Default threshold settings
1 Gb Ethernet	Interface with attributes: ■ IsManaged = TRUE ■ MaxSpeed = 1000000000 ■ Type = *ETHER*|*CSMACD*	Ethernet Interface/Port Performance
10/100 Mb Ethernet	Interface with attributes: ■ IsManaged = TRUE ■ Type = *ETHER*|*CSMACD*	Ethernet Interface/Port Performance
ATM	Interface with attributes: ■ IsManaged = TRUE ■ Type = *ATM*	Generic Interface/Port Performance Interface/Port Flapping
Token Ring	Interface with attributes: ■ IsManaged = TRUE ■ Type = *TOKEN*	Generic Interface/Port Performance
ISDN Physical Interface	Interface with attributes: ■ IsManaged = TRUE ■ InterfaceCode = *ISDNPHYSICAL*	Generic Interface/Port Performance Interface/Port Flapping
ISDN B Channel	Interface with attributes: ■ IsManaged = TRUE ■ InterfaceCode = *ISDNBCHANNEL*	Backup Interface Support
ISDN D Channel	Interface with attributes: ■ IsManaged = TRUE ■ InterfaceCode = *ISDNDCHANNEL*	Interface/Port Flapping

Table 15-18. Default interface threshold groups for the IP Manager (Continued)

Interface groups	Target class and matching criteria	Default threshold settings
Serial	Interface with attributes: ■ IsManaged = TRUE ■ Type = *Serial*|*FrameRelay*	Generic Interface/Port Performance Interface/Port Flapping
FDDI	Interface with attributes: ■ IsManaged = TRUE ■ Type = *FDDI*	Generic Interface/Port Performance
Backup	Interface with attributes: ■ IsManaged = TRUE ■ Type = *ISDN*	Backup Interface Support
Dial-On-Demand	Interface with attributes: ■ IsManaged = TRUE ■ Type = *PPP*|*SLIP*	Dial-On-Demand Interface Support
Other Interfaces	Interface with attribute: ■ IsManaged = TRUE	Interface/Port Flapping

Four things to note about Default interface threshold groups for the IP Manager:

- The default group-to-setting mappings in the table are the mappings that users would typically use. The settings that are available to an interface threshold group are as follows:
  - Backup Interface Support
  - Dial-on-Demand Interface Support
  - Disable Fault Analysis for Interface/Port
  - Disable Performance Analysis for Interface/Port
  - Ethernet Interface/Port Performance
  - Generic Interface/Port Performance
  - Interface/Port Flapping
- The “Other Interfaces” threshold group has the lowest priority. Managed interfaces that do not match the criteria for the other interface threshold groups become members of the Other Interfaces threshold group.
- Only discovered objects that match the type and attribute values in the “Target class and matching criteria” column for a particular group can become members of that group.
- By default, all discovered objects that match the type and attribute values in the "Target class and matching criteria" column for a particular group become members of that group.

  You can specify matching criteria for a threshold group to limit its membership, as explained in *“Editing matching criteria” on page 146*.

Port Groups - Access Ports

Threshold groups for access ports are used to configure parameters for access port analysis. Thresholds are determined by the access port's media type; for example, Ethernet or ATM.

An access port is a port that provides a connection for end users or node devices, such as routers or servers. An access port becomes managed if it has a connection or is explicitly managed.

Default access port threshold groups for the IP Manager shows the default access port threshold groups, their target classes and matching criteria, and their default settings. The target class for all access port threshold groups is Port.

Table 15-19. Default access port threshold groups for the IP Manager

Access port group	Target class and matching criteria	Default settings
1 Gb Ethernet	Port with attributes: ■ IsManaged = TRUE ■ IsConnector = FALSE ■ Max Speed = 1000000000 ■ Type = *ETHER*|*CSMACD*	Ethernet Interface/Port Performance
10/100 Mb Ethernet	Port with attributes: ■ IsManaged = TRUE ■ IsConnector = FALSE ■ Type = *ETHER*|*CSMACD*	Ethernet Interface/Port Performance
ATM	Port with attributes: ■ IsManaged = TRUE ■ IsConnector = FALSE ■ Type = *ATM*	Generic Interface/Port Performance
Other Ports	Port with attributes: ■ IsManaged = TRUE ■ IsConnector = FALSE	Generic Interface/Port Performance

Two things to note about Default access port threshold groups for the IP Manager:

- The default group-to-setting mappings in the table are the mappings that users would typically use. The settings that are available to an access port threshold group are as follows:
  - Disable Fault Analysis for Interface/Port
  - Disable Performance Analysis for Interface/Port
  - Ethernet Interface/Port Performance
  - Generic Interface/Port Performance
  - Interface/Port Flapping
- The "Other Ports" threshold group has the lowest priority. Managed access ports that do not match the criteria for the other access port threshold groups become members of the Other Ports threshold group.

Port Groups - Trunk Ports

Threshold groups for trunk ports are used to configure parameters for trunk port analysis. Thresholds are determined by the trunk port's media type; for example, Ethernet or ATM.

A trunk port is any port that connects to another port or interface on a device that participates in the Layer 2 bridging protocol. By default, all trunk ports are managed, which means that by default all trunk ports can be associated with trunk port threshold groups.

Because trunk ports are inherently more critical than access ports, trunk port threshold groups typically have lower thresholds than access port threshold groups for utilization, errors, and so on. That is, the thresholds for trunk port threshold groups are more stringent than the thresholds for access port threshold groups.

Default trunk port threshold groups for the IP Manager shows the default trunk port threshold groups, their target classes and matching criteria, and their default settings. The target class for all trunk port threshold groups is Port.

Table 15-20. Default trunk port threshold groups for the IP Manager

Trunk port groups	Target class and matching criteria	Default settings
1 Gb Ethernet	Port with attributes: ■ IsManaged = TRUE ■ IsConnector = TRUE ■ Max Speed = 1000000000 ■ Type = *ETHER*|*CSMACD*	Ethernet Interface/Port Performance
10/100 Mb Ethernet	Port with attributes: ■ IsManaged = TRUE ■ IsConnector = TRUE ■ Type = *ETHER*|*CSMACD*	Ethernet Interface/Port Performance
ATM	Port with attributes: ■ IsManaged = TRUE ■ IsConnector = TRUE ■ Type = *ATM*	Generic Interface/Port Performance
Other Ports	Port with attributes: ■ IsManaged = TRUE ■ IsConnector = TRUE	Generic Interface/Port Performance

Two things to note about Default trunk port threshold groups for the IP Manager:

- The default group-to-setting mappings in the table are the mappings that users would typically use. The settings that are available to a trunk port threshold group are as follows:
  - Disable Fault Analysis for Interface/Port
  - Disable Performance Analysis for Interface/Port
  - Ethernet Interface/Port Performance
  - Generic Interface/Port Performance

  - Interface/Port Flapping
- The “Other Ports” threshold group has the lowest priority. Managed trunk ports that do not match the criteria for the other trunk port threshold groups become members of the Other Ports threshold group.

System Resource Groups

Threshold groups for system resources are used to configure parameters for system analysis. The sensitivity of the system thresholds is determined by the role of the system.

