

# *InCharge*<sup>TM</sup>

## IP Availability Manager User's Guide

Version 6.2



Copyright ©1996-2004 by System Management ARTS Incorporated. All rights reserved.

The Software and all intellectual property rights related thereto constitute trade secrets and proprietary data of SMARTS and any third party from whom SMARTS has received marketing rights, and nothing herein shall be construed to convey any title or ownership rights to you. Your right to copy the software and this documentation is limited by law. Making unauthorized copies, adaptations, or compilation works is prohibited and constitutes a punishable violation of the law. Use of the software is governed by its accompanying license agreement. The documentation is provided "as is" without warranty of any kind. In no event shall System Management ARTS Incorporated ("SMARTS") be liable for any loss of profits, loss of business, loss of use of data, interruption of business, or for indirect, special, incidental, or consequential damages of any kind, arising from any error in this documentation.

The InCharge products mentioned in this document are covered by one or more of the following U.S. patents or pending patent applications: 5,528,516, 5,661,668, 6,249,755, 10,124,881 and 60,284,860.

"InCharge," the InCharge logo, "SMARTS," the SMARTS logo, "Graphical Visualization," "Authentic Problem," "Codebook Correlation Technology," and "Instant Results Technology" are trademarks or registered trademarks of System Management ARTS Incorporated. All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

Third-Party Software. The Software may include software of third parties from whom SMARTS has received marketing rights and is subject to some or all of the following additional terms and conditions:

#### Bundled Software

Sun Microsystems, Inc., Java(TM) Interface Classes, Java API for XML Parsing, Version 1.1. "Java" and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. SMARTS is independent of Sun Microsystems, Inc.

#### W3C IPR Software

Copyright © 2001-2003 World Wide Web Consortium (<http://www.w3.org>), (Massachusetts Institute of Technology (<http://www.lcs.mit.edu>), Institut National de Recherche en Informatique et en Automatique (<http://www.inria.fr>), Keio University (<http://www.keio.ac.jp>)). All rights reserved (<http://www.w3.org/Consortium/Legal/>). Note: The original version of the W3C Software Copyright Notice and License can be found at <http://www.w3.org/Consortium/Legal/copyright-software-19980720>.

#### The Apache Software License, Version 1.1

Copyright ©1999-2003 The Apache Software Foundation. All rights reserved. Redistribution and use of Apache source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of Apache source code must retain the above copyright notice, this list of conditions and the Apache disclaimer as written below.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the Apache disclaimer as written below in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:  
"This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)."  
Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "The Jakarta Project", "Tomcat", "Xalan", "Xerces", and "Apache Software Foundation" must not be used to endorse or promote products derived from Apache software without prior written permission. For written permission, please contact [apache@apache.org](mailto:apache@apache.org).
5. Products derived from this Apache software may not be called "Apache," nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

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

This Apache software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation and was originally based on software copyright © 1999, Lotus Development Corporation., <http://www.lotus.com>. For information on the Apache Software Foundation, please see <http://www.apache.org>.

#### FLEXIm Software

© 1994 - 2003, Macrovision Corporation. All rights reserved. "FLEXIm" is a registered trademark of Macrovision Corporation. For product and legal information, see <http://www.macrovision.com/solutions/esd/flexim/flexim.shtml>.

#### JfreeChart – Java library for GIF generation

The Software is a "work that uses the library" as defined in GNU Lesser General Public License Version 2.1, February 1999 Copyright © 1991, 1999 Free Software Foundation, Inc., and is provided "AS IS" WITHOUT WARRANTY OF ANY KIND EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED IN THE ABOVE-REFERENCED LICENSE BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. JfreeChart library (included herein as .jar files) is provided in accordance with, and its use is covered by the GNU Lesser General Public License Version 2.1, which is set forth at <http://www.object-refinery.com/lgpl.html>.

#### BMC – product library

The Software contains technology (product library or libraries) owned by BMC Software, Inc. ("BMC Technology"). BMC Software, Inc., its affiliates and licensors (including SMARTS) hereby disclaim all representations, warranties and liability for the BMC Technology.

#### Crystal Decisions Products

The Software may contain certain software and related user documentation (e.g., Crystal Enterprise Professional, Crystal Reports Professional and/or Crystal Analysis Professional) that are owned by Crystal Decisions, Inc., 895 Emerson Street, Palo Alto, CA 94301 ("Crystal Decisions"). All such software products are

the technology of Crystal Decisions. The use of all Crystal Decisions software products is subject to a separate license agreement included with the Software electronically, in written materials, or both. YOU MAY NOT USE THE CRYSTAL DECISIONS SOFTWARE UNLESS AND UNTIL YOU READ, ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS OF THE CRYSTAL DECISIONS' SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE CRYSTAL DECISIONS' SOFTWARE LICENSE, YOU MAY RETURN, WITHIN THIRTY (30) DAYS OF PURCHASE, THE MEDIA PACKAGE AND ALL ACCOMPANYING ITEMS (INCLUDING WRITTEN MATERIALS AND BINDERS OR OTHER CONTAINERS) RELATED TO THE CRYSTAL DECISIONS' TECHNOLOGY, TO SMARTS FOR A FULL REFUND, OR YOU MAY WRITE, CRYSTAL WARRANTIES, P.O. BOX 67427, SCOTTS VALLEY, CA 95067, U.S.A.

GNU eTeks PJA Toolkit

Copyright © 2000-2001 Emmanuel PUYBARET/eTeks info@eteks.com. All Rights Reserved.

The eTeks PJA Toolkit is resident on the CD on which the Software was delivered to you. Additional information is available at eTEks' web site:

<http://www.eteks.com>. The eTeks PJA Toolkit program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (GPL) as published by the Free Software Foundation; version 2 of the License. The full text of the applicable GNU GPL is available for viewing at <http://www.gnu.org/copyleft/gpl.txt>. You may also request a copy of the GPL from the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. The eTeks PJA Toolkit program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

For a period of three years from the date of your license for the Software, you are entitled to receive under the terms of Sections 1 and 2 of the GPL, for a charge no more than SMARTS' cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code for the GNU eTeks PJA Toolkit provided to you hereunder by requesting such code from SMARTS in writing: Attn: Customer Support, SMARTS, 44 South Broadway, White Plains, New York 10601.

IBM Runtime for AIX

The Software contains the IBM Runtime Environment for AIX(R), Java™ 2 Technology Edition Runtime Modules © Copyright IBM Corporation 1999, 2000 All Rights Reserved.

HP-UX Runtime Environment for the Java™ 2 Platform

The Software contains the HP-UX Runtime for the Java™ 2 Platform, distributed pursuant to and governed by Hewlett-Packard Co. ("HP") software license terms set forth in detail at: <http://www.hp.com>. Please check the Software to determine the version of Java runtime distributed to you.

DataDirect Technologies

Portions of this software are copyrighted by DataDirect Technologies, 1991-2002.

NetBSD

Copyright © 2001 Christopher G. Demetriou. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed for the NetBSD Project. See <http://www.netbsd.org/> for information about NetBSD.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. <<Id: LICENSE, v 1.2 2000/06/14 15:57:33 cgd Exp>>

RSA Data Security, Inc.

Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved. License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

AES

Copyright © 2003, Dr Brian Gladman <brg@gladman.me.uk>, Worcester, UK. All rights reserved.

License Terms:

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

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

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

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

---



# Contents

<b>Preface</b>	<b>ix</b>
Intended Audience	ix
Prerequisites	ix
Document Organization	x
Documentation Conventions	x
InCharge Installation Directory	xi
Additional Resources	xiii
InCharge Commands	xiii
Documentation	xiii
Common Abbreviations and Acronyms	xiv
Technical Support	xiv
<b>1 Introduction</b>	<b>1</b>
Availability Monitoring	2
Availability Notifications	2
<b>2 Network Elements and Their Failures</b>	<b>3</b>
Summary of Faults, Symptomatic Events, and Exceptions	3
Systems	7
Failures Diagnosed for Systems	8
Exceptions Notified for Systems	9
Discovery Errors Notified for Systems	10
Symptomatic Events Notified for Systems	11
Network Adapters	11
Failures Diagnosed for Network Adapters	12
Symptomatic Events Notified for Network Adapters	15
Connections	16
Failures Diagnosed for Connections	16

Symptomatic Events Notified for Connections	17
VLANs	18
Exceptions Diagnosed for VLANs	18
Chassis	19
Failures Diagnosed for Chassis	19
Cards	19
Failures Diagnosed for Cards	19
Symptomatic Events Notified for Cards	20
Partitions	20
Failures Diagnosed for Partitions	21
Management Agents	22
Failures Diagnosed for Management Agents	22
Symptomatic Events Notified for Management Agents	23
Redundancy Groups	23
Symptomatic Events Notified for Redundancy Groups	24
Creating Redundancy Groups	24
Protocol Endpoints	28
Symptomatic Event Notified for Protocol Endpoints	28
<b>3 Diagnosis of Unstable Elements</b>	<b>31</b>
Thresholds Associated with Unstable Analysis	32
Example of Unstable Analysis	32
Unstable Notifications for Backup or Dial-on-Demand Interfaces	33
<b>4 Viewing Analysis Results and Network Topology</b>	<b>35</b>
Viewing Analysis Results in Notifications	35
Viewing Network Topology in Maps	36
Opening a Network Topology Map	36
About the Network Topology Maps	37
Network Topology Map Type Summary	39
Physical Connectivity Map	40
IP Network Connectivity Map	41
IP Network Membership Map	41
VLAN Connectivity Map	41

---

VLAN Membership Map	42
Group Maps	42
Examples of Maps	43
<b>5 Groups and Settings</b>	<b>45</b>
Default Polling Groups and Settings	46
Polling Groups	46
Polling Settings	46
Default Threshold Groups and Settings	48
Threshold Groups	48
Threshold Settings	51
Unmanaging Interfaces With the Interface Management Policy	54
Ensuring Appropriate VLAN Assignments With the VLAN Tagging Policy	55
Opening the Polling and Thresholds Console	56
Layout of the Polling and Thresholds Console	57
Polling and Thresholds Console Toolbar Buttons	58
Working With Groups and Settings	58
How Managed Elements Are Assigned to Groups	59
Modifying the Properties of a Group	59
Method for Adding or Removing Settings	60
Method for Modifying the Priority of Groups	60
Method for Editing Matching Criteria	61
Method for Modifying the Parameters of a Setting	62
Creating New Polling and Threshold Groups	63
<b>A MIBs Polled and SNMP Traps Processed</b>	<b>65</b>
Standard SNMP MIBs	65
Enterprise MIBs	66
SNMP Traps	67

<b>B</b>	<b>Subscribing to Notifications</b>	<b>69</b>
<b>C</b>	<b>Selected Attributes of Managed Elements</b>	<b>73</b>
	System Attributes	73
	Network Adapter Attributes	74
	Network Connection Attributes	76
	Card Attributes	77
	SNMP Agent Attribute	78
	IP Attributes	78
	Redundancy Group Attributes	79
	HSRP Group Attributes	80
	HSRP Endpoint Attributes	81
<b>D</b>	<b>Polling for Analysis</b>	<b>83</b>
	ICMP Poller	83
	SNMP Poller	84
	Just-In-Time Polling	85
	Request-Consolidation Polling	85
	ICMP and SNMP Polling Coordination	86
	<b>Index</b>	<b>87</b>



# Preface

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

## Intended Audience

This document is intended to be read by IT managers seeking to better understand the value of InCharge IP Availability Manager, by system administrators configuring and using Availability Manager, and by operators receiving and acting upon notifications.

## Prerequisites

Before performing procedures in this document, InCharge IP Availability Manager and InCharge Service Assurance Manager must be installed. The Global Console is required to configure Polling Groups and Threshold Groups. For information about installing these products, see the *InCharge IP Management Suite Installation Guide* and the *InCharge Service Assurance Management Suite Installation Guide*.

# Document Organization

This document consists of the following chapters:

<b>1. INTRODUCTION</b>	Describes concepts of managing network connectivity and the value of InCharge IP Availability Manager.
<b>2. NETWORK ELEMENTS AND THEIR FAILURES</b>	Describes the network elements discovered and managed by Availability Manager and identifies the root-cause failures, symptoms, and exceptions for each element type.
<b>3. DIAGNOSIS OF UNSTABLE ELEMENTS</b>	Describes how Availability Manager determines whether a network adapter or system is unstable.
<b>4. VIEWING ANALYSIS RESULTS AND NETWORK TOPOLOGY</b>	Describes using the Global Console to view the analysis results of Availability Manager in the form of notifications, and to view the network topology of Availability Manager in the form of maps.
<b>5. GROUPS AND SETTINGS</b>	Provides information about the default polling and threshold settings used by Availability Manager.
<b>A. MIBS POLLED AND SNMP TRAPS PROCESSED</b>	Identifies the MIBs and SNMP traps used by Availability Manager to diagnose connectivity problems.
<b>B. SUBSCRIBING TO NOTIFICATIONS</b>	Lists the default set of events subscribed to by Availability Manager and identifies the classes from which all events notified by Availability Manager originate.
<b>C. SELECTED ATTRIBUTES OF MANAGED ELEMENTS</b>	Lists attributes of selected managed elements.
<b>D. POLLING FOR ANALYSIS</b>	Describes the ICMP and SNMP polling engines used by Availability Manager for correlation analysis.