Default system resource threshold groups for the IP Manager shows the default system resource threshold groups, their target classes and matching criteria, and their default settings. The target class for all system resource threshold groups is UnitaryComputerSystem.

Table 15-21. Default system resource threshold groups for the IP Manager

System resource group	Target class and matching criteria	Default threshold settings
Switches	UnitaryComputerSystem with attributes: ■ IsManaged = TRUE ■ Type = SWITCH ■ CreationClassName=~WirelessController|~WirelessAccessPoint	Connectivity Environment Processor and Memory
Routers	UnitaryComputerSystem with attributes: ■ IsManaged = TRUE ■ Type = ROUTER	Connectivity Environment Processor and Memory
Hubs and Bridges	UnitaryComputerSystem with attributes: ■ IsManaged = TRUE ■ Type = HUB|BRIDGE	Connectivity Environment Processor and Memory
Other Systems	UnitaryComputerSystem with attribute: ■ IsManaged = TRUE	Connectivity Environment FileSystem Processor and Memory
ComputeFabric	■ Description = ~*Version*\([0-1].[0-3]*\),* ■ SystemObjectID = .1.3.6.1.4.1.9.12.3.1.3.847|.1.3.6.1.4.1.9.12.3.1.3.899||.1.3.6.1.4.1.9.12.3.1.3.1062	Connectivity Environment Processor and Memory
WirelessControllers **Note** The priority of groups should be adjusted as required in both Polling tabs and Threshold Tab for System Resource Groups.	CreationClassName = WirelessController	Connectivity Environment Processor and Memory WirelessController Thresholds **Note** System Resource Groups lists the parameters for WirelessControllers Thresholds.

Table 15-21. Default system resource threshold groups for the IP Manager (Continued)

System resource group	Target class and matching criteria	Default threshold settings
WirelessAccessPoints **Note** The priority of groups should be adjusted as required in both Polling tabs and Threshold Tab for System Resource Groups.	CreationClassName = WirelessAccesspoints	Connectivity Environment Processor and Memory WirelessAccessPoints Thresholds **Note** System Resource Groups lists the parameters for WirelessAccessPoints Thresholds.
MediaGateway	Type = MEDIAGATEWAY	Connectivity Environment Processor and Memory

Two things to note about Default system resource threshold groups for the IP Manager:

- The default group-to-setting mappings in the table are the mappings that users would typically use. The settings that are available to a system resource threshold group are as follows:
  - Cisco Fast and NvRam Memory
  - Connectivity
  - Environment
  - FileSystem
  - Interface Management Policy
  - Juniper Environment
  - Processor and Memory
  - VLAN Tagging Policy
- The “Other Systems” group has the lowest priority. Managed systems that do not match the criteria for the other system resource threshold groups become members of the Other Systems group. For example, managed host systems become members of the Other Systems group.

Settings for WirelessController Thresholds

Settings for WirelessController Thresholds lists the default threshold settings for WirelessControllers.

Note *WirelessAccessPointThresholdExceeded* and *Wirelessclient ThresholdExceeded* events are generated depending on the threshold values.

Table 15-22. Settings for WirelessController Thresholds

Parameters	Default value	Description
MaxSupportedWirelessAccessPointsThreshold	99999	This is the maximum number of WirelessAccessPoints supported by the WirelessController. Valid range is from 0 to 99999.
MaxSupportedWirelessClientsThreshold	99999	This is the maximum number of WirelessClients supported by the WirelessController. Valid range is from 0 to 99999.
UseMIBValues	TRUE	When UseMIBValues=TRUE, then MIB values are used to get the count of the WirelessAccessPoint and WirelessClient, which are required to generate Threshold alarms. If the MIB does not have any value, then the discovered topology count is used. When UseMIBValues= FALSE, only discovered topology count is used.
UseMIBThresholds	TRUE	When UseMIBThresholds=TRUE, MIB values are used to get the Threshold valus for the WirelessAccessPoint and WirelessClient.If the MIB does not have any value, then the settings in the Threshold Window are used. When UseMIBThresholds=FALSE, the settings in the Threshold Window are used.

Settings for WirelessAccessPoints Thresholds

Settings for WirelessAccessPoints Thresholds lists the default threshold settings for WirelessAccessPoints.

Note WirelessClientThresholdExceeded event is generated depending on the threshold value.

Table 15-23. Settings for WirelessAccessPoints Thresholds

Threshold setting	Default value	Description
MaxSupportedWirelessClientsThreshold	99999	Maximum number of WirelessClients supported by this WirelessAccessPoint. Valid range is form 0 to 99999.

System VLAN Tag Groups

Threshold groups for VLAN tagging are used to ensure that systems are assigned to their appropriate VLAN. These groups are described in *"Using a policy setting to ensure appropriate VLAN assignments" on page 194*.

Default system VLAN tag groups for the IP Manager shows the default system VLAN tag groups, their target classes and matching criteria, and their default settings. The target class for all system VLAN tag groups is UnitaryComputerSystem.

Table 15-24. Default system VLAN tag groups for the IP Manager

System VLAN tag group	Target class and matching criteria	Default settings
Switches	UnitaryComputerSystem with attributes: ■ IsManaged = TRUE ■ Type = SWITCH	VLAN Tagging Policy
Other Systems	UnitaryComputerSystem with attribute: ■ IsManaged = TRUE	No default settings

Two things to note about Default system VLAN tag groups for the IP Manager:

- Even though the following settings are available to a system VLAN tag group, only the “VLAN Tagging Policy” setting is valid:
  - Cisco Fast and NvRam Memory
  - Connectivity
  - Environment
  - FileSystem
  - Interface Management Policy
  - Juniper Environment
  - Processor and Memory
  - VLAN Tagging Policy
- The “Other Systems” group has the lowest priority. Managed systems that do not match the criteria for the Switches system VLAN tag group become members of the Other Systems group. For example, managed host systems become members of the Other Systems group.

Thresholds for Temperature and Voltage sensors

Voltage and Temperature thresholds are set to generate alarms when the actual values in the devices cross the defined threshold values.

Events and thresholds for Temperature and Voltage sensors

Events and thresholds for Temperature and Voltage sensors gives the default threshold setting and events generated for temperature and voltage sensors.

Table 15-25. Events and thresholds for Temperature and Voltage sensors

Event	Utilization threshold	Description of threshold	Default value	Condition
OutOfRange	RelativeTemperature	How close the current temperature value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value.	10% Range: 0 to 100%	If the shutdown temperature is 50 degrees C and the RelativeTemperatureThreshold is 10%, the OutOfRange event is notified if the temperature exceeds 45 degrees C.
OutOfRange	TemperatureHigh Threshold	High threshold value of the temperature sensor, in degrees C.	50 degrees C Range: 0 to 100 degrees C	This event is generated when the temperature exceeds the configured threshold value.
OutOfRange	RelativeVoltage Threshold	How close the current voltage value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown temperature is 50 degrees C, and the RelativeTemperatureThreshold is 10%, the OutOfRange event is notified if the temperature exceeds 45 degrees C.	0 % Range: 0 to 5%	If the shutdown value is +30V, and the RelativeVoltageThreshold is 10%, the OutOfRange event is notified if the voltage exceeds +27V.
OutOfRange	VoltageSensorHigh Threshold	High threshold value of the voltage sensor test point, in volts.	5 volts 0 to 100 volts	This event is generated when the voltage exceeds the configured threshold value.
OutOfRange	VoltageSensorLow Threshold	Low threshold value of the voltage sensor test point, in volts.	1 volt 0 to 100 volts	This event is generated when the voltage exceeds the configured threshold value.
StateNotNormal	N/A	N/A	N/A	Indicates that the temperature or voltage sensor test point for this system is in the CRITICAL or WARNING state. The sensor state can be in one of four states: NORMAL, WARNING, CRITICAL, or SHUTDOWN.

Attributes for Temperature sensor threshold

Temperature sensor threshold attributes lists the Temperature sensor threshold attributes.

Table 15-26. Temperature sensor threshold attributes

Attribute	Description
MajorAlarmThreshold	The attribute MajorAlarmThreshold is a value directly polled from the MIB. Temperature sensors are created based on entPhysicalIndex from the entPhysicalClass OID (1.3.6.1.2.1.47.1.1.1.1.5) having value of sensor(8). For each entPhysicalIndex, the entSensorThresholdIndex having a value of minor(10) from the entSensorThresholdSeverity OID (1.3.6.1.4.1.9.9.91.1.2.1.1.2) is selected. This is used to obtain the corresponding threshold value from the entSensorThresholdValue OID (1.3.6.1.4.1.9.9.91.1.2.1.1.4). Threshold value OIDs are part of the CISCO-ENTITY-SENSOR-MIB.
MibEntSensorThreshold	The attribute MibEntSensorThreshold is a value after computing Precision from entSensorPrecision. The precision is obtained from Entity MIB's entSensorPrecision attribute OID (1.3.6.1.4.1.9.9.91.1.1.1.1.3). The entSensorPrecision indicates the number of decimal places of precision in fixed-point sensor values. ■ If the entSensorPrecision is 1, the entSensorValue is divided by 10. ■ If the entSensorPrecision is 2, the entSensorValue is divided by 100. ■ If the entSensorPrecision is 3, the entSensorValue is divided by 1000. ■ If the entSensorPrecision is zero, the MibEntSensorThreshold will be zero.
CurrentValue	The attribute CurrentValue is a polled value from the MIB attribute entSensorValue after considering the entSensorPrecision attribute value. The entSensorPrecision indicates the number of decimal places of precision in fixed-point sensor values. The entSensorPrecision indicates the number of decimal places of precision in fixed-point sensor values. ■ If the entSensorPrecision is 1, the entSensorValue is divided by 10. ■ If the entSensorPrecision is 2, the entSensorValue is divided by 100. ■ If the entSensorPrecision is 3, the entSensorValue is divided by 1000. ■ If the entSensorPrecision is zero, the entSensorValue is considered as such for CurrentValue.
RelativeTemperatureThreshold	The attribute RelativeTemperatureThreshold is from the user specified Threshold Group. It indicates how close the current temperature value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown temperature is 50 degrees C and the RelativeTemperatureThreshold is 10%, the OutOfRange event is notified if the temperature exceeds 45 degrees C.
TemperatureHighThreshold	The attribute TemperatureHighThreshold value is populated from the Threshold Group. Though the TemperatureHighThreshold value is populated, it is considered only for the computation of HighThreshold when the MibEntSensorThreshold value is negative.
HighThreshold	The value for the attribute HighThreshold is computed from the MibEntSensorThreshold attribute's value if it is greater than zero. If the value of MibEntSensorThreshold is negative, then the value is computed from attribute TemperatureHighThreshold's value.

VLAN Impact Propagation Groups

Threshold groups for VLAN impact propagation are used to prevent device impact propagation in certain (user-specified) VLANs, such as management VLANs and default VLANs. These groups are described in *"Using a policy setting to prevent VLAN impacts" on page 197*.

The default VLAN impact propagation groups do not automatically appear. As explained in *"Creating VLAN impact propagation group objects" on page 200*, Auser must issue a certain command for the default VLAN impact propagation groups to appear.

Default VLAN impact propagation groups for the IP Manager shows the default VLAN impact propagation groups, their target classes and matching criteria, and their default settings. The target class for all VLAN impact propagation groups is VLAN.

Table 15-27. Default VLAN impact propagation groups for the IP Manager

VLAN impact propagation group	Target class and matching criteria	Default settings
VLANs	VLAN with attributes: ■ IsManaged = TRUE ■ CreationClassName = VLAN ■ VLANKey = *<user-defined value>*	Problem impact propagation policy over VLANs
Other VLANs	VLAN with attribute: ■ IsManaged = TRUE	No default settings

Two things to note about Default VLAN impact propagation groups for the IP Manager:

- The only setting that is available to a VLAN impact propagation group is "Problem Impact propagation policy over VLANs."
- The Other VLANs group has the lowest priority. VLANs that do not match the criteria for the VLANs group become members of the Other VLANs group.

Threshold settings

Threshold settings for the IP Manager lists the IP Manager Threshold settings.

Table 15-28. Threshold settings for the IP Manager

Threshold group category	Threshold setting	Type
Interface Groups	Backup Interface Support	Availability monitoring
	Dial-on-Demand Interface Support	
	Disable Fault Analysis for Interface/Port	Control
	Disable Performance Analysis for Interface/Port	
	Ethernet Interface/Port Performance	Performance monitoring
	Generic Interface/Port Performance	
	Interface/Port Flapping	Availability monitoring
Port Groups - Access Ports Port Groups - Trunk Ports	Disable Fault Analysis for Interface/Port	Control
	Disable Performance Analysis for Interface/Port	
	Ethernet Interface/Port Performance	Performance monitoring
	Generic Interface/Port Performance	
	Interface/Port Flapping	Availability monitoring

Table 15-28. Threshold settings for the IP Manager (Continued)

Threshold group category	Threshold setting	Type
System Resource Groups System VLAN Tag Groups	Cisco Fast and NvRam Memory	Performance monitoring
	Connectivity	Availability monitoring
	Environment	Performance monitoring
	FileSystem	
	Interface Management Policy	Policy management
	Juniper Environment	Performance monitoring
	Processor and Memory	
	VLAN Tagging Policy	Policy management
VLAN Impact Propagation Groups	Problem Impact propagation policy over VLANs	Policy management

In general, a group category, such as “Interface Groups,” has a set of settings that are available to any group in the group category. Thus, all settings for a particular group category are available to each of the default groups in that category.

But even though you can apply any available setting for a particular group category to any default group in that category, not all group-to-setting mappings are valid. The default group-to-setting mappings in Threshold settings through Threshold settings are the mappings that users would typically use.

Control-type threshold settings are described in “Threshold settings for control” on page 219.

Availability-type threshold settings are described in Threshold settings for IP Availability monitoring.

Performance-type threshold settings are described in Threshold settings for IP performance monitoring.