**Table 1:** Document Organization

## Documentation Conventions

Several conventions may be used in this document as shown in Table 2.

CONVENTION	EXPLANATION
sample code	Indicates code fragments and examples in Courier font
<b>keyword</b>	Indicates commands, keywords, literals, and operators in bold
%	Indicates C shell prompt
#	Indicates C shell superuser prompt
<parameter>	Indicates a user-supplied value or a list of non-terminal items in angle brackets
[option]	Indicates optional terms in brackets
<i>/InCharge</i>	Indicates directory path names in italics
<b><i>yourDomain</i></b>	Indicates a user-specific or user-supplied value in bold, italics
<i>File &gt; Open</i>	Indicates a menu path in italics
▼▲	Indicates a command that is formatted so that it wraps over one or more lines. The command must be typed as one line.

**Table 2:** Documentation Conventions

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

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

Finally, unless otherwise specified, the term InCharge Manager is used to refer to InCharge programs such as Domain Managers, Global Managers, and adapters.

## InCharge Installation Directory

In this document, the term **BASEDIR** represents the location where InCharge software is installed.

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

The <n> represents the InCharge software platform version number. The <productsuite> represents the InCharge product suite that the product is part of.

Table 3 defines the <productsuite> directory for each InCharge product.

PRODUCT SUITE	INCLUDES THESE PRODUCTS	DIRECTORY
InCharge IP Management Suite	<ul style="list-style-type: none"> <li>• IP Availability Manager</li> <li>• IP Performance Manager</li> <li>• IP Discovery Manager</li> <li>• InCharge Adapter for HP OpenView NNM</li> <li>• InCharge Adapter for IBM/Tivoli NetView</li> </ul>	/IP
InCharge Service Assurance Management Suite	<ul style="list-style-type: none"> <li>• Service Assurance Manager</li> <li>• Global Console</li> <li>• Business Dashboard</li> <li>• Business Impact Manager</li> <li>• Report Manager</li> <li>• SAM Failover System</li> <li>• Notification Adapters</li> <li>• Adapter Platform</li> <li>• SQL Data Interface Adapter</li> <li>• SNMP Trap Adapter</li> <li>• Syslog Adapter</li> <li>• XML Adapter</li> <li>• InCharge Adapter for Remedy</li> <li>• InCharge Adapter for TIBCO Rendezvous</li> <li>• InCharge Adapter for Concord eHealth</li> <li>• InCharge Adapter for InfoVista</li> <li>• InCharge Adapter for NetIQ AppManager</li> </ul>	/SAM
InCharge Application Management Suite	<ul style="list-style-type: none"> <li>• Application Services Manager</li> <li>• Beacon for WebSphere</li> <li>• Application Connectivity Monitor</li> </ul>	/APP
InCharge Security Infrastructure Management Suite	<ul style="list-style-type: none"> <li>• Security Infrastructure Manager</li> <li>• Firewall Performance Manager</li> <li>• InCharge Adapter for Check Point/Nokia</li> <li>• InCharge Adapter for Cisco Security</li> </ul>	/SIM
InCharge Software Development Kit	<ul style="list-style-type: none"> <li>• Software Development Kit</li> </ul>	/SDK

**Table 3:** Product Suite Directory for InCharge Products

For example, on UNIX operating systems, InCharge IP Availability Manager is, by default, installed to `/opt/InCharge6/IP/smarts`. This location is referred to as **BASEDIR**/`smarts`.

Optionally, you can specify the root of **BASEDIR** to be something other than */opt/InCharge6* (on UNIX) or *C:\InCharge6* (on Windows), but you cannot change the *<productsuite>* location under the root directory.

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

## Additional Resources

In addition to this manual, SMARTS provides the following resources.

### InCharge Commands

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

### Documentation

Readers of this manual may find other SMARTS documentation (also available in the **BASEDIR**/*smarts/doc/pdf* directory) helpful.

#### **InCharge Documentation**

The following SMARTS documents are product independent and thus relevant to users of all InCharge products:

- *InCharge Release Notes*
- *InCharge Documentation Roadmap*
- *InCharge System Administration Guide*
- *InCharge ICIM Reference*
- *InCharge ASL Reference Guide*
- *InCharge Perl Reference Guide*

#### **InCharge IP Management Documentation**

The following SMARTS documents are relevant to users of the InCharge IP Management product suite.

- *InCharge IP Management Suite Installation Guide*
- *InCharge IP Deployment Guide*

- *InCharge IP Discovery Guide*
- *InCharge IP Availability Manager User's Guide*
- *InCharge IP Performance Manager User's Guide*
- *InCharge IP Adapters User's Guide*

## Common Abbreviations and Acronyms

The following lists common abbreviations and acronyms that are used in the InCharge guides.

ASL	Adapter Scripting Language
CDP	Cisco Discovery Protocol
ICIM	InCharge Common Information Model
ICMP	Internet Control Message Protocol
IP	Internet Protocol
MSFC	Multilayer Switch Feature Card
MIB	Management Information Base
MODEL	Managed Object Definition Language
RSFC	Router Switch Feature Card
RSM	Router Switch Module
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network

## Technical Support

SMARTS provides technical support by e-mail or phone during normal business hours (8:00 A.M.—6:00 P.M. U.S. Eastern and Greenwich Mean Time). In addition, SMARTS offers the InCharge Express self-service web tool. The web tool allows customers to access a personalized web page and view, modify, or create help/trouble/support tickets. To access the self-service web tool, point your browser to:

<https://websupport.smarts.com/SelfService/smarts/en-us>

**U.S.A Technical Support**

E-Mail: [support@smarts.com](mailto:support@smarts.com)

Phone: +1.914.798.8600

**EMEA Technical Support**

E-Mail: [support-emea@smarts.com](mailto:support-emea@smarts.com)

Phone: +44 (0) 1753.878140

**Asia-Pac Technical Support**

E-Mail: [support-asiapac@smarts.com](mailto:support-asiapac@smarts.com)

You may also contact SMARTS at:

	<b>U.S.A WORLD HEADQUARTERS</b>	<b>UNITED KINGDOM</b>
<b>ADDRESS</b>	SMARTS 44 South Broadway White Plains, New York 10601 U.S.A	SMARTS Gainsborough House 17-23 High Street Slough Berkshire SL1 1DY United Kingdom
<b>PHONE</b>	+1.914.948.6200	+44 (0)1753.878110
<b>FAX</b>	+1.914.948.6270	+44 (0)1753.878111

For sales inquiries, contact SMARTS Sales at:

[sales@smarts.com](mailto:sales@smarts.com).

SMARTS is on the World Wide Web at:

<http://www.smarts.com>





## Introduction

In a typical managed network, a management station monitors the network's elements by frequently probing its devices. The management station generates an alarm when elements fail to respond to a probe. One failed element in the network breaks the connectivity between the management station and all other network elements reached through the failed element. As a result of a failure, the management station generates an alarm for each unreachable element, making it difficult to determine which element has failed. The challenge of managing network connectivity is determining which alarms are real problems in the network and which alarms are symptomatic events that are caused by other element failures.

InCharge IP Availability Manager (Availability Manager) correlates the alarms that are generated as a result of a failure, pinpoints the failed element, and identifies all managed elements affected by the failure. With Availability Manager, you can focus on addressing the failed element and can consider all other alarms as symptomatic events.

Availability Manager diagnoses connectivity failures in multi-vendor, switched, and routed networks. It also discovers and manages physical and logical Layer 2 and Layer 3 elements. Layer 2 elements transmit packets from network node to network node based on station address. Layer 3 elements route data to different Local Area Networks (LANs) and Wide Area Networks (WANs) based on network address.

# Availability Monitoring

Availability Manager monitors and discovers the network by sending Internet Control Message Protocol (ICMP) polls and Simple Network Management Protocol (SNMP) polls. The results of this polling, in conjunction with traps, are used to diagnose the failed elements that interrupt network connectivity.

# Availability Notifications

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

- Root-cause notifications indicate points of failure diagnosed by Availability Manager. Each root-cause notification indicates a separate failure.
- Symptomatic events indicate abnormal conditions and are used by Availability Manager to determine the root-cause failures.
- Exception notifications, or aggregate events, indicate one or more related failures are associated with a high-level network element or any of the element's components. For example, an exception notification is generated for a router when a card on the router has a problem or the router is down.

Notifications are displayed in the Notification Log of the Global Console. Root-cause failures diagnosed by Availability Manager display a value of "Yes" for the value of the `IsRoot` attribute and identify the Availability Manager Domain Manager by name in the `Source` attribute.

# 2

## Network Elements and Their Failures

This chapter describes the elements discovered and managed by InCharge IP Availability Manager and the connectivity-related failures diagnosed for each element. The diagnosis identifies root-cause failures in a managed network, indicating problems that require immediate attention. Availability Manager correlates the apparent failures of other elements reached through the failed element to the root cause and only notifies you of the problem origin.

In addition to root-cause failures, Availability Manager also reports exceptions for network elements that encounter a failure in one or more of their components.

### Summary of Faults, Symptomatic Events, and Exceptions

The following tables summarize the notifications generated by Availability Manager for each type of managed element.

Table 4 lists the root-cause problems diagnosed by Availability Manager, including the symptomatic events for each problem and any additional conditions that must be satisfied to result in the proper diagnosis. For more information about where the listed symptomatic events are observed, refer to the appropriate section of this chapter in which the problem is described in more detail.

MANAGED ELEMENT	ROOT CAUSE	CONDITION	SYMPTOMS OF ROOT CAUSE
System	Down	None	System Might Be Down
			Network Adapter Down or Flapping
	Unstable	None	SNMPAgent Repeated Restarts
Network Adapter	Down	Port or interface is managed and not connected	Network Adapter Down or Flapping
			System Might Be Down
	Unstable	Port or interface is managed and not connected	Network Adapter Down or Flapping
			IsFlapping=TRUE
	Disabled	Port or interface is connected or is a physical interface with sub-interfaces layered over it	Network Adapter Administratively Down
			Network Adapter Down or Flapping
System Might Be Down			
Logical Connection Down	No failure symptoms at physical layer	Network Adapter Down or Flapping	
		Physical interface with sub-interfaces layered over it	System Might Be Down
Connection	Down	Physical connection such as cable, serial, or point-to-point	Network Adapter Down
			Unstable
		IsNetworkAdapterFlapping=TRUE	
Chassis	Down	Chassis packages more than one system	System Down
Card	Down	None	Card Operationally Down
			Card Down
			Network Adapter Down
			System Down
			Card Switch Over
Partition	Down	None	System Unresponsive
Management Agent	Not Responding	None	Management Agent Unresponsive

Table 4: Root-Cause Problems Diagnosed by Availability Manager

Table 5 lists the exceptions notified by Availability Manager and the events that can cause each exception to be notified.

<b>MANAGED ELEMENT</b>	<b>EXCEPTION</b>	<b>CAUSE</b>
System	Connectivity Exception	System Down
		System Unstable
		SNMP Agent Not Responding
		Network Adapter Down
		Network Adapter Unstable
		Network Adapter Logical Connection Down
		Network Adapter Disabled
		Card Down
		Chassis Down
	Operational Exception	System Unresponsive
		SNMP Agent Unresponsive
		SNMP Agent Repeated Restarts
		Card Operationally Down
		Network Adapter Down or Flapping
		Network Adapter Backup Activated
		Network Adapter Exceeded Maximum Uptime
	VLAN	Connectivity Exception
Port Down		
Port Unstable		
Port Disabled		
Operational Exception		Port Down Or Flapping
		Port Backup Activated
		Port Exceeded Maximum Uptime

**Table 5:** Exceptions Notified by Availability Manager

Table 6 lists the symptomatic events, and their associated thresholds, Availability Manager monitors for each managed element.

MANAGED ELEMENT	SYMPTOMATIC EVENT	THRESHOLD (SETTING)
System	Discovery Error	None
	Might Be Down	None
	Unresponsive	None
Network Adapter	Backup Activated	Maximum Uptime (Backup Interface Support)
	Exceeded Maximum Uptime	Maximum Uptime (Backup Interface Support or Dial-On-Demand Interface Support)
	Administratively Down	None
	Down Or Flapping	Link Trap Threshold Link Trap Window (Interface/Port Flapping)
Connection	Down Or Flapping	See Down Or Flapping for Network Adapters
Card	Operationally Down	None
	Switch Over	
Management Agent	Unresponsive	None
	Repeated Restarts	Restart Trap Threshold Restart Trap Window (Connectivity)
IP	Down	None
	Unresponsive	
Duplicate IP	Duplicate	None
Redundancy Group	All Components Down	At Risk Threshold (not user-configured)
	At Risk	
	Reduced Redundancy	
	Switch Over Failed (HSRP Group only)	
HSRP Endpoint	Switch Over	None

**Table 6: Symptomatic Events Notified by Availability Manager**

# Systems

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

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

The router may also be a *virtual router* (VR) which is a software emulation of a router implemented within a physical router or switch. Virtual routers have independent IP routing and forwarding tables and they are isolated from each other even when implemented in the same physical device. This permits routing using any routing technology and forwarding packets as with standard routers. Virtual routers are often used with virtual private networks (VPNs) to allow a greater separation of VPN traffic while using the same equipment.