Policy management settings are described in the following sections:

- *“Using a policy setting to control the managed state of interfaces” on page 191*
- *“Using a policy setting to ensure appropriate VLAN assignments” on page 194*
- *Using a policy setting to prevent VLAN impacts on page 197*

Threshold settings for IP Availability monitoring

Through the threshold settings for IP availability monitoring, you control the ICMP and SNMP connectivity polling thresholds of the managed network objects in your network. The polled information serves as input to IP Availability Manager‘s availability analysis of switches, routers, hubs, bridges, and other systems.

The IP Manager provides the following threshold settings for IP availability monitoring:

- Backup Interface Support
- Connectivity
- Dial-on-Demand Interface Support
- Interface/Port Flapping

Backup Interface Support threshold setting

The Backup Interface Support threshold setting configures analysis for interfaces that are used as backup. When an interface is identified as a backup, the connectivity failure diagnosis is modified for it as follows:

- The BackupActivated notification is generated if the interface comes up.
- The ExceededMaximumUptime notification is generated if the interface stays up for a time that equals or exceeds the MaximumUptime value.

Note In case of a backup interface, a Down notification is not generated if that interface is down.

Default values for the Backup Interface Support threshold setting lists the Backup Interface Support threshold setting parameters.

Table 15-29. Default values for the Backup Interface Support threshold setting

Parameter	Default value	Description
MaximumUptime	0 to 86400 seconds Default: 0	Maximum length of time, in seconds, that the interface may be up before the ExceededMaximumUptime notification is generated. If the value of this parameter is 0, the ExceededMaximumUptime event is disabled.

Connectivity threshold setting

The Connectivity threshold setting configures connectivity threshold parameters for interfaces and ports. It also controls:

- The use of bridging connectivity for root-cause analysis.
- The analysis of systems that repeatedly restart, and are thus considered unstable.

  The VMware Smart Assurance IP Availability Manager User Guide provides information about how the IP Availability Manager concludes that a system is unstable.
- Whether SystemRestarted traps are sent to the VMware Smart Assurance Service Assurance Manager Adapter Platform (Adapter Platform).

  “Enabling the SystemRestarted and ConfigChange events” on page 64 provides information about how the IP Availability Manager concludes that a system is restarted.

  Default values for the Connectivity threshold setting lists the Connectivity threshold setting parameters.

Table 15-30. Default values for the Connectivity threshold setting

Parameter	Default value	Description
CorrelationUseBridgingMode	ENABLED,DISABLED Default: DISABLED	Enables or disables the use of bridging connectivity for root-cause analysis. Bridging connectivity is not as precise as physical connectivity, and this parameter controls the extent to which the analysis relies on bridging connectivity. The parameter is set to ENABLED by default because, under normal conditions, most physical connectivity is discovered and there is sparse bridging connectivity. However, you can set the parameter to DISABLED in cases where there is sparse physical connectivity and heavily meshed bridging connectivity.
EnableGenericOIEvent	ENABLED,DISABLED Default: DISABLED	Enables or disables the sending of a SystemRestarted trap for a system to the Adapter Platform whenever the uptime of the system equals or exceeds the MaxUpTimeThreshold parameter value. ENABLED activates the sending of a SystemRestarted trap to the Adapter Platform. DISABLED suppresses the sending of a SystemRestarted trap to the Adapter Platform.
MaxUpTimeThreshold	1 to 1436 minutes Default: 60 minutes	Threshold uptime, in minutes, at or above which a system is considered to be restarted. That is, if the uptime of the system equals or exceeds the time that is specified for this parameter, the system is considered to be restarted.
NumberOfBridgedViaThreshold	Default: 20	Determines whether a BridgedVia relationship is used in correlation. If a MAC endpoint is BridgedVia less than the number of ports that are specified by this threshold, the BridgedVia relationship is used for correlation.
NumberOfBridgesThreshold	Default: 20	Determines whether a Bridges relationship is used in correlation. If a port bridges less than the number of MAC endpoints that are specified by this threshold, the Bridges relationship is used for correlation.
RestartTrapThreshold	0 to 10 Default: 3	Number of SNMP cold or warm start traps that must be received within the amount of time set by the RestartTrapWindow parameter in order for the system to be considered unstable. A value of 0 turns off restart analysis.

Table 15-30. Default values for the Connectivity threshold setting (Continued)

Parameter	Default value	Description
RestartTrapWindow	30 to 3600 seconds Default: 900 seconds (15 minutes)	Window of time that is used to monitor a system's repeated restarts. If the number of start traps equals or exceeds the RestartTrapThreshold during this window of time, the system is considered to be unstable.
TestingNotificationMode	ENABLED,DISABLED Default: ENABLED	Enables or disables the generation of the Down notification for an interface or port. ENABLED activates the diagnosis of an interface or port that is in testing status. DISABLED suppresses the diagnosis of an interface or port that is in testing status.

Dial-On-Demand Interface Support threshold setting

The Dial-on-Demand Interface Support threshold setting configures the analysis for interfaces that are used as dial-on-demand. When an interface is identified as dial-on-demand, the connectivity failure diagnosis is modified for it as follows:

- The Down notification is not generated if the interface is down.
- The ExceededMaximumUptime notification is generated if the interface stays up for a time that equals or exceeds the MaximumUptime value.

  Default values for the Dial-On-Demand Interface Support threshold setting lists the Dial-On-Demand Interface Support threshold setting parameters.

Table 15-31. Default values for the Dial-On-Demand Interface Support threshold setting

Parameter	Default value	Description
MaximumUptime	0 to 86400 seconds Default: 7200 seconds (2 hours)	Maximum length of time that the interface may be up before the ExceededMaximumUptime notification is generated. If the value of this parameter is 0, the ExceededMaximumUptime event is disabled.

Interface/Port Flapping threshold setting

The Interface/Port Flapping threshold setting controls the analysis of interfaces and ports that are continually going up and down. Unstable analysis monitors SNMP link down traps to identify a flapping interface or port and then generates a notification to report that the interface or port is unstable.

The VMware Smart Assurance IP Availability Manager User Guide provides information about how the IP Availability Manager concludes that an interface or port is unstable. An interface or port is also known as a network adapter.

Default values for the Interface/Port Flapping threshold setting lists the Interface/Port Flapping threshold setting parameters.

Table 15-32. Default values for the Interface/Port Flapping threshold setting

Parameter	Default value	Description
LinkTrapThreshold	0 to 10 Default: 3	Number of SNMP link down traps that must be received within the LinkTrapWindow for the IP Availability Manager to consider the interface or port flapping. A value of 0 turns off flapping analysis.
LinkTrapWindow	30 to 3600 seconds Default: 300 seconds (5 minutes)	Window of time that is used to monitor flapping analysis of an interface or port. If the number of link down traps equals or exceeds the LinkTrapThreshold during this window of time, the interface or port is considered to be flapping.

Threshold settings for IP performance monitoring

Through the threshold settings for IP performance monitoring, you control the ICMP and SNMP performance polling thresholds of the managed network objects in your network. The polled information serves as input to IP Performance Manager‘s fault and performance analysis of interfaces and ports, processors and memory, disks and filesystems, fans and power supplies, and voltage and temperature sensors.

The IP Manager provides the following threshold settings for IP performance monitoring:

- Ethernet Interface/Port Performance
- Generic Interface/Port Performance
- Cisco Fast and NvRam Memory
- Environment
- FileSystem
- Juniper Environment
- Processor and Memory

Ethernet Interface/Port Performance threshold setting

The Ethernet Interface/Port Performance threshold setting configures the monitoring of an Ethernet network adapter’s performance characteristics. Parameters in this setting control the notification of these faults:

- High Broadcast Rate
- High Collision Rate
- High Discard Rate
- High Queue Drop Rate
- High Error Rate

- High Utilization

  One other parameter in this setting determines whether the IP Performance Manager analyzes subinterfaces, which are interfaces LayeredOver physical interfaces. For example, a physical interface in a Frame Relay or ATM network is configured with multiple virtual circuits, and each virtual circuit is associated with a subinterface.

  Note A subinterface, similar to an interface, is an instance of the Interface class.

  Default values for the Ethernet Interface/Port Performance threshold setting lists the Ethernet Interface/Port Performance threshold setting parameters.

Table 15-33. Default values for the Ethernet Interface/Port Performance threshold setting

Parameter	Default Value	Description
AnalysisModeOfSubInterface-Performance	ENABLED,DISABLED Default: DISABLED	When enabled, the IP Performance Manager analyzes the performance of all subinterfaces of all objects in the threshold group.
BroadcastThreshold	0 to 100% Default: 15%	Upper threshold for broadcast traffic, expressed as a percentage of the total bandwidth.
CollisionThreshold	0 to 100% Default: 10%	Upper threshold for collisions, expressed as a percentage of the total number of output packets.
DiscardThreshold	0 to 100% Default: 5%	Upper threshold for dropped packets, expressed as a percentage of the total number of packets.
ErrorThreshold	0 to 100% Default: 10%	Upper threshold for packet errors, expressed as a percentage of the total number of packets.
MinimumTrafficThreshold	0 to 100% Default: 2%	Minimum packet rate for a network adapter, expressed as a percentage of total bandwidth. Value can be any number between 0.1 and 100.0. For example, 0.2 is a valid value.
QueueDropThreshold	0 to 100% Default: 1%	Acceptable percentage of packets that are dropped because of full queues, expressed as a percentage of the total number of packets.
UtilizationThreshold	0 to 100% Default: 40%	Upper threshold for link utilization, expressed as a percentage of the total bandwidth.

Generic Interface/Port Performance threshold setting

The Generic Interface/Port Performance threshold setting configures the monitoring of a non-Ethernet network adapter's performance characteristics. It includes basic parameters that are common to all media types, such as utilization, errors, broadcast, and packet drops. (These basic parameters are also included in the Ethernet Interface/Port Performance setting, although their default values may be different.) Parameters in this setting control the notification of these faults:

- High Broadcast Rate
- High Discard Rate
- High Error Rate

- High Queue Drop Rate
- High Utilization

  Similar to the Ethernet Interface/Port Performance threshold setting, one other parameter in this setting determines whether the IP Performance Manager analyzes subinterfaces, which are interfaces LayeredOver physical interfaces.

  Default values for the Generic Interface/Port Performance threshold setting lists the Generic Interface/Port Performance threshold setting parameters.

Table 15-34. Default values for the Generic Interface/Port Performance threshold setting

Parameter	Default value	Description
AnalysisModeOfSubInterface-Performance	ENABLED,DISABLED Default: ENABLED	When enabled, the IP Performance Manager analyzes the performance of all subinterfaces of all objects in the threshold group.
BroadcastThreshold	0 to 100% Default: 15%	Upper threshold for broadcast traffic, expressed as a percentage of the total bandwidth.
DiscardThreshold	0 to 100% Default: 5%	Upper threshold for dropped packets, expressed as a percentage of the total number of packets.
ErrorThreshold	0 to 100% Default: 10%	Upper threshold for packet errors, expressed as a percentage of the total number of packets.
MinimumTrafficThreshold	0 to 100% Default: 2%	Minimum packet rate for a network adapter, expressed as a percentage of total bandwidth. Value can be any number between 0.1 and 100.0. For example, 0.2 is a valid value.
QueueDropThreshold	0 to 100% Default: 1%	Acceptable percentage of packets that are dropped because of full queues, expressed as a percentage of the total number of packets.
UtilizationThreshold	0 to 100% Default: 60%	Upper threshold for link utilization, expressed as a percentage of the total bandwidth.

Cisco Fast and NvRam Memory threshold setting

The Cisco Fast and NvRam Memory threshold setting enables users to set the free memory thresholds for two different memory types:

- Fast memory
- Non-volatile memory (NVRAM)

  The setting overrides the FreeMemoryThreshold parameter in the Processor and Memory setting, which is described in Processor and Memory threshold setting. The Cisco Fast and NvRam Memory setting is intended for Cisco devices only.

  The Cisco Fast and NvRam Memory setting is not the default setting for any threshold group, but is available to any of the system resource groups:

- ComputeFabric

- Switches
- Routers
- Hubs and Bridges
- MediaGateways
- Other System

The system resource groups are described in Cisco Fast and NvRam Memory threshold setting.

To add the Cisco Fast and NvRam Memory setting to a system resource group, consult “Adding or removing settings” on page 144 to add the setting to the Current Settings list. Also, consult “Editing matching criteria” on page 146 to add the “Vendor=CISCO” matching criteria to the group, to limit the group’s membership to just Cisco devices.

Default values for the Cisco Fast and NvRam Memory threshold setting lists the Cisco Fast and NvRam Memory threshold setting parameters.

Table 15-35. Default values for the Cisco Fast and NvRam Memory threshold setting

Parameter	Default value	Description
FastMemoryThreshold	0 to 100% Default: 15%	Lower threshold for the acceptable amount of free Fast memory as measured by the ratio of free Fast memory to the total Fast memory.
NvramMemoryThreshold	0 to 100% Default: 15%	Lower threshold for the acceptable amount of free NVRAM memory as measured by the ratio of free NVRAM memory to the total NVRAM memory.

Environment threshold setting

The Environment threshold setting configures the monitoring of a system’s environmental conditions. System components such as the fan, memory, power supply, temperature sensor, and voltage sensor objects are monitored.

Default values for the Environment threshold setting lists the Environment threshold setting parameters.

Table 15-36. Default values for the Environment threshold setting

Parameter	Value	Description
RelativeTemperature-Threshold	0 to 100% Default: 10%	How close the current temperature value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown temperature is 50 degrees C and the RelativeTemperatureThreshold is 10%, the OutOfRange event is notified if the temperature exceeds 45 degrees C.
RelativeVoltage-Threshold	0 to 5% Default: 0%	How close the current voltage value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown value is +30V, and the RelativeVoltageThreshold is 10%, the OutOfRange event is notified if the voltage exceeds +27V.