- *Router Switch Feature Card (RSFC)* — A card in a Cisco Catalyst switch that runs Cisco IOS router software and is used to perform routing between VLANs.

- *Router Switch Module (RSM)* — An RSM is a router installed as a card in a switch to perform routing between VLANs.
- *Switch* — A switch is a network element that switches packets, typically at wire speeds, between physically separate network segments.
- *Terminal Server* — A specialized system that connects terminals to a network.
- *Unsupported* — An unsupported element identifies a system that is not supported. This class is no longer used but is retained for backward compatibility.

## Failures Diagnosed for Systems

Availability Manager diagnoses two root-cause failures for systems.

### **System Down**

*Down* indicates that a system has failed. A system failure causes all ports or interfaces on the system and all elements accessed through the system to be unreachable.

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

When a system is connected to one or more systems, the symptomatic events for *Down* include:

- *Might Be Down* for the system itself and any connected systems.
- *Down Or Flapping* for any peer network adapter and any peer sub-interfaces.

### **System Unstable**

*Unstable* indicates that a system has repeatedly restarted over a short period of time and is considered unstable. The Restart Trap Threshold and the Restart Trap Window parameters in the Connectivity setting for the System Resources Groups control the analysis for a system unstable condition. For information about these parameters, refer to [Connectivity](#) on page 52.

For more information about how Availability Manager concludes that a system is unstable, refer to [Diagnosis of Unstable Elements](#) on page 31.

The symptomatic event used to diagnose *Unstable* is *SNMP Agent Repeated Restarts*.



## Exceptions Notified for Systems

Availability Manager notifies an exception for a system when it diagnoses one or more faults for the affected system. For example, when Availability Manager diagnoses *SNMP Agent Not Responding* for a system, Availability Manager also notifies a *Connectivity Exception*. The Details tab in the Notification Properties dialog for the Connectivity Exception notification lists all of the active connectivity-related faults that resulted in the exception. Likewise, when Availability Manager diagnoses a fault such as *SNMP Agent Repeated Restarts* for a system, Availability Manager notifies an *Operational Exception*.

### **System Connectivity Exception**

*Connectivity Exception* is an aggregate event that indicates that one or more connectivity-related root-cause failures 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 *Connectivity Exception* will be reported for the system.

Root-cause failures that result in a *Connectivity Exception* include:

- System Down
- System Unstable
- SNMP Agent Not Responding
- VR Agent Not Responding
- Network Adapter Down
- Network Adapter Unstable
- Network Adapter Logical Connection Down
- Network Adapter Disabled
- Card Down
- Chassis Down

### **System Operational Exception**

*Operational Exception* 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 SNMP agent is repeatedly restarting.

Failures and symptomatic events that cause an *Operational Exception* include:

- System Unresponsive

- SNMP Agent Unresponsive
- SNMP Agent Repeated Restarts
- VR Agent Unresponsive
- VR Agent Repeated Restarts
- Card Operationally Down
- Network Adapter Down or Flapping
- Network Adapter Backup Activated
- Network Adapter Exceeded Maximum Uptime
- Disk Operationally Down

---

**Note:** Disk Operationally Down is a symptomatic event that causes an *Operational Exception* for host systems. This event is notified by the InCharge IP Server Performance Manager.

---

## Discovery Errors Notified for Systems

A *Discovery Error* notification is a symptomatic event that indicates that the discovery process did not discover a device. Any root-cause problem diagnosed by Availability Manager can explain a discovery error. For example, a Discovery Error might result if a system is diagnosed as *Down* and is not, therefore, reachable during discovery.

A Discovery Error is notified under the following conditions:

- SNMP request times out
- SNMP agent 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 Discovery Error notification. For information about resolving Discovery Errors, see the *InCharge IP Discovery Guide*.

---

**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 InCharge volume licenses. For information about the effects of this event, see the *InCharge IP Discovery Guide*.

---

## Symptomatic Events Notified for Systems

Table 7 lists the symptomatic events notified for systems.

SYMPTOMATIC EVENT	DESCRIPTION
Might Be Down	Indicates that all of the system's Host Access Points (IP interfaces) and Host Services (SNMPAgent) are not responding and the system is logically near the root-cause problem.
Unresponsive	Indicates that all of the system's Host Access Points (IP interfaces) and Host Services (SNMPAgent) are not responding.
Discovery Error	Indicates that an error occurred while discovering the system.

**Table 7:** Symptomatic Events Notified for Systems

## Network Adapters

A network adapter is a logical or physical component of a network device at which the device connects to a network. Ports and interfaces are examples of network adapters.

- *Port* – A port is 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.

Availability Manager separates ports into two groups: trunk ports and access ports. A trunk port is a switch port that is connected to a switch, router, hub, or bridge. An access port is connected to a host. Access ports are only managed if the connected host is also a member of the managed topology or the port is explicitly managed.

- *Interface* – An interface is 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.
- *Sub-interface* – A sub-interface is a logical division of a physical interface. A physical interface can be divided into one or more sub-interfaces. 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 sub-interface.

## Failures Diagnosed for Network Adapters

Problems diagnosed for a network adapter failure include *Down*, *Unstable*, *Disabled*, and *Logical Connection Down*. Availability Manager also notifies the *Backup Activated* and *Exceeded Maximum Uptime* symptomatic events for network adapters.

### Network Adapter Down

*Down* indicates that a port or interface has failed or is in testing mode. A *Down* notification is only generated when the port or interface is not physically connected. When a port or interface is physically connected, *Network Adapter Down* is superseded by a *Network Connection Down* notification.

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

- *Trunk Cable Down* if the port is connected via a trunk cable.
- *Cable Down* if the port is connected via a cable.

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

- *Network Connection Down* if the interface is connected via a physical network connection.
- *Cable Down* if the interface is connected via a cable.

Notification of *Network Adapter Down* is controlled by the Testing Notification Mode threshold. For information about the Testing Notification Mode threshold, see [Connectivity](#) on page 52.

The symptomatic events used to diagnose *Down* include:

- *Down Or Flapping* for the network adapter and any sub-interfaces
- *Down Or Flapping* for any peer interfaces
- *Might Be Down* 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 Link Trap Threshold and Link Trap Window parameters contained in the Interface/Port Flapping setting control analysis for the network adapter unstable condition. For more information about these parameters, refer to [Interface/Port Flapping \(Unstable\)](#) on page 53.

For more information about how Availability Manager concludes that a network adapter is unstable, refer to [Diagnosis of Unstable Elements](#) on page 31.

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 *Network Connection Unstable* notification.

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

- *Trunk Cable Unstable* if the port is connected via a trunk cable.
- *Cable Unstable* if the port is connected via a cable.

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

- *Network Connection Unstable* if the interface is connected via a physical network connection
- *Cable Unstable* if the interface is connected via a cable.

---

**Note:** By default, *Interface Unstable* analysis is not performed on ISDN B channel, ISDN D channel, backup, or dial-on-demand interfaces. To enable *Interface Unstable* analysis for these types of interfaces, see [Unstable Notifications for Backup or Dial-on-Demand Interfaces](#) on page 33.

---

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

- *Down Or Flapping* for the network adapter and any sub-interfaces
- *Down Or Flapping* for any peer interfaces
- *Might Be Down* 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 sub-interfaces layered over them, and for ports or interfaces that are logically connected.

The symptomatic events used to diagnose *Disabled* include:

- *Administratively Down* for the port or interface
- *Down Or Flapping* or *Administratively Down* all sub-interfaces
- *Down Or Flapping* for all peer sub-interfaces
- *Might Be Down* for all physically or logically connected systems

### **Network Adapter Logical Connection Down**

*Logical Connection Down* indicates a fault within the Wide Area Network, which could be, for example, a Frame Relay cloud. Availability Manager isolates the problem to the nearest physical interface using only symptoms from the logical layer. *Logical Connection Down* is only notified when there are no failure symptoms at the physical layer and the network adapter is a physical interface with sub-interfaces layered over it.

The symptomatic events used to diagnose *Logical Connection Down* are also used to diagnose *Network Adapter Down*. However, for *Logical Connection Down*, the *DownOrFlapping* symptomatic event for the interface is not present.

The symptomatic events used to diagnose *Logical Connection Down* include:

- *Down Or Flapping* for all sub-interfaces and peer sub-interfaces
- *Might Be Down* for all logically connected systems

## Symptomatic Events Notified for Network Adapters

Table 8 lists the symptomatic events notified for network adapters.

SYMPTOMATIC EVENT	DESCRIPTION
Backup Activated	<p><i>Backup Activated</i> indicates that a backup port/interface has become operational. By default, interfaces with a value of <i>ISDN</i> for the Type attribute are marked as backup and use the Backup Interface Support setting.</p> <p>Because a backup should not normally be online, Availability Manager notifies you when the backup interface or port becomes operational. For more information about backup activation, see <a href="#">Backup Interface Support</a> on page 51.</p>
Exceeded Maximum Uptime	<p><i>Exceeded Maximum Uptime</i> indicates that a backup or dial-on-demand port/interface has been in the <i>Up</i> 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:</p> <ul style="list-style-type: none"> <li>• ISDNBCHANNEL (Backup)</li> <li>• ISDN (Backup)</li> <li>• PPP or SLIP (Dial-On-Demand)</li> </ul> <p>Because a backup should not normally be up for very long, Availability Manager notifies you when the <i>Maximum Uptime</i> has been exceeded for a device marked as backup or dial-on-demand.</p> <p>For more information about the Maximum Uptime threshold, see either <a href="#">Backup Interface Support</a> on page 51 or <a href="#">Dial-On-Demand Interface Support</a> on page 53.</p>
Administratively Down	<p><i>Administratively Down</i> indicates that a port or interface is down because it has been explicitly disabled, which is indicated by the value of the AdminStatus attribute.</p>
Down Or Flapping	<p><i>Down Or Flapping</i> indicates that the port/interface is operationally down (value of the AdminStatus attribute is UP and the value of OperStatus is DOWN) or that too many link down traps have been received within the link trap window (value of IsFlapping attribute is TRUE). Flapping is a symptom of a network adapter unstable problem.</p> <p>For more information about how Availability Manager concludes that a network adapter is unstable, refer to <a href="#">Interface/Port Flapping (Unstable)</a> on page 53.</p>

**Table 8:** Symptomatic Events Notified for Network Adapters

## Connections

A connection is a link between two network adapters. (For more information, see [Network Adapters](#) on page 11.) The following types of connections are discovered and managed:

- *Cable*—A cable is a connection between a port and an interface. For example, a cable connects a port on a switch to an interface on a router.
- *Trunk Cable*—A trunk cable is a connection between two ports. Switches are often trunked to connect multiple segments or to provide redundant pathways through the network.
- *Network Connection*—A network connection is a connection between two interfaces. A network connection can be a logical connection or a physical connection. An example of a logical connection is when routers are connected via 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 via a serial or point-to-point connection.

## Failures Diagnosed for Connections

A connection can be a cable, trunk cable, or network connection. Problems diagnosed for a connection include *Down* and *Unstable*.

### Connection Down

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

- A *Cable Down* notification supersedes a *Port Down* or an *Interface Down* notification if the port, interface, or both are down.
- A *Trunk Cable Down* notification supersedes a *Port Down* notification if one or both ports are down.
- A *Network Connection Down* notification supersedes an *Interface Down* notification if one or both interfaces are down.

If the network adapters are not physically connected, a *Network Adapter Logical Connection Down* notification supersedes a *Connection Down* notification.



The symptomatic event for *Connection Down* is *Network Adapter Down Or Flapping* for one or both of the network adapters. To distinguish *Connection Down* from *Connection Unstable*, the value of the `IsNetworkAdapterFlapping` attribute must also be `FALSE`.

### 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* notification supersedes a *Port Unstable* or *Interface Unstable* notification if a cable connects a port or an interface that is unstable.
- A *Trunk Cable Unstable* notification supersedes a *Port Unstable* notification if a trunk cable connects a port that is unstable.
- A *Network Connection Unstable* notification supersedes an *Interface Unstable* notification if a network connection connects an interface that is unstable to another interface.

The symptomatic event for *Connection Unstable* is *Network Adapter Down Or Flapping*. To distinguish *Connection Unstable* from *Connection Down*, the value of the `IsNetworkAdapterFlapping` attribute must also be `TRUE`.

Flapping for network adapters is diagnosed using the setting described in [Interface/Port Flapping \(Unstable\)](#) on page 53. The flapping condition can be diagnosed for network adapters as well as any sub-interfaces.

## Symptomatic Events Notified for Connections

Table 9 lists the symptomatic events for connection elements.

SYMPTOMATIC EVENT	DESCRIPTION
Down Or Flapping	Indicates that one or both of the network adapters on either end of the connection are operationally down or unstable.  This symptomatic event is used to enhance the display of maps in the Global Console.

**Table 9:** Symptomatic Events Notified for Connections

## VLANs

A VLAN is a logical subgroup within a local area network that is created by software rather than by manually moving cables in the wiring closet. The VLAN groups user stations and network devices into a single logical network regardless of the physical LAN segment that the stations or devices are attached to. A VLAN allows traffic to flow within populations of mutual interest.

### Exceptions Diagnosed for VLANs

Availability Manager reports connectivity and operational exceptions for VLAN elements.