Table 15-36. Default values for the Environment threshold setting (Continued)

Parameter	Value	Description
TemperatureHigh-Threshold	0 to 100 degrees C Default: 50 degrees C	High threshold value of the temperature sensor, in degrees C.
UseMIBThresholds	True, False Default: True	This variable allows for using thresholds defined in the SNMP agent instead of manually set ones. When the threshold value is available in the MIB for sensors, then this attribute value decides if that should be used. If the value is set to True and the MIB thresholds are not available for the sensor, then the threshold values defined in the Environment threshold settings are used.
VoltageSensorHigh-Threshold	0 to 100 volts Default: 5 volts	High threshold value of the voltage sensor test point, in volts.
VoltageSensorLow-Threshold	0 to 100 volts Default: 1 volt	Low threshold value of the voltage sensor test point, in volts.

Juniper Environment threshold setting

The Juniper Environment threshold setting configures the monitoring of a Juniper system's environmental conditions. Juniper system components such as the fan, memory, power supply, temperature sensor, and voltage sensor objects are monitored.

Relative to the Environment threshold setting, this setting provides an additional parameter for monitoring the environmental conditions of a Juniper system for temperature sensor objects.

Default values for the Juniper Environment threshold setting lists the Juniper Environment threshold setting parameters.

Table 15-37. Default values for the Juniper Environment threshold setting

Parameter	Default Value	Description
HighTemperature-Threshold	0 to 100 degrees C Default: 40 degrees C	High temperature threshold in degrees C. This value, in conjunction with the RelativeTemperatureThreshold value determines the temperature that triggers an emergency shutdown. For example, if the HighTemperatureThreshold is 50 degrees C and the RelativeTemperatureThreshold is 10%, the OutOfRange event is notified if the temperature exceeds 45 degrees C.
RelativeTemperature-Threshold	0 to 100% Default: 10%	How close the current temperature value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown temperature is 50 degrees C and the RelativeTemperatureThreshold is 10%, the OutOfRange event is notified if the temperature exceeds 45 degrees C.

Table 15-37. Default values for the Juniper Environment threshold setting (Continued)

Parameter	Default Value	Description
RelativeVoltage-Threshold	0 to 5% Default: 0%	How close the current voltage value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown value is +30V, and the RelativeVoltageThreshold is 2%, the OutOfRange event is notified if the voltage exceeds +29.4V.
TemperatureHigh-Threshold	0 to 100 degrees C Default: 50 degrees C	High threshold value of the temperature sensor, in degrees C.
VoltageSensorHigh-Threshold	0 to 100 volts Default: 5 volts	High threshold value of the voltage sensor test point, in volts.
VoltageSensorLow-Threshold	0 to 100 volts Default: 1 volt	Low threshold value of the voltage sensor test point, in volts.

FileSystem threshold setting

The FileSystem threshold setting configures the performance monitoring of a host system's filesystem. Although available to all threshold groups in System Resource Groups and System VLAN Tag Groups, this setting is contained only in the Other Systems threshold group in System Resource Groups.

Default value for the FileSystem threshold setting lists the FileSystem threshold setting parameters. The MaxUtilizationPct parameter controls the notification of the HighUtilization fault.

Table 15-38. Default value for the FileSystem threshold setting

Parameter	Default value	Description
MaxUtilizationPct	0 to 100% Default: 95%	Upper threshold for a filesystem's utilization, expressed as a percentage of the total size that is currently in use.
MinAvailableSpace	Default: 1024 KB	Threshold for a filesystem's minimum available space, expressed as total free space in kilobytes (KB).

Processor and Memory threshold setting

The Processor and Memory threshold setting configures the performance monitoring of a system's processor and its associated memory objects. Parameters in this setting control the notification of these faults:

- High Utilization
- High Backplane Utilization (Chassis)
- High Buffer Miss Rate
- High Buffer Utilization
- Fragmentation

- Insufficient Free Memory

  Default values for the Processor and Memory threshold setting lists the Processor and Memory threshold setting parameters.

Table 15-39. Default values for the Processor and Memory threshold setting

Parameter	Default value	Description
BackplaneUtilizationThreshold	0 to 100% Default: 80%	Upper threshold for a switch's backplane utilization expressed as a percentage of the total backplane bandwidth.
FreeMemoryThreshold	0 to 100% Default: 15%	Lower threshold for the acceptable amount of free memory as measured by the ratio of free memory to the total memory.
MemoryBufferMissThreshold	0 to 100% Default: 10%	Upper threshold for the number of buffer misses, expressed as a percentage of the total number of buffer requests.
MemoryBufferUtilization-Threshold	0 to 100% Default: 90%	Upper threshold for the number of buffers that are used, expressed as a percentage of the total number of buffers.
MemoryFragmentation-Threshold	0 to 100% Default: 5%	Lower threshold for memory fragmentation. The fragmentation value is the ratio of the largest number of contiguous unallocated bytes to the total amount of free memory. For example, a value of 5 indicates that the largest free buffer must be at least 5% of the free memory.
ProcessorUtilizationThreshold	0 to 100% Default: 90%	Upper threshold for processor utilization, expressed as a percentage of the total capacity of the processor.

IPv6 Address Conventions

16

This chapter includes the following topics:

- Overview
- Conventions for specifying an IPv6 address with port number
- Conventions for specifying an IPv6 address in a class instance name

Overview

Internet Protocol version 6 (IPv6) uses colons (:) in its addresses instead of periods (.), which are used in Internet Protocol version 4 (IPv4) addresses. Because colons are also used as delimiters in VMware Smart Assurance command lines, configuration files, seed files, Add Agent commands, and class instance names, special syntax must be observed when representing a host as an IPv6 address.

The special syntax, which is identified in this appendix, does not apply to hosts that are represented as hostnames, or as hostnames that include an explicit IP version suffix (:v6v4, :v4v6, :v6, or :v4).

Hostnames in command lines or configuration files

The following <*hostname*>:<*port number*> entries in a command line or a configuration file do not require any special syntax:

- frame.vmware.com:426
- frame.vmware.com:v6v4:426
- frame.vmware.com:v4v6:426
- frame.vmware.com:v6:426
- frame.vmware.com:v4:426

  The hostname, frame.vmware.com, in these entries will be resolved to an IP address as stated in *"Controlling the IP version for name resolution" on page 57*. For the first entry, the hostname will be resolved in accordance to the SM_IP_VERSIONS environment variable setting, which is described in SM_IP_VERSIONS environment variable.

Hostnames in seed files or Add Agent commands

The following <*hostname*>:<*port number*> entries in a seed file or an Add Agent command do not require any special syntax:

- Core-ROUTER-1:200
- Core-ROUTER-1:v6v4:200
- Core-ROUTER-1:v4v6:200
- Core-ROUTER-1:v6:200
- Core-ROUTER-1:v4:200

  The hostname, Core-ROUTER-1, in these entries will be resolved to an IP address as stated in *"Controlling the IP version for name resolution" on page 57*. For the first entry, the hostname will be resolved in accordance to the SM_IP_VERSIONS environment variable setting, which is described in SM_IP_VERSIONS environment variable.

Hostnames in class instance names

A hostname in a class instance name does not require any special syntax. For example, "R1" in Router::R1 does not require any special syntax. A hostname in a class instance name does not include an explicit IP version suffix.