#### **VLAN Connectivity Exception**

*Connectivity Exception* is an aggregate event diagnosed for a VLAN. A connectivity exception indicates that one or more connectivity-related root-cause failures exist for any port, card, or switch that is a member of the VLAN.

Failures that cause a *Connectivity Exception* include:

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

#### **VLAN Operational Exception**

*Operational Exception* is an aggregate event diagnosed for a VLAN. An operational exception indicates that one or more operational exceptions exist for any port or card that is a member of the VLAN.

Failures that cause an *Operational Exception* include:

- Port Down Or Flapping
- Port Backup Activated
- Port Exceeded Maximum Uptime

## Chassis

A chassis is a physical package 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.

### Failures Diagnosed for Chassis

*Down* is the only problem diagnosed for chassis elements.

#### **Chassis Down**

*Down* indicates that a chassis has failed. A chassis failure causes all devices in the chassis to fail. If the chassis packages only one system, *System Down* supersedes *Chassis Down*.

The symptomatic events used to diagnose *Chassis Down* are *System Down* for systems packaged by the chassis or *System Down* for systems packaged by the cards that are a part of the chassis.

## Cards

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

### Failures Diagnosed for Cards

Availability Manager diagnoses *Down* problems for cards.

#### **Card Down**

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

- Operationally Down for the card
- Card Down for any sub-cards
- Switch Over 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

## Symptomatic Events Notified for Cards

Table 10 lists the symptomatic events notified for cards.

SYMPTOMATIC EVENT	DESCRIPTION
Operationally Down	Indicates that the card is instrumented and the value of the Status attribute is CRITICAL. Typically, Operationally Down means that the card has failed or been removed.
Switch Over	<p>Indicates that the standby status of the card has changed from INACTIVE to ACTIVE within the last 30 minutes.</p> <p>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 <i>Card Down</i> or a <i>Redundancy Group AtRisk</i> notification because it is not caused by a physical failure.</p> <p><i>Switch Over</i> is notified when the standby status of the card changes, as indicated by the moduleStandbyStatus MIB. In order for the <i>Switch Over</i> event to be notified, 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.</p> <p>Analysis for <i>Switch Over</i> is only supported for switches that support the CISCO-STACK-MIB and where the moduleStandbyStatus correctly reflects the status of the card.</p>

**Table 10:** Symptomatic Events Notified for Cards

## Partitions

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

Some elements along the path, however, may not actually be represented in your network topology. For example, those elements might not have SNMP agents; Availability Manager may not have access to their SNMP agents; 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 elements on the path.

Availability Manager's root-cause analysis algorithms need to determine the connectivity among managed elements. When the topology is incomplete, Availability Manager creates partitions to allow analysis to proceed. Within a single partition, any two managed elements are indeed connected by a path. However, elements within distinct partitions have no path between them in the topology, even though they are connected in the actual network.

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

You can assign names to the partitions in your network using the *partition.conf* file. For more information about naming partitions, see the *InCharge IP Discovery Guide*.

## Failures Diagnosed for Partitions

A partition is another type of logical link, similar to a VLAN or an IP Network. Availability Manager diagnoses the *Down* problem for partitions.

### **Partition Down**

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

## Management Agents

A management agent is a type of service. A service is a logical element that contains the information necessary to represent, configure, or manage some functionality provided by a device or software feature.

- *SNMP Agent*—An agent that manages and monitors network devices and their functions. An SNMP agent implements one or more MIBs and provides access to MIB data for management applications. An SNMP Agent typically listens on UDP port 161.
- *VR Agent*—An agent that manages and monitors virtual routers, and their functions and interfaces.

## Failures Diagnosed for Management Agents

Availability Manager diagnoses the *Not Responding* problem for management agents.

### **Agent Not Responding**

*Not Responding* indicates that a management agent is not responding to SNMP requests but that the host system is responding to ICMP pings. This is typically caused by the use of an incorrect community string (SNMP V1 or V2C) or it may indicate that the agent is hung.

Availability Manager automatically subscribes to management agent *Not Responding* notifications. When Availability Manager receives a management agent *Not Responding* notification, it adds the agent to the Pending Devices List.

The symptomatic event used to diagnose management agent *Not Responding* is management agent *Unresponsive*.

## Symptomatic Events Notified for Management Agents

Table 11 lists the symptomatic events notified for management agents.

SYMPTOMATIC EVENT	DESCRIPTION
Unresponsive	Indicates that the management agent is not responding to SNMP requests but that the system hosting the management agent is responding to ICMP pings.
Repeated Restarts	Indicates that Availability Manager has received an abnormal number of Restart traps from the management agent within a short period of time. This symptomatic event is used to diagnose <i>System Unstable</i> problems.  The Restart Trap Threshold and the Restart Trap Window parameters in the Connectivity setting for the System Resources Groups control the analysis for a system unstable condition. For more information about these parameters, refer to <a href="#">Connectivity</a> on page 52.

**Table 11:** Symptomatic Events Notified for Management Agents

## Redundancy Groups

A redundancy group consists of two or more elements of the same type that are configured in such a way as to provide backup resources for critical network elements. For example, a remote site accessed through two routers can be modeled as a redundancy group that contains two routers. If one router experiences a failure, access is not interrupted but less resilient to additional failures. A failure in the other router renders the remote site inaccessible.

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

- *HSRP Group*—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 HSRP group share an IP address and a MAC (Layer 2) address.
- Card Redundancy Group
- Network Adapter Redundancy Group

- Network Connection Redundancy Group
- System Redundancy Group

The state of a redundancy group is based on the status of its component elements. The following symptomatic events are diagnosed for redundancy groups.

### Symptomatic Events Notified for Redundancy Groups

Availability Manager notifies symptomatic events for redundancy groups. The *AtRiskThreshold*, which is used for the analysis of both *At Risk* and *Reduced Redundancy* symptomatic events, is the lower bound for the 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 *At Risk* notification is generated. The value of the *AtRiskThreshold* is 1.

#### **All Components Down**

*All Components Down* is a symptomatic event that indicates that all elements in the redundancy group are down.

#### **At Risk**

*At Risk* is a symptomatic event that indicates that the number of responsive or operational elements in the redundancy group is below the *AtRiskThreshold*.

#### **Reduced Redundancy**

*Reduced Redundancy* is a symptomatic event that indicates that at least one element in the redundancy group is unresponsive or not operational but the number of responsive or operational elements is above the *AtRiskThreshold*.

#### **Switch Over Failed (HSRP Group only)**

*Switch Over Failed* is a symptomatic event that indicates that traffic fails to switch from an active interface to a standby interface in an HSRP Group and that all interfaces in the HSRP Group are inactive.

### Creating Redundancy Groups

Analysis and monitoring of a redundancy group occurs automatically when a redundancy group is created and its member elements are inserted into the group.



### Creating HSRP Groups

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

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

### Card Redundancy Groups

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

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

### System Redundancy Groups

Redundancy groups for network adapters, network connections, and systems must be manually created using the *dmctl* utility or an ASL script.

To create a redundancy group for one of these types of elements, complete the following steps:

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

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

```
% BASEDIR/smarts/bin/dmctl -s INCHARGE-AM-PM
Server INCHARGE-AM-PM User: admin
admin's Password: XXXXXXXX
Domain Manager Control Program (V6.0) -- Type 'help' for a
list of commands.
Attached to 'INCHARGE-AM-PM'
dmctl> create SystemRedundancyGroup::RouterRedundancyGroup
```

```
dmctl> insert SystemRedundancyGroup::RouterRedundancyGroup::  
ComposedOf Router::router1.smarts.com  
dmctl> insert SystemRedundancyGroup::RouterRedundancyGroup::  
ComposedOf Router::router2.smarts.com
```

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

### Network Adapter Redundancy Groups

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

---

**Note:** By default, a value of testing for the network adapter's status results in a Down notification. You can modify this behavior with the Testing Notification Mode, which is described in [Connectivity](#) on page 52.

---

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

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

In the first example, both network adapters are part of the host named *host\_1*. Because of this, the redundancy group is inserted into the *PartOf* relationship with the host. If *host\_1* is unresponsive, Availability Manager does not generate any notifications about the redundancy group. If the group is not part of the system, Availability Manager would notify *AllComponentsDown* when *host\_1* is unresponsive.

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

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

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

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

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

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

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

```
rg = create("NetworkAdapterRedundancyGroup",
            My-Redundancy-Group");
```

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

## Protocol Endpoints

A protocol endpoint is a type of service access point. Availability Manager supports the creation and analysis of protocol endpoints for the following elements:

- An HSRP endpoint is a logical element defined for each interface of an HSRP group on the hosting router.
- An IP endpoint describes the IP layer characteristics of a network-attached interface. An IP endpoint is designated by a unique IP address.

## Symptomatic Event Notified for Protocol Endpoints

Availability Manager notifies the following symptomatic events for protocol endpoints: *Down*, *Unresponsive*, *Duplicate IP*, and *Switch Over*.

### **Down (IP Endpoint only)**

*Down* indicates that an IP endpoint is not responding to ICMP polls and 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 may be disabled but the physical interface is still up.

### **Unresponsive (IP Endpoint only)**

*Unresponsive* indicates that an IP endpoint is not responding to ICMP polls. Similar to *Down*, the value of the IPStatus attribute is not OK or UNKNOWN.

**Duplicate IP (IP Endpoint only)**

*Duplicate* indicates that the discovery process discovered two or more devices with the same IP address. When this event occurs, Availability Manager classifies the IP address as a Duplicate IP, suspends IP-related analysis for the address, and generates a *Duplicate* notification.

For information about correcting Duplicate IP errors, see the *InCharge IP Discovery Guide*.

**Switch Over (HSRP Endpoint only)**

Availability Manager notifies the *Switch Over* symptomatic event for HSRP endpoints. This event indicates that traffic at the endpoint is switching from an active interface to a standby interface.



## Diagnosis of Unstable Elements

This chapter describes how InCharge IP Availability Manager concludes that an element is unstable. A system or network adapter is considered to be unstable if it fluctuates too often between up and down states over a short period of time. Availability Manager monitors a system or network adapter's state via the SNMP traps it receives. Availability Manager determines when to send an *Unstable* notification based on a combination of fixed values and user-controlled settings. Availability Manager also calculates a stable time in which to wait before clearing an *Unstable* notification.

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

- *Warm Start Traps* and *Cold Start Traps* for a system (see [Connectivity](#) on page 52)
- *Link Up* or *Link Down Traps* for a network adapter (see [Interface/Port Flapping \(Unstable\)](#) on page 53)

---

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

---

## Thresholds Associated with Unstable Analysis

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

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

## Example of Unstable Analysis

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

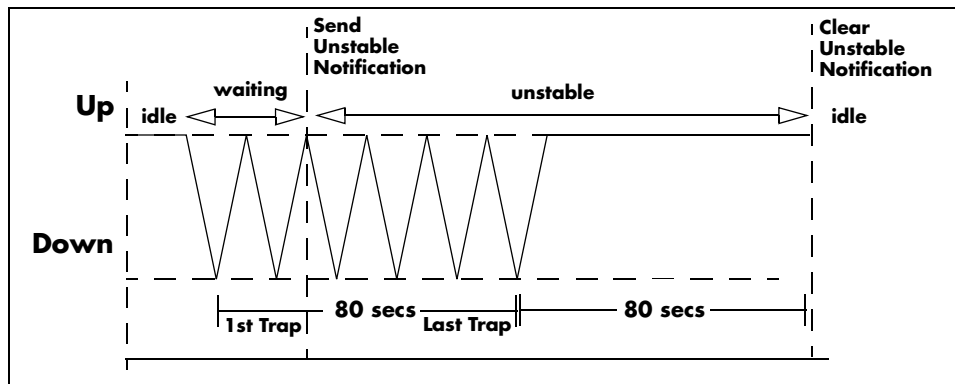


Figure 1: Unstable System/Network Adapter Diagnosis



In the example, assume that the Link/Restart Trap Window parameter has a value of 30 seconds and that the Link/Restart Trap Threshold parameter has a value of 2. Availability Manager would perform the following actions:

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

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

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

## Unstable Notifications for Backup or Dial-on-Demand Interfaces

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

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

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

Table 12 summarizes the notifications that may appear after you apply the Interface/Port Flapping setting to backup interfaces or dial-on-demand interfaces.

SETTINGS	RESULTING NOTIFICATIONS
Interface/Port Flapping Backup Interface Support	<ul style="list-style-type: none"><li>• The <i>Down</i> notification is not generated if the interface is down.</li><li>• The <i>Backup Activated</i> notification is generated if the interface comes up.</li><li>• The <i>Exceeded Maximum Uptime</i> notification is generated if the interface stays up too long.</li><li>• The <i>Unstable</i> notification is generated if the interface or port is going up and down.</li></ul>
Interface/Port Flapping Dial-On-Demand Interface Support	<ul style="list-style-type: none"><li>• The <i>Down</i> notification is not generated if the interface is down.</li><li>• The <i>Exceeded Maximum Uptime</i> notification is generated if the interface stays up too long.</li><li>• The <i>Unstable</i> notification is generated if the interface or port is going up and down.</li></ul>

**Table 12:** Combined Settings and Their Notifications

For more information about working with groups and settings, see [Working With Groups and Settings](#) on page 58.

# 4

## Viewing Analysis Results and Network Topology

This chapter describes using the Global Console to view the results of the analysis provided by Availability Manager in the form of notifications. It also describes using the Global Console to view the network topology in the form of the following maps:

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

### Viewing Analysis Results in Notifications

Availability Manager reports notifications to the InCharge Service Assurance Manager, and Service Assurance Manager combines these notifications with the notifications from the other InCharge Domain Managers connected to Service Assurance Manager. You can view the notifications through the Global Console.

The Global Console displays notifications in two basic ways:

- Through the tabular format of a Notification Log Console view
- Through the uniquely colored indicators appearing with the device icons in a Map Console view

For information about the topology elements monitored by Availability Manager and the problems diagnosed, see [Network Elements and Their Failures](#) on page 3. For information about the Notification Log Console, see the *InCharge Operator's Guide*.

---

**Note:** Service Assurance Manager is also known as the Global Manager.

---

## Viewing Network Topology in Maps

Availability Manager sends a copy of its network topology to InCharge Service Assurance Manager, and Service Assurance Manager combines this topology with the topologies received from the other InCharge Domain Managers connected to Service Assurance Manager.

You can view a variety of network topology maps using the Map Console view of the Global Console. For information about the Map Console and general map concepts such as hops and color-coding in maps, see the *InCharge Operator's Guide*.

## Opening a Network Topology Map

The network topology maps are available when you attach the Global Console to a Global Manager. Several methods exist to access a map, the most common methods are:




- Open the Map Console from the Global Console by selecting *File > New > Map Console*. In the Topology tab of the Map Console, click a network topology element to display a map of the element. To select a different map type for the element, right-click the element and select a different map type in the pop-up menu.









- Select the Show Map option from any opened console attached to Service Assurance Manager. For example, in the Notification Log Console, click a notification and then select *Event > Show Map*, or right-click the notification and then select Show Map in the pop-up menu. In the Topology Browser Console, right-click an element and select Show Map in the pop-up menu.
- Right-click on an element in a map and select a network map from the pop-up menu.



## About the Network Topology Maps

A network topology map contains elements that may include IP networks, VLANs, routers, switches, hosts, and various types of connections such as cables and trunk cables. Table 13 identifies and describes the default icons and other visual indicators that may appear in a network topology maps. In the Map Console, you can also select *Map > Map Legend* to see a similar list.

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

ICON / VISUAL INDICATOR	DESCRIPTION
	Icon can represent a bridge, host, probe, terminal server, node, or an unsupported device.
	Icon represents a hub.
	Icon can represent a router, a router switch module (RSM), a multilayer switch feature card (MSFC), or a router switch feature card (RSFC).

ICON / VISUAL INDICATOR	DESCRIPTION
	<p>Icon represents a switch.</p>
	<p>Icon represents an IP network.</p>
	<p>Icon represents a VLAN.</p>
	<p>Icon represents a firewall.</p>
	<p>Icon represents a redundancy group.</p>
	<p>Icon represents a network connection or a Permanent Virtual Circuit (PVC).</p>
	<p>Solid line can represent a physical connection, a logical IP connection, a logical VLAN connection, a membership, or a group relationship. A green line indicates a normal connection.</p>
	<p>Jagged line represents a network connection. A green line indicates a normal connection.</p>

ICON / VISUAL INDICATOR	DESCRIPTION
	Solid down arrow represents dependency. A green arrow indicates a normal dependency.
	Dotted down arrow represents composition. A green arrow indicates a normal composition.
Light blue background	Light blue background appears in Physical Connectivity and Group Physical Connectivity maps.
Light yellow background	Light yellow background appears in IP Connectivity and Group IP Connectivity maps.
Light green background	Light green background appears in VLAN Connectivity and Group VLAN Connectivity maps.
Beige background	Beige background appears in IP Membership, VLAN Membership, and Group Membership maps.

**Table 13:** Default Nodes, Edges, and Other Indicators for Network Topology Maps

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

In a map display, a *node* is a graphical representation of an element, and an *edge* is a graphical representation of a relationship or connection between elements.

## Network Topology Map Type Summary

Table 14 summarizes the types of maps available for each type of element.

ELEMENT	AVAILABLE MAP TYPES
Bridge Host Hub Multilayer Switch Feature Card (MSFC) Probe Router, Router Switch Module (RSM) Router Switch Feature Card (RSFC) Switch Terminal Server Node	Physical Connectivity IP Network Connectivity VLAN Connectivity
IP Network	Physical Connectivity IP Network Membership IP Network Connectivity
VLAN	Physical Connectivity VLAN Membership VLAN Connectivity
Group	Group Physical Connectivity Group IP Network Connectivity Group VLAN Connectivity Group Membership

**Table 14:** Available Network Topology Maps for Topology Elements

## Physical Connectivity Map

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

For a Physical Connectivity map, the edges display as:

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



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

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

## IP Network Connectivity Map

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

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

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

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

## IP Network Membership Map

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

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

## VLAN Connectivity Map

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

For a VLAN Connectivity map, the edges display as:

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

In a VLAN Connectivity map, a hop is a logical hop. It represents the distance between an element (router or switch) and the VLAN.

If a switch appears in a VLAN Connectivity map and no edge connects the switch to the VLAN, the switch is not capable of recognizing the VLAN even though the switch has another port that participates in the VLAN.

## VLAN Membership Map

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

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

## Group Maps

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

Four types of group maps exist:

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

## Examples of Maps

Figure 2 illustrates a Physical Connectivity map and Figure 3 illustrates a Group IP Network Connectivity map.

### Physical Connectivity Map Example

To display a Physical Connectivity map, perform these steps:

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

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

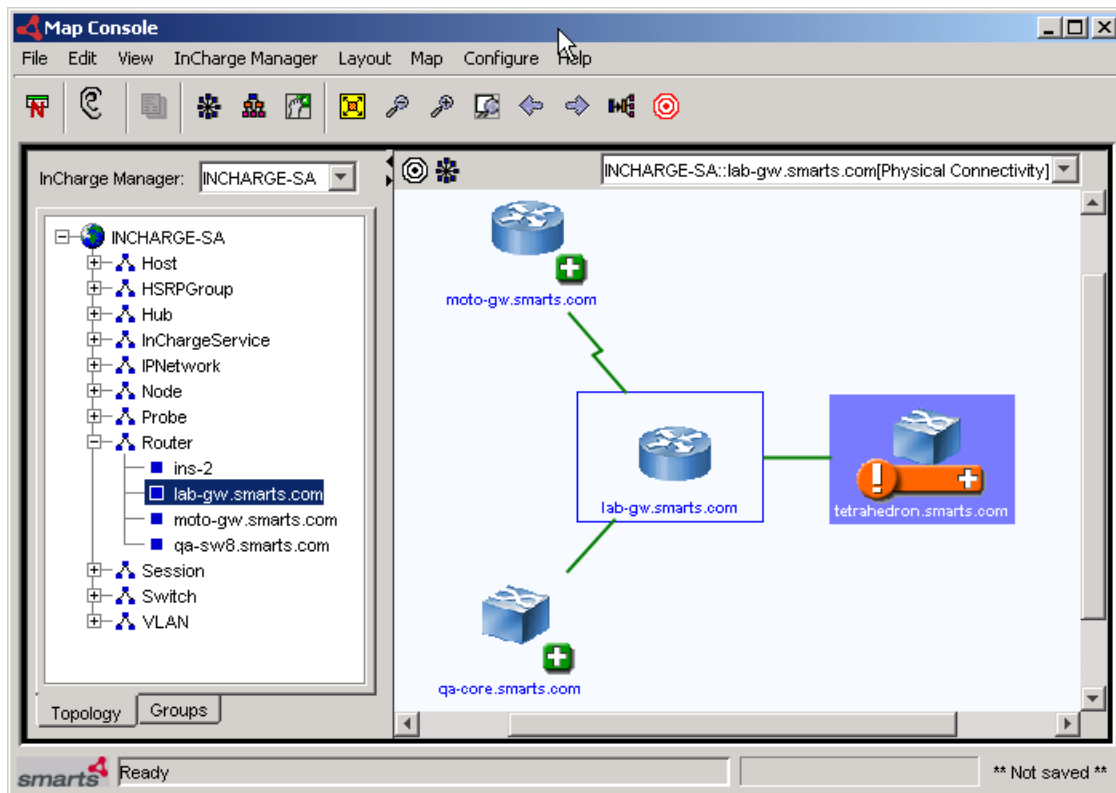


Figure 2: Physical Connectivity Map

### Group IPNetwork Connectivity Map Example

To display a Group IPNetwork Connectivity map, perform these steps:

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

Figure 3 shows a Group IPNetwork Connectivity map for a subgroup named Routing Infrastructure in the Southeast Asia group.

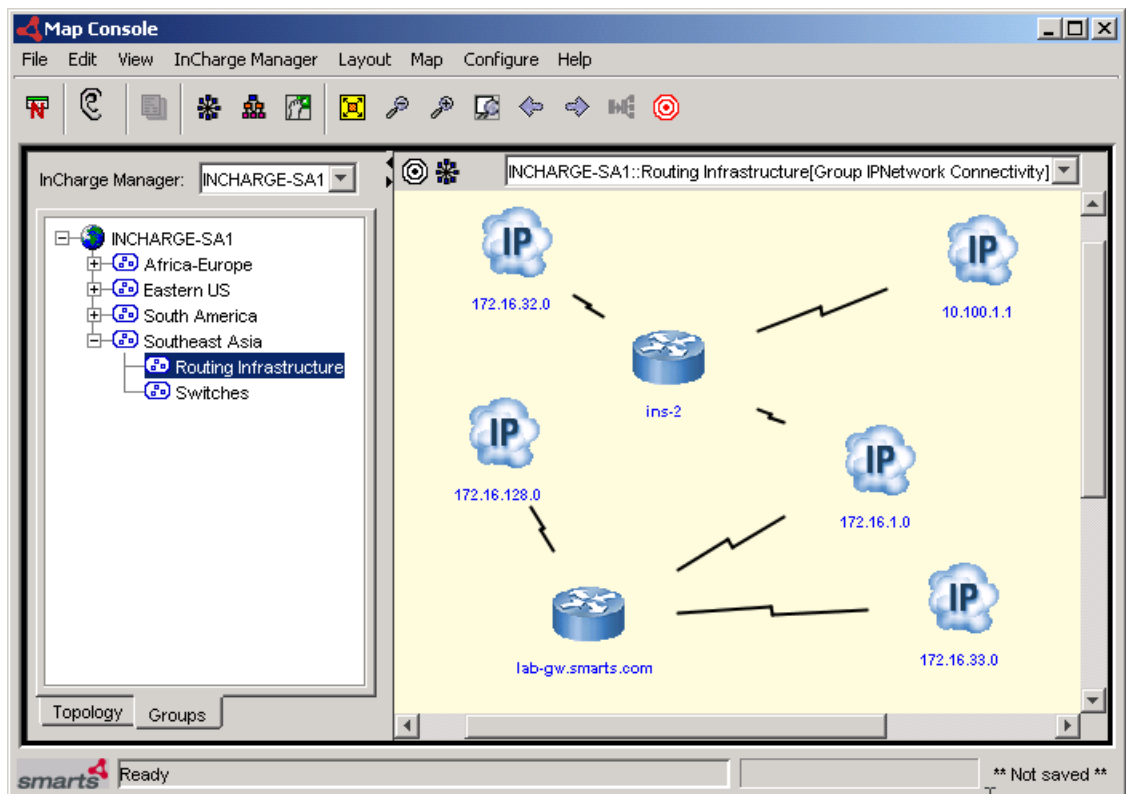


Figure 3: Group IP Network Connectivity Map

# 5

## Groups and Settings

Availability Manager monitors the network by sending Internet Control Message Protocol (ICMP) polls and Simple Network Management Protocol (SNMP) polls. The results of this polling are then compared to threshold values that define acceptable and unacceptable levels of connectivity. The thresholds, in conjunction with traps, are used to diagnose the failed elements that interrupt network connectivity.

Availability Manager uses *settings* to assign polling and threshold parameters to *groups* of managed elements. A *setting* is a collection of parameters common to a particular type of analysis (for example, environment polling). A *group*, which may be a polling group or a threshold group, contains zero or more settings and is related to the managed elements based on matching criteria (for example, element type SWITCH). The parameters defined for the settings of the polling and threshold groups define the management policies for Availability Manager.

Each member of a group meets the defined matching criteria for the group and is polled and evaluated based on the parameters defined in the group's settings. In this way, different polling and threshold values can be applied to different groups of systems, ports, and interfaces.

This chapter describes the default groups and settings provided with Availability Manager and provides instructions for modifying the properties of a group and the parameters of a setting.

## Default Polling Groups and Settings

This section lists the default polling groups, their matching criteria, and their associated settings. It also describes the threshold and parameters for each setting and their default values.

### Polling Groups

Availability Manager provides four default polling groups:

- Switches
- Routers
- Hubs and Bridges
- Other Systems

Table 15 lists all of the default polling groups and their settings.

POLLING GROUPS	MATCHING CRITERIA	DEFAULT SETTINGS
Switches	Type = SWITCH	Connectivity Polling
Routers	Type = ROUTER	Connectivity Polling
Hubs and Bridges	Type = HUB or BRIDGE	Connectivity Polling
Other Systems	None	Connectivity Polling

**Table 15:** Default Polling Groups and Settings

The Other Systems polling group does not contain any matching criteria and has the lowest priority. Devices that do not match the criteria for the other polling groups become members of the Other Systems polling group.

### Polling Settings

The following settings are accessible via the Polling tab of the Polling and Thresholds Console:

- Connectivity Polling
- Connectivity Polling - External Poller

### Connectivity Polling

The Connectivity Polling setting configures connectivity monitoring of a system. System connectivity is monitored using a combination of ICMP (Ping) requests for IP status and SNMP requests for interface, port, and card status. For more information about how Availability Manager uses ICMP and SNMP requests, refer to the *InCharge IP Discovery Guide*.

Table 16 lists the Connectivity Polling parameters.

PARAMETER	DEFAULT VALUE	DESCRIPTION
Analysis Mode	ENABLED	Enables or disables connectivity polling
Polling Interval	240 seconds	Time between successive connectivity polls.
Retries	3	Number of retry connectivity polls to perform when the initial poll fails.
Timeout	700 milliseconds	Amount of time allowed for the first poll request before it times out. Successive retries use longer times.

**Table 16:** Default Values for Connectivity Polling Setting

### Connectivity Polling - External Poller

The Connectivity Polling - External Poller setting configures connectivity analysis to use instrumentation data collected by a poller other than the one included with Availability Manager.

---

**Note:** This setting is not assigned to any default group and would only be used in place of the Connectivity Polling setting. Also, you must create an event adapter (using the Adapter Scripting Language (ASL) provided with the InCharge Software Development Kit) to communicate with your external poller and update the instrumentation data in the Domain Manager’s repository.

---

Table 17 lists the Connectivity Polling - External Poller parameters.

PARAMETER	DEFAULT VALUE	DESCRIPTION
Analysis Mode	DISABLED	Enables or disables the connectivity analysis of data collected by an external poller.
Initial Status	UNKNOWN	Determines the desired initial state for the instrumentation data. Initial status value can be UP or UNKNOWN.
Instrument Cards	FALSE	Determines if placeholders should be created for card data. If TRUE, it creates placeholders (stored instrumentation objects) for card data. If FALSE, it does not create placeholders for card data.
Instrument IP	TRUE	Determines if placeholders should be created for IP data. If TRUE, it creates placeholders (stored instrumentation objects) for IP data. If FALSE, it does not create placeholders for IP data.
Instrument Network Adapters	TRUE	Determines if placeholders should be created for interface and port data. If TRUE, it creates placeholders (stored instrumentation objects) for interface and port data. If FALSE, it does not create placeholders for interface and port data.
Instrument SNMP Agents	TRUE	Determines if placeholders should be created for SNMP agent data. If TRUE, it creates placeholders (stored instrumentation objects) for SNMP agent data. If FALSE, it does not create placeholders for SNMP agent data.

**Table 17:** Default Values for Connectivity Polling - External Poller Setting

## Default Threshold Groups and Settings

This section lists the default threshold groups, their matching criteria, and their associated settings. It also describes the threshold and parameters for each setting and their default values.

### Threshold Groups

Availability Manager provides four default threshold groups, each of which of divided into subgroups.

- Interface Groups
- Port Groups - Access Ports



- Port Groups - Trunk Ports
- System Resource Groups

**Interface Groups**

Thresholds for the interface groups configure parameters for interface analysis. Thresholds are determined by the interface’s media type (e.g., Ethernet, ATM) and its role (primary, backup, or dial-on-demand).

Table 18 lists the default interface groups and their settings.

INTERFACE GROUPS	MATCHING CRITERIA	SETTINGS
1 Gb Ethernet	Max Speed = 1,000,000,000 Type = ETHER or CSMACD	None
10/100 Mb Ethernet	Type = ETHER or CSMACD	None
ATM	Type = ATM	Interface/Port Flapping
Token Ring	Type = TOKEN	None
ISDN Physical Interface	InterfaceCode = ISDNPHYSICAL	Interface/Port Flapping
ISDN B Channel	InterfaceCode = ISDNBCHANNEL	Backup Interface Support
ISDN D Channel	InterfaceCode = ISDNDCHANNEL	Interface/Port Flapping
Serial	Type = Serial or FrameRelay	Interface/Port Flapping
FDDI	Type = FDDI	None
Backup	Type = ISDN	Backup Interface Support
Dial-On-Demand	Type = PPP or SLIP	Dial-On-Demand Interface Support
Other Interfaces	None	Interface/Port Flapping

**Table 18: Default Interface Groups and Settings**

The Other Interfaces threshold group does not contain any matching criteria and has the lowest priority. Interfaces that do not match the criteria for the other interface threshold groups become members of the Other Interfaces group.

**Port Groups - Access Ports and Trunk Ports**

Threshold groups for ports configure parameters for port analysis. Thresholds are determined by the port’s media type (e.g., Ethernet, ATM) and its role (access or trunk).

An access port is a switch port that is connected to a host. Access ports are unmanaged by default and are not associated with the access ports groups. An access port automatically becomes managed if the host that it is connected to is managed or if the port is explicitly managed. A trunk port is a switch port that is connected to a switch, router, hub, or bridge.

Table 19 shows the default access and trunk port groups and their matching criteria. By default, no settings are applied to the port threshold groups.

ACCESS AND TRUNK PORTS GROUPS	MATCHING CRITERIA	SETTINGS
1 Gb Ethernet	Max Speed = 1,000,000,000 Type = ETHER or CSMACD	None
10/100 Mb Ethernet	Type = ETHER or CSMACD	None
ATM	Type = ATM	None
Other Ports	None	None

**Table 19:** Default Access and Trunk Port Threshold Groups

The Other Ports group does not contain any matching criteria and has the lowest priority. Access ports that do not match the criteria for the other access ports groups become members of the Other Ports group.

### System Resource Groups

System resource thresholds configure parameters for device analysis. The sensitivity of the device thresholds is determined by the role of the device.

Table 20 shows the default system resource groups, their matching criteria, and respective settings.

SYSTEM RESOURCE GROUPS	MATCHING CRITERIA	SETTINGS
Switches	Type = SWITCH	Connectivity
Routers	Type = ROUTER	Connectivity
Hubs and Bridges	Type = HUB or BRIDGE	Connectivity
Other Systems	None	Connectivity

**Table 20:** Default System Resource Groups

The Other Systems Polling Group does not contain any matching criteria and has the lowest priority. Devices that do not match the criteria for the other system resource groups become members of the Other Systems threshold group.

## Threshold Settings

The following settings are accessible via the Thresholds tab of the Polling and Thresholds Console:

- Backup Interface Support (by default, contained in the Interface Group - ISDN B Channel and Interface Group - Backup)
- Connectivity (by default, contained in all System Resource Groups)
- Dial-on-Demand Interface Support (by default, contained in the Interface Group - Dial-on-Demand)
- Interface Management Policy (by default, not contained in any group but available for all System Resource Groups)
- Interface/Port Flapping (by default, contained in Interface Groups for ATM, ISDN Physical Interfaces, ISDN D Channel, Serial, and Other Interfaces)

### Backup Interface Support

The Backup Interface Support setting configures analysis for interfaces used as backup. When an interface is identified as a backup, the connectivity failure diagnosis is modified for it as follows:

- The *Down* notification is not generated if the interface is down.
- The *Backup Activated* notification is generated if the interface comes up.
- The *Exceeded Maximum Uptime* notification is generated if the interface stays up too long.

Table 21 lists the Backup Interface Support setting parameters.

PARAMETER	DEFAULT VALUE	DESCRIPTION
Maximum Uptime	0	Maximum length of time, in seconds, that the interface may be up before the Exceeded Maximum Uptime notification is generated. If the value of this parameter is 0, the Exceeded Maximum Uptime event is disabled.

**Table 21:** Default Value for Backup Interface Support Parameters

### Connectivity

The Connectivity setting configures connectivity threshold parameters for network adapters (ports and interfaces). It also controls:

- The analysis of systems that repeatedly restart, and are thus considered unstable. For more information about how Availability Manager concludes that a system is unstable, refer to [Diagnosis of Unstable Elements](#) on page 31.
- The use of bridging connectivity for root-cause analysis.

Table 22 lists the Connectivity threshold setting parameters.

PARAMETER	DEFAULT VALUE	DESCRIPTION
Correlation Use Bridging Mode	ENABLED	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 ENABLE by default because, under normal conditions, most physical connectivity is discovered and there is sparse bridging connectivity. However, you can set the parameter to DISABLE in cases where there is sparse physical connectivity and heavily meshed bridging connectivity.
Number Of Bridged Via Threshold	20	Determines whether a BridgedVia relationship is used in correlation. If a MAC endpoint is BridgedVia less than the number of Ports specified by this threshold, the BridgedVia relationship is used for correlation.
Number Of Bridges Threshold	20	Determines whether a Bridges relationship is used in correlation. If a Port Bridges less than the number of MAC endpoints specified by this threshold, the Bridges relationship is used for correlation.
Restart Trap Threshold	3	Sets the number of SNMP cold or warm start traps that must be received within the amount of time set by the Restart Trap Window parameter in order for Availability Manager to consider a system unstable. A value of 0 turns off restart analysis.

Restart Trap Window	900 seconds (15 minutes)	Sets the window of time used to monitor a system's repeated restarts. If the number of start traps meets or exceeds the Restart Trap Threshold during this window of time, the system is considered to be unstable.
Testing Notification Mode	ENABLE	Enables or disables generation of the <i>Down</i> notification for a port or interface. ENABLE activates the diagnosis of a port or interface that is in testing status. DISABLE suppresses the diagnosis of a port or interface that is in testing status.

**Table 22:** Default Values for Connectivity Threshold Group Parameters

### Dial-On-Demand Interface Support

The Dial-on-Demand Interface Support setting configures the analysis for interfaces 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 *Exceeded Maximum Uptime* notification is generated if the interface stays up too long.

Table 23 lists the Dial-On-Demand Interface Support setting parameters.

PARAMETER	DEFAULT VALUE	DESCRIPTION
Maximum Uptime	7200 seconds (2 hours)	Sets the maximum length of time that the interface may be up before the Exceeded Maximum Uptime notification is generated. If the value of this parameter is 0, the Exceeded Maximum Uptime event is disabled.

**Table 23:** Default Values for Dial-On-Demand Interface Support Parameters

### Interface/Port Flapping (Unstable)

The Interface/Port Flapping setting controls the analysis of network adapters (ports and interfaces) that are continually going up and down. Unstable analysis monitors SNMP link down traps to identify a flapping network adapter and then generates a notification to report that it is unstable. For more information about how Availability Manager concludes that a network adapter is unstable, refer to [Diagnosis of Unstable Elements](#) on page 31.

Table 24 lists the Interface/Port Flapping setting parameters.

PARAMETER	DEFAULT VALUE	DESCRIPTION
Link Trap Threshold	3	Sets the number of SNMP link down traps that must be received within the Link Trap Window in order for Availability Manager to consider the interface or port flapping. A value of 0 turns off flapping analysis.
Link Trap Window	300 seconds (5 minutes)	Sets the window of time used to monitor flapping analysis of a port or interface. If the number of link down traps meets or exceeds the Link Trap Threshold during this window of time, the interface or port is considered to be flapping.

**Table 24:** Default Values for Interface/Port Flapping Parameters

## Unmanaging Interfaces With the Interface Management Policy

The Interface Management Policy is a system-level setting for controlling the managed state of interfaces. This setting is available as a Systems Resource Groups Threshold policy. By default, this policy is not active.

If you do not use this setting, *all* discovered network elements, including interfaces, are automatically managed. (One possible exception is access ports. An access port is only managed when the system to which it is connected is managed.) Interfaces exist on hosts, routers, and layer 3 switches.

---

**WARNING:** If you are using one of the InCharge IP adapters described in the *InCharge IP Adapters User's Guide*, you must allow the third-party source to control the managed status of network elements. When the adapter's topology reader synchronizes the topology of InCharge with the topology of the third-party source, the topology reader must be able to overwrite the managed status of elements in the InCharge topology.

---

You should apply the Interface Management Policy setting to a group (and set the Default Management Status parameter to UNMANAGED) if you *do not want* to manage the interfaces that are part of the system or systems that are members of the group.

Table 25 lists the Interface Management Policy parameters.

PARAMETER	DEFAULT VALUE	DESCRIPTION
Default Management Status	MANAGED	Indicates the default management status of interfaces on systems that this setting applies to. The value can be MANAGED or UNMANAGED

**Table 25:** Values for Interface Management Support

---

**Note:** If you set an interface management policy, the policy can be overridden for a particular interface using the manage/unmanage commands available through the Domain Manager Administration Console. For more information about managing and unmanaging specific elements in the topology, refer to the *InCharge IP Discovery Guide*.

---

## Ensuring Appropriate VLAN Assignments With the VLAN Tagging Policy

When VLANs are configured on systems, the VLAN memberships are automatically discovered using the VLAN probe. VLAN membership assignments may be inaccurate based on the following:

- Duplication of VLAN names by different data centers: In this situation, InCharge combines these identically named but locally distinct VLANs into a single VLAN.
- VLAN names that automatically include the name of the device manufacturer: devices from different manufacturers always appear in different VLANs.

Use the VLAN Tagging Policy settings to ensure that systems are assigned to their appropriate VLAN. Currently, only devices from Cisco, Extreme, Foundry, and Lucent are supported.