Conventions for specifying an IPv6 address with port number

Sometimes when you use an VMware Smart Assurance command line utility, such as dmctl, sm_tpmgr, or sm_snmpwalk, you want to specify a Broker other than the default Broker, which is identified in the BASEDIR/smarts/local/conf/runcmd_env.sh file of the installation directory from which the command line utility is invoked; for example, localhost:426. To do so, you include the -b <*Broker*> option in the command line invocation.

The <*Broker*> syntax is hostname or IP address, followed by a colon (:) delimiter, followed by a port number. The combination of an IP (v4 or v6) address and port number is also called a socket.

For an IPv6 address and port number to be interpreted correctly in a command line, enclose the IPv6 address within a pair of double quotation marks and square brackets. The syntax is:

```
"[<ipv6_address>]:<port>"
```

An example is:

```
"[2001:0db8::0010]:65000"
```

If you want to use the default port, omit the port number and specify only the IPv6 address; no additional convention notations are needed. For example:

```
2001:0db8::0010
```

In addition, for a seed-file entry or an Add Agent command, you can specify the port number of the SNMP agent that is running on the candidate system by typing a colon (:) and the port number after the hostname or IP (v4 or v6) address; for example:

CoreROUTER-1:200

For an IPv6 address and port number to be interpreted correctly in a seed-file entry or an Add Agent command, enclose the IPv6 address within a pair of square brackets. The syntax is:

```
[<ipv6_address>]:<port>
```

An example is:

```
[2001:0db8::0010]:200
```

And finally, for an IPv6 address and port number to be interpreted correctly in a configuration file, observe the same syntax as used in a seed-file entry or an Add Agent command.

Conventions for specifying an IPv6 address in a class instance name

For the **dmctl** utility, if your class instance name contains either square brackets or double colons, you need to specify one of the following conventions:

- In dmctl command line mode, if the instance uses square brackets or double colons in its name, enclose the instance with single and double quotation marks. Here are two examples:

  ```
  MyClass::"'[2001:db8:0:0:0:0:0102:0304]'"
  MyClass::"'::instance'"
  ```

- In dmctl interactive mode, if the instance uses square brackets or double colons in its name, enclose the instance with either single or double quotation marks. Here are four examples:

  ```
  MyClass::'[2001:db8:0:0:0:0:0102:0304]'
  MyClass::"[2001:db8:0:0:0:0:0102:0304]"
  MyClass::'::instance'
  MyClass::"::instance"
  ```

SM_IP_VERSIONS environment variable

Valid values for the SM_IP_VERSIONS environment variable are:

- v6v4 (default)

  Hostname is resolved to an IPv6 address. If that resolution fails, the local name resolution service tries to resolve the hostname to an IPv4 address.

- v4v6

  Hostname is resolved to an IPv4 address. If that resolution fails, the local name resolution service tries to resolve the hostname to an IPv6 address.

- v6

  Hostname is resolved to an IPv6 address.

- v4

  Hostname is resolved to an IPv4 address.

  Values v6v4, v4v6, v6, and v4 are not case-sensitive.

Wildcard Patterns

17

Types of wildcard patterns

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

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

A compound wildcard pattern consists of one or more basic wildcard patterns separated by ampersand (&) or tilde (~) characters. A compound wildcard pattern is matched by attempting to match each of its component basic wildcard patterns against the entire input string. For compound wildcard patterns, see Compound wildcard patterns.

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

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

Table 17-1. Basic wildcard patterns

Character	Description
?	Matches any single character. For example, server?.example.com matches server3.example.com and serverB.example.com, but not server10.example.com.
*	Matches an arbitrary string of characters. The string can be empty. For example, server*.example.com matches server-ny.example.com and server.example.com (an empty match).

Table 17-1. Basic wildcard patterns (Continued)

Character	Description
[set]	Matches any single character that appears within [set]; or, if the first character of [set] is (^), any single character that is *not* in the set. A hyphen (-) within [set] indicates a range, so that [a-d] is equivalent to [abcd]. The character before the hyphen (-) must precede the character after it or the range will be empty. The character (^) in any position except the first, or a hyphen (-) at the first or last position, has no special meaning. For example, server[789-].example.com matches server7.example.com through server9.example.com, but not server6.example.com. It also matches server-.example.com. For example, server[^12].example.com does not match server1.example.com or server2.example.com, but will match server8.example.com.
<n1-n2>	Matches numbers in a given range. Both *n1* and *n2* must be strings of digits, which represent non-negative integer values. The matching characters are a non-empty string of digits whose value, as a non-negative integer, is greater than or equal to *n1* and less than or equal to *n2*. If either end of the range is omitted, no limitation is placed on the accepted number. For example, 98.49.<1-100>.10 matches a range of IP addresses from 98.49.1.10 through 98.49.100.10. Example of an omitted high end of the range: <50-> matches any string of digits with a value greater than or equal to 50. Example of an omitted low end of the range: <-150> matches any value between zero and 150. For a more subtle example: The pattern <1-10>* matches 1, 2, up through 10, with * matching no characters. Similarly, it matches strings like 9x, with * matching the trailing x. However, it does not match 11, because <1-10> always extracts the longest possible string of digits (11) and then matches only if the number it represents is in range.
|	Matches alternatives. For example,”ab|bc|cd” without spaces matches exactly the three following strings: “ab”, “bc”, and “cd”. A | as the first or last character of a pattern accepts an empty string as a match. Example with spaces “ab | bc” matches the strings “ab” and “ bc”.
\	Removes the special status, if any, of the following character. Backslash (\) has no special meaning within a set ([set]) or range (<n1-n2>) construct.

Special characters for compound wildcard patterns are summarized in Compound wildcard patterns.

Table 17-2. Compound wildcard patterns

Character	Description
&	“And Also” for a compound wildcard pattern. If a component basic wildcard pattern is preceded by & (or is the first basic wildcard pattern in the compound wildcard pattern), it *must* successfully match. Example: *NY*&*Router* matches all strings which contain NY and also contain Router. Example: <1-100>&*[02468] matches even numbers between 1 and 100 inclusive. The <1-100> component only passes numbers in the correct range and the *[02468] component only passes numbers that end in an even digit. Example: *A*|*B*&*C* matches strings that contain either an A or a B, and also contain a C.
~	“Except” for a compound wildcard pattern (opposite function of &).If a component basic wildcard pattern is preceded by ~, it *must not* match. Example: 10.20.30.*~10.20.30.50 matches all devices on network 10.20.30 except 10.20.30.50. Example: *Router*~*Cisco*&*10.20.30.*~10.20.30.<10-20>* matches a Router, except a Cisco router, with an address on network 10.20.30, except not 10.20.30.10 through 10.20.30.20.

Audit Logging

18

Enhanced Domain Audit Logging Format

The audit log contains one line per entry. The entry consists of multiple tab-delimited fields. The first nine fields have fixed meaning and order, with additional fields in a tag=value format. The tagged fields that are present depend on the action that is logged. Different actions will have different additional data available. For example, for an invoke, the tag oper would indicate the operation being invoked.