Table 26 lists the VLAN Tagging Policy parameter.

PARAMETER	DEFAULT VALUE	DESCRIPTION
Tag		Determines tag for VLANs configured on the systems that belong to the group. If the tag is specified, the VLANs will be named as VLAN-<Tag>-<VLANNumber>, for example, VLAN-Marketing-100. Discovery is required for any change to take effect.

**Table 26:** Values for VLAN Tagging Support

## Opening the Polling and Thresholds Console

The Polling and Thresholds Console is used to display groups and modify their properties. To access the Polling and Threshold Console, you must first open the Domain Manager Administration Console.

Attaching to a Domain Manager with either the Domain Manager Administration Console or the Polling and Thresholds Console requires an InCharge user account with the following privileges and permissions:

- All privileges, specified in the *serverConnect.conf* file (or its equivalent) read by the Domain Manager.
- Permission to use the console operation *Configure Domain Manager Admin Console*. Through the Global Manager Administration Console, this permission is specified in the Console Operations section of the user profile.

For information about configuring access privileges, see the *InCharge System Administration Guide*. For information about configuring permissions to perform specific console operations, see the *InCharge Service Assurance Manager Configuration Guide*.

To open the Polling and Thresholds Console, follow these steps:

- 1** Attach to the Domain Manager with the Global Console. The Topology Browser Console opens.
- 2** In the Topology Browser Console, select *Configure > Domain Manager Administration Console*. The Domain Manager Administration Console opens.
- 3** In the Domain Manager Administration Console, select *Edit > Polling and Thresholds*. The Polling and Thresholds Console opens.



## Layout of the Polling and Thresholds Console

The Polling and Thresholds Console is divided into two panels.

- The left panel displays the icon for the analysis domain in the upper-left corner and provides two tabs, Polling and Thresholds, at the bottom. When the Polling tab is selected, the console displays polling groups. Likewise, when the Thresholds tab is selected, the console displays threshold groups.

For each group, there are settings that provide adjustable parameters and a membership list of managed elements to which the settings are applied.

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

Figure 4 provides an example of a Polling and Thresholds Console.

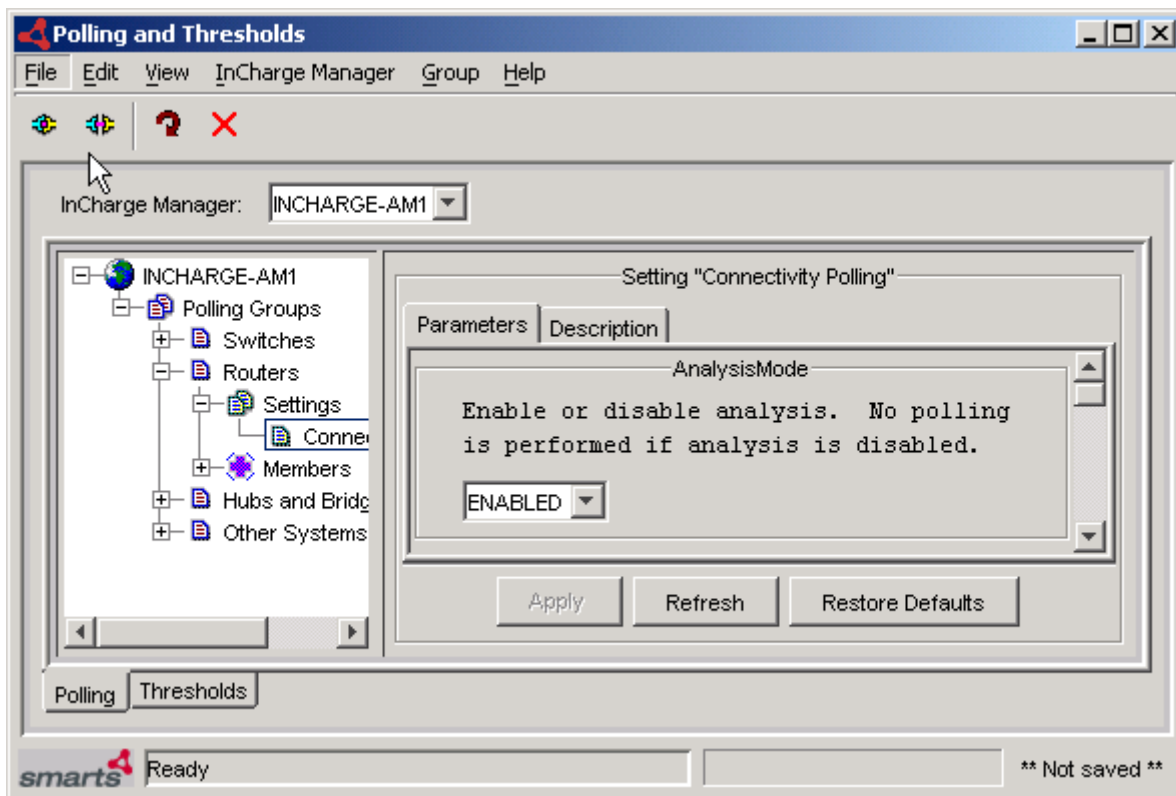






Figure 4: Polling and Thresholds Console

## Polling and Thresholds Console Toolbar Buttons

The toolbar of the Polling and Thresholds Console provides quick access to the commands described in Table 27.

BUTTON	DESCRIPTION
	Attach to a Domain Manager
	Detach from a Domain Manager
	Reconfigure polling and thresholds groups
	Delete selected item

**Table 27:** Polling and Thresholds Console Toolbar Buttons

## Working With Groups and Settings

This section describes how to configure an InCharge application using the Polling and Thresholds Console. The configuration of an InCharge application applies polling and threshold parameters to defined sets of managed elements.

- A group is composed of settings and members. There are two distinct types of groups: Polling Groups and Threshold Groups.
- A setting is composed of one or more related parameters. For example, parameters related to port or interface utilization analysis may be organized into a setting.
- A member is an element of the managed topology that belongs to a group. A managed element can be a member of one Polling group and one Threshold group.

Using the Polling and Thresholds Console, you can perform the following configuration tasks:

- Modify the properties of existing Polling and Threshold groups.
  - Determine what settings are applied to a group.

- Modify the parameters of a setting.
- Create new Polling and Threshold groups.

## How Managed Elements Are Assigned to Groups

When InCharge performs discovery, it automatically assigns each managed element to a group based on the group's matching criteria and priority. Matching criteria are defined using the attributes of the managed element. The following components define a group:

- Name
- Settings associated with the group
- Matching criteria defined for the group
- Priority, which determines membership when a device meets the matching criteria for more than one group

A managed element can be a member of one Polling group and one Threshold group.

## Modifying the Properties of a Group

Although there are two distinct types of groups, Polling and Thresholds, both types of groups are configured similarly. A group is composed of settings and members. A setting includes one or more polling or threshold parameters. The matching criteria specified for the group and the group's priority determine which managed elements are members of the group.

When a group is selected in the left panel of the Polling and Thresholds Console, four tabs are displayed.

- Settings
- Priorities
- Matching Criteria
- Description

Modifying the properties under each of these tabs changes the configuration of the group. When you finish editing the properties of a group, click the **Apply** button to save the changes and then select **Reconfigure** from the Group menu to make the configuration changes take effect.

### Method for Adding or Removing Settings

A group's settings determine what polling parameters or threshold parameters are applied to the managed elements that are members of the group.

The Settings tab is divided into two sections: Current Settings and Available Settings. The Current Settings section lists the settings that are applied to the group. The Available Settings section lists additional available settings.

#### **Adding or Removing a Setting**

- 1** Select a setting from the Current Settings list or from the Available Settings list.
- 2** Click **Add** to move an available setting to the Current Settings list or click **Remove** to move a current setting to the Available Settings list.
- 3** Click **Apply**.
- 4** Select **Reconfigure** from the Group menu.

### Method for Modifying the Priority of Groups

Priority and Matching Criteria parameters determine which managed elements are members of what group. When an element matches the criteria for two or more groups, the managed element becomes a member of the group with the highest priority.

The Priority tab lists groups in the order of their priority, from highest to lowest.

#### **Changing the Priority of a Group**

- 1** Select the group for which you want to change the priority.
- 2** Click the up or down arrow to change its position relative to the other groups.
- 3** Click **Apply**.
- 4** Select **Reconfigure** from the Group menu.

## Method for Editing Matching Criteria

Matching criteria and priority determine which managed elements are members of what group. Matching criteria consist of one or more wildcard patterns that are compared against the values of one or more attributes. If the value of the attribute matches the wildcard pattern, the managed element is eligible to become a member of that group. When more than one matching criterion is specified, a managed element must match all criteria to become a member of the group.

For example, if a matching criterion uses the attribute `SystemName` with a value of `172.16.*`, all members of the group must contain the string `172.16` in their `SystemName` attribute. If another matching criterion that uses the attribute `CreationClassName` with a value of `Host` is added, all members of the group must be hosts with the string `172.16` in their `SystemName`.

Active matching criteria, which appear in the top of the Matching Criteria tab, have three fields: Name, Description, and Value.

- Name identifies the attribute that is used as a matching criterion. The attributes of managed elements can be viewed in the Global Console.
- Description is the description of the attribute taken from the ICIM model.
- Value is the string that is matched against the value of the attribute in the managed element. The value field can contain any combination of text, integers, and wildcards.

---

**Note:** The Value field for a matching criterion is case-sensitive.

---

### Adding or Removing Matching Criteria

- 1 Select a matching criterion.
- 2 Click **Enable** to make the criterion active, moving it to the top of the Matching Criteria tab.  
  
Use **Disable** to deactivate the criterion, moving it to the bottom of the Matching Criteria tab.
- 3 If you are adding a matching criterion, type a matching pattern in the Value field.
- 4 Click **Apply**.
- 5 Select **Reconfigure** from the Group menu.

### Changing the Value of a Matching Criterion

- 1 Select the string in the Value field or double-click the Value field to highlight the current value.
- 2 Type the text, integers, or wildcard to match against the attribute.
- 3 Click **Apply**.
- 4 Select **Reconfigure** from the Group menu.

InCharge processes matching criteria in the following manner. First, managed elements are compared against the matching criteria of the group with the highest priority. If an element matches all the criteria, it is added as a member of the group. If an element does not match all the criteria, it is compared against the matching criteria of the group with the second highest priority, and so on.

---

**Note:** When no matching criteria are active (or appear in the top of the Matching Criteria dialog box), the group matches all managed elements. Priority determines whether the group contains members.

---

## Method for Modifying the Parameters of a Setting

The parameters of a setting, whether they define a polling parameter or set a threshold, are adjusted in a similar manner. A setting can contain a drop-down menu from which you choose a value, or a slider and a Value field where you can provide a value within a discrete range.

### Changing the Parameters of a Setting

- 1 Select the setting in the left panel of the Polling and Thresholds Console. The parameters of a setting are listed in the right panel of the console.
- 2 Change the value of a parameter using one of the following methods:  
For a drop-down menu, click the menu and select a value.  
For a threshold, you can:
  - Type a new number into the Value field and press **Enter**.
  - Select the slider and drag it with the mouse or select the slider and use the arrow keys to incrementally change the value.
- 3 Click **Apply** to save the changes.
- 4 Select **Reconfigure** from the Group menu.

### Restoring the Default Values of a Setting

The **Restore Defaults** button, which is visible when a setting is selected in the left panel of the Polling and Thresholds Console, restores the default values of all the parameters for the selected setting.

- 1 Select the setting.
- 2 Click **Restore Defaults**.
- 3 Select **Reconfigure** from the Group menu.

## Creating New Polling and Threshold Groups

Creating a new group enables you to customize the polling or threshold settings for a group of managed elements. After you create a new group, use procedures previously described to adjust the settings and thresholds of the new group.

You can use two methods to create a new group:

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

The resulting group, regardless of the method you use to create it, is assigned the lowest priority.

For information regarding settings, see [Method for Modifying the Parameters of a Setting](#) on page 62, and for information regarding groups, see [Modifying the Properties of a Group](#) on page 59.

### Copying an Existing Group

- 1 Right-click the Polling or Threshold group that you want to copy.
- 2 Select **Copy** from the pop-up menu to display the Copy Group dialog.
- 3 In the dialog, type a name and an optional description for the new group and click **OK**. The new group contains the same settings and thresholds as the group you copied.
- 4 Edit the settings, matching criteria, and priority of the new group. Change the value of any thresholds or parameters as necessary.
- 5 Select **Reconfigure** from the Group menu.

### Creating an Empty Group

- 1** In the left panel of the Polling and Threshold Console, right-click the group type for which you want to create a new group. (When an InCharge application provides more than one default group, you may be able to create more than one type of group.)
- 2** Select **New Group** from the pop-up menu to display the New Group dialog.
- 3** In the dialog, type a name and an optional description for the new group and click **OK**.
- 4** Add settings and matching criteria, and set the priority of the new group. Change the values of any thresholds or parameters as necessary.
- 5** Select **Reconfigure** from the Group menu.





# MIBs Polled and SNMP Traps Processed

This appendix lists the MIBs polled and the SNMP traps processed by InCharge IP Availability Manager. Availability Manager supports SNMP V1, SNMP V2C, and SNMP V3 for MIBs and traps. Availability Manager considers all received SNMP V3 traps as genuine and therefore does not authenticate V3 traps.

## Standard SNMP MIBs

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

## Enterprise MIBs

The following is a list of vendor-specific MIBs that Availability Manager polls:

- AI194HUB-MIB
- AI198CLC-MIB
- ARROWPOINT-CHASSISMGREXT-MIB
- ATM-FORUM-TC-MIB
- CENTILLION-BRIDGE-MIB
- CENTILLION-IF-EXTENSIONS-MIB
- CENTILLION-FDB-MIB
- CISCO-2900XL-MIB
- CISCO-CPU-MIB
- CISCO-CDP-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-FRAME-RELAY-MIB
- CISCO-FRU-CONTROL-MIB
- CISCO-HSRP-MIB
- CISCO-PAGP-MIB
- CISCO-PROCESS-MIB
- CISCO-RF-MIB
- CISCO-RHINO-MIB
- CISCO-STACK-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-SYSTEM-MIB
- CNT21-MIB
- CNT241-MIB
- COSINE-ORION-MIB
- CT-CONTAINER-MIB

- CTRON-CHASSIS-MIB
- EXTREME-EDP-MIB
- EXTREME-FDB-MIB
- EXTREME-SYSTEM-MIB
- EXTREME-VLAN-MIB
- Fore-Common-MIB
- Fore-Switch-MIB
- FOUNDRY-SN-AGENT-MIB
- FOUNDRY-SN-SWITCH-GROUP-MIB
- GDCSCM-MIB
- GENERIC-3COM-TRUNK-MIB (A3Com)
- JUNIPER-MIB
- LANPLEX-SYSTEM-MIB-1-1-1
- RAPID CITY
- REPEATER-REV4-MIB (Cabletron)
- SSG-5000-CHASSIS-MIB (Shasta)
- STRATACOM-MIB
- SW-MIB (BCSI)
- SYNOPTICS-LS-ETHERNET-MIB
- UNISPHERE-DATA-ERX-SYSTEM-MIB
- Wellfleet-CCT-NAME-MIB
- Wellfleet-HARDWARE-MIB
- Wellfleet-IP-MIB
- XYLAN-BASE-MIB

## SNMP Traps

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

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

Table 28 lists the SNMP traps that are processed by Availability Manager.

MIB	TRAPS
Standard SNMP (RFC 1215 MIB)	<ul style="list-style-type: none"><li>• Cold Start</li><li>• Warm Start</li><li>• Link Up</li><li>• Link Down</li></ul>
GENERIC-3COM-TRUNK-MIB	<ul style="list-style-type: none"><li>• Module Inserted</li></ul>
AI198CLC-MIB	<ul style="list-style-type: none"><li>• (card) Down Trap</li><li>• (card) Up Trap</li></ul>
CISCO-HSRP-MIB	<ul style="list-style-type: none"><li>• cHsrpStateChange</li></ul>
CISCO-ISDN-MIB	<ul style="list-style-type: none"><li>• demandNbrLayer2Change</li></ul>
CISCO-STACK-MIB	<ul style="list-style-type: none"><li>• Module Up</li><li>• Module Down</li></ul>

**Table 28:** SNMP Traps Processed by Availability Manager

# B

## Subscribing to Notifications

This appendix lists the default set of events subscribed to by InCharge IP Availability Manager, and the class from which they originate, as well as the complete list of the failures, exceptions, and symptomatic events that can be reported by Availability Manager.

Table 29 lists the default set of events subscribed to and reported by Availability Manager. The default subscription includes all root-cause events diagnosed by Availability Manager.

ELEMENT	EVENT	CLASS OF ORIGIN
System	Down (r)	ICIM_UnitaryComputerSystem
	Unstable (r)	
	Unresponsive (s)	
	Discovery Error (s)	
Network Adapter	Down (r)	ICIM_NetworkAdapter
	Unstable (r)	
	Disabled (r)	
	Logical Connection Down (r)	
	Backup Activated (s)	NetworkAdapter_Fault
	Exceeded Maximum Uptime (s)	
Connection	Down (r)	ICIM_NetworkDeviceConnection
	Unstable (r)	

ELEMENT	EVENT	CLASS OF ORIGIN
Chassis	Down (r)	Chassis
Card	Down (r)	Card
	Switch Over (s)	
Partition	Down (r)	Partition
SNMP Agent	Not Responding (r)	SNMPAgent
VR Agent	Not Responding (r)	VRAgent
Card Redundancy Group	All Components Down (s)	CardRedundancyGroup
	At Risk (s)	
	Reduced Redundancy (s)	
Network Adapter Redundancy Group	All Components Down (s)	NetworkAdapterRedundancyGroup
	At Risk (s)	
	Reduced Redundancy (s)	
Network Connection Redundancy Group	All Components Down (s)	NetworkConnectionRedundancyGroup
	At Risk (s)	
	Reduced Redundancy (s)	
System Redundancy Group	All Components Down (s)	SystemRedundancyGroup
	At Risk (s)	
	Reduced Redundancy (s)	
HSRP Group	Switch Over Failed (s)	HSRPGroup
	All Components Down (s)	
	At Risk (s)	
	Reduced Redundancy (s)	
HSRP Endpoint	Switch Over (s)	HSRPEndPoint
Duplicate IP	Duplicate (s)	DuplicateIP
<b>KEY</b> (r) = Root cause (s) = Symptomatic event		

**Table 29:** Default Set of Events Subscribed To by Availability Manager

Availability Manager does not, by default, subscribe to either *IP Down* or *IP Unresponsive* events. These symptomatic events are not required to diagnose any of the root-cause problems reported by Availability Manager.

Table 30 lists all of the notifications diagnosed by Availability Manager.

ELEMENT	EVENT	CLASS OF ORIGIN
System	Down	ICIM_UnitaryComputerSystem
	Unstable	
	Discovery Error	
	Might Be Down	
	Unresponsive	
	Connectivity Exception	
	Operational Exception	
Network Adapter	Down	ICIM_NetworkAdapter
	Disabled	
	Logical Connection Down	
	Unstable	NetworkAdapter_Fault
	Backup Activated	
	Exceeded Maximum Uptime	
	Administratively Down	
	Down Or Flapping	
Connections	Down	ICIM_NetworkDeviceConnection
	Unstable	
	Down Or Flapping	
VLAN	Connectivity Exception	VLAN
	Operational Exception	
Chassis	Down	Chassis
Cards	Down	Card
	Operationally Down	
	Switch Over	
Partition	Down	Partition

ELEMENT	EVENT	CLASS OF ORIGIN
SNMP Agent	Not Responding	SNMPAgent
	Unresponsive	
	Repeated Restarts	SNMPAgent_Fault
VR Agent	Not Responding	VRAgent
	Unresponsive	
	Repeated Restarts	VRAgent_Fault
Card Redundancy Group	All Components Down	CardRedundancyGroup
	At Risk	
	Reduced Redundancy	
Network Adapter Redundancy Group	All Components Down	NetworkAdapterRedundancyGroup
	At Risk	
	Reduced Redundancy	
Network Connection Redundancy Group	All Components Down	NetworkConnectionRedundancyGroup
	At Risk	
	Reduced Redundancy	
System Redundancy Group	All Components Down	SystemRedundancyGroup
	At Risk	
	Reduced Redundancy	
HSRP Group	Switch Over Failed	HSRPGroup
	All Components Down	
	At Risk	
	Reduced Redundancy	
HSRP Endpoint	Switch Over	HSRPEndPoint
IP	Down	IP
	Unresponsive	
Duplicate IP	Duplicate	DuplicateIP

**Table 30:** Notifications Generated By Availability Manager and Their Origin



# C

## Selected Attributes of Managed Elements

This chapter lists attributes of various ICIM elements used by Availability Manager to diagnose failures and distinguish between problems with similar symptoms.

### System Attributes

Attributes for system include:

- IsUnresponsive
- Certification

Table 31 lists the values of the IsUnresponsive attribute.

VALUE	DESCRIPTION
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.

**Table 31:** IsUnresponsive Attribute

Table 32 lists the values of the Certification attribute.

VALUE	DESCRIPTION
UNSUPPORTED	Deprecated
GENERIC	Indicates that the OID is not recognized. The system is classified as GENERIC and added to the Node class. Analysis is performed using MIB-II data.
TEMPLATE	Indicates that OID is recognized but that no information about the MIBs this system supports is known.
CERTIFIED	Indicates that the system has the highest level of certification and is discovered using standard MIB-II data and enterprise MIBS.
VALIDATED	Deprecated
UNDISCOVERED	Indicates the system is not discovered.

**Table 32:** Certification Attribute

## Network Adapter Attributes

Attributes for network adapters include:

- AdminStatus
- OperStatus
- IsFlapping

Table 33 lists the values of the AdminStatus attribute.

Availability Manager uses the values of the AdminStatus and OperStatus attributes to determine the state of a network adapter. When the value of AdminStatus is UP, the value of OperStatus determines the state of the network adapter. Otherwise, the value of AdminStatus determines the state of the network adapter.

VALUE	DESCRIPTION
UP	Indicates that the port or interface is administratively enabled.
DOWN	Indicates that the port or interface is administratively disabled.
TESTING	Indicates that the port or interface is in testing mode.
OTHER	Indicates that the port or interface is in an unknown state.
NOTPRESENT	AdminStatus has a value of NOTPRESENT when Availability Manager receives one of the following SNMP errors: <ul style="list-style-type: none"> <li>• SNMP_EXP_NOSUCHOBJECT</li> <li>• SNMP_ERR_NOSUCHNAME</li> <li>• SNMP_EXP_NOSUCHINSTANCE</li> <li>• SNMP_EXP_ENDOFMIB</li> </ul>
UNKNOWN	Indicates that the port or interface has not yet been polled.

**Table 33: AdminStatus Attribute**

Table 34 lists the values for the OperStatus attribute.

VALUE	DESCRIPTION
UP	Indicates that the port or interface is operationally up.
DOWN	Indicates that the port or interface is operationally down.
TESTING	Indicates that the port or interface is in testing mode.
OTHER	Indicates that the port or interface is in an unknown state.
NOTPRESENT	AdminStatus has a value of NOTPRESENT when Availability Manager receives one of the following SNMP errors: <ul style="list-style-type: none"> <li>• SNMP_EXP_NOSUCHOBJECT</li> <li>• SNMP_ERR_NOSUCHNAME</li> <li>• SNMP_EXP_NOSUCHINSTANCE</li> <li>• SNMP_EXP_ENDOFMIB</li> </ul>
UNKNOWN	Indicates that the port or interface has not yet been polled.

**Table 34: OperStatus Attribute**

Table 35 lists the values for the IsFlapping attribute.

VALUE	DESCRIPTION
TRUE	Indicates that the port or interface is flapping.
FALSE	Indicates that the port or interface is not flapping.

**Table 35: IsFlapping Attribute**

## Network Connection Attributes

Attributes for network connections include:

- IsNetworkAdapterDown
- IsNetworkAdapterFlapping

Table 36 lists the values for the IsNetworkAdapterDown attribute.

VALUE	DESCRIPTION
TRUE	Indicates that at least one connected port or interface is operationally down.
FALSE	Indicates that no connected port or interface is operationally down.

**Table 36: IsNetworkAdapterDown Attribute**

Table 37 lists the value of the IsNetworkAdapterFlapping attribute.

VALUE	DESCRIPTION
TRUE	Indicates that at least one connected port or interface is flapping.
FALSE	Indicates that no connected port or interface is flapping.

**Table 37: IsNetworkAdapterFlapping Attribute**

## Card Attributes

Attributes for cards include:

- Status
- StandbyStatus

Table 38 lists the values of the Status attribute.

VALUE	DESCRIPTION
OK	Indicates that the card is operating normally.
CRITICAL	Indicates that the card is at critical status.
MARGINAL	Indicates that the card is at marginal status.
OTHER	Indicates that the status of the card is other than the above. Can also indicate that Availability Manager received an unrecognized SNMP error.
NOTPRESENT	Status has a value of NOTPRESENT when Availability Manager receives one of the following SNMP errors: <ul style="list-style-type: none"> <li>• SNMP_EXP_NOSUCHOBJECT</li> <li>• SNMP_ERR_NOSUCHNAME</li> <li>• SNMP_EXP_NOSUCHINSTANCE</li> <li>• SNMP_EXP_ENDOFMIB</li> </ul>
UNKNOWN	Indicates that the card has not yet been polled.

**Table 38:** Status Attribute

Table 39 lists the values of the StandbyStatus attribute.

VALUE	DESCRIPTION
ACTIVE	Indicates that the card is the active card within a card redundancy group.
INACTIVE	Indicates that the card is not the active card within a card redundancy group.
ERROR_STANDBY	Indicates that the redundant card has encountered an error.
NOTAPPLICABLE	Indicates that the card does not support card redundancy.
OTHER_STANDBY	Indicates that the status of the card is other than one of the above. Can also indicate that an SNMP error was received during polling.
UNKNOWN_STANDBY	Indicates that the card has not yet been polled.

**Table 39:** StandbyStatus Attribute

## SNMP Agent Attribute

Attributes for SNMP agents include SNMPStatus. Table 40 lists the values of the SNMPStatus attribute.

VALUE	DESCRIPTION
OK	Indicates that the agent is responding