The order of the tab-delimited fields in an entry is:

date login ID ClientDescription pid IP user@host action [tag1=value [tag2=value […]]]

Example:

2010/03/25 12:52:21 +442ms admin 2 dmctl 23168 127.0.0.1 root@host01.example.com createInstance object=MyClass::MyInstance

Note The text in the example appears on one line in the log, though it has been wrapped in this document.

Table 18-1. Description of fields in the audit log

Field	Description
Date	The date and time at which the event occurred, formatted according to the setting of SM_DATETIME_FORMAT.
Login	The login identifier used to authenticate to the domain.
ID	The client identification number for the particular session.
Client Description	Information of the client, for example, dmctl, console. This information is reported by the client as it cannot be verfied independently. A malicious user could manipulate this information.
PID	The process ID of the client on the system where the connection originated. This information is reported by the client as it cannot be verified independently. A malicious user could manipulate this information.
IP	The network address of the system from which the connection originated. This is obtained from the network stack. Due to the presence of NAT or other factors, it may not reflect the actual IP address of the client system.
User	The operating system login name of the user on the system where the connection originated. This information is reported by the client as it cannot be verified independently. A malicious user could manipulate this information.

Table 18-1. Description of fields in the audit log (Continued)

Field	Description
Host	The hostname of the system where the connection originated. This hostname is reported by the client. A malicious user could manipulate this information. incase of an uncertainty, perform a reverse lookup on the IP provided. This field is provided as it may allow identification of individual clients behind a NAT, while a reverse lookup of the IP would resolve to a single router.
Action	An API operation called by the client. For example, put, create, delete, invoke.

Description of fields in the audit log lists the fields and its description.

Actions

Many actions are read-only and thus would not appear in the audit log. Such actions are not listed in the table.

Table 18-2. Description of actions in the audit log

Action	Description
consistencyUpdate	Requests that the codebook be recomputed.
correlate	Causes the domain manager to begin a correlation.
create	Create a new object instance in the domain. Tagged values include object, the class name, and instance name of the object to create.
delete	Delete the object with the given name. Tagged values include object, the object to be deleted.
exec	Causes the domain to execute a program object. Tagged values include program.
insert	Add a new value to a table of an object. Tagged values include attribute, which identifies the object and attribute to be affected, and value, the desired new value.
invoke	Invoke a model operation. If an operation can be determined to be read-only, it will not be logged. Tagged values include object, the name of the object to invoke the operation, oper, the name of the operation, and args, the list of argument values.
loadLibrary	Requests the domain manager to load a shared library, such as one containing a compiled model. Tagged values include library.
loadProgram	Requests to load a program object into the domain. Tagged values include program.
put	Set an attribute of an object. Tagged values include attribute, which identifies the object and attribute to be affected, and value, the desired new value.
remove	Remove a value from a table of an object. Tagged values include attribute, which identifies the object and attribute to be affected, and value, the value to be removed.
removeByKey	Remove a value from a table of an object. Tagged values include attribute, which identifies the object and attribute to be affected, and key, the key of the value to be removed.
restore	Restore object instances from a file. Tagged values include filename, the file to restore from.
save	Store the repository to a file. Tagged values include filename, the file the objects will be stored in, and class if the request was to save a subset of instances by class.
shutdown	Requests the domain manager to shut down.
transactionAbort	Abort a previously started repository transaction.

Table 18-2. Description of actions in the audit log (Continued)

Action	Description
transactionCommit	Commit a previously started repository transaction
transactionStart	Start a repository transaction.

Description of actions in the audit log lists the actions and its description.

Tags

Table 18-3. Description of tags in the audit log

Tag	Description
args	A list of values used as argument to an operation.
attribute	The fully qualified name of an attribute of an object, in the format ClassName::InstanceName::AttributeName.
class	The name of a model class.
filename	The name of a file.
value	A value used as a table key.
library	The name of a shared library.
object	The name of an object instance, in the format ClassName::InstanceName.
oper	The name of a model operation.
program	The name of a program object loaded or executed.
value	The value of an attribute.

Description of tags in the audit log lists the tags and its description.

Commands

19

This chapter includes the following sections:

- Issuing commands to modify configuration parameters

Issuing commands to modify configuration parameters

You can issue any of the following commands from the BASEDIR/smarts/bin directory to change configuration parameters for the IP Manager:

- dmctl put
- dmctl invoke
- dmctl get
- sm_tpmgr

  The **dmctl** utility is described in the HTML pages that are located in the BASEDIR/smarts/doc/html/usage directory of any Domain Manager installation area. Chapter 16 IPv6 Address Conventions provides additional syntax information. You can use "?" in dmctl to see a list of all available commands.

dmctl put

In general, you can use the dmctl put command to change the value of any basic-type attribute (string, boolean, integer, float, and so on) of any VMware Smart Assurance object. Upon issuing a dmctl command, you might be prompted for a username and password. Respond with your user account. For example, to specify the default administrative account, enter username *admin* and password *changeme*.

For IP Manager, you use the dmctl put command to override parameter settings in the discovery.conf file or the name-resolver.conf file. These parameters are defined as attributes of the ICF-TopologyManager object, which is an instance of the ICF_TopologyManager class.

The syntax for the dmctl put command is:

```
dmctl -s <IP Manager instance name> put
ICF_TopologyManager::ICF-TopologyManager::<configuration parameter name> <value>
```

For example:

```
dmctl -s INCHARGE-AM put ICF_TopologyManager::ICF-TopologyManager::numberProbeThreads 12
```

dmctl invoke

You use the dmctl invoke command to override parameter settings in the tpmgr-param.conf file. These parameters are entries for a table that is defined inside the ICF-TopologyManager object.

The syntax for the dmctl invoke command is:

```
        dmctl -s <IP Manager instance name> invoke
ICF_TopologyManager::ICF-TopologyManager insertParameter
<configuration parameter name> <value>
```

For example:

```
dmctl -s INCHARGE-AM invoke
ICF_TopologyManager::ICF-TopologyManager insertParameter
        DisableMPLSDiscovery FALSE
```

dmctl get

You can use the dmctl get command to verify the value of the attribute that has been set.

The syntax for the dmctl get command is:

```
        dmctl -s <IP Manager instance name> get
        ICF_TopologyManager::ICF-TopologyManager::<configuration
parameter name>
```

For example:

```
        dmctl -s INCHARGE-AM get ICF_TopologyManager::ICF-TopologyManager:: HSRPEnabled
```

sm_tpmgr

You use the sm_tpmgr command to reload the parameters in the discovery.conf, tpmgr-param.conf, or name-resolver.conf file or any other IP Manager user configuration files.

Note A discovery cycle should not be in progress when you issue this command.

After you use the sm_edit utility to make a parameter change in the discovery.conf, tpmgr-param.conf, or name-resolver.conf file, you can use the sm_tpmgr command to make that change known to the target IP Manager instance without the need to restart the target server. The syntax for the sm_tpmgr command is:

```
        sm_tpmgr -b <host>:<port> -s <IP Manager instance name>
 --load-conf=<configuration file name>
```

For example:

```
        sm_tpmgr -b localhost:426 -s INCHARGE-AM --load-conf=user-defined-connections.conf
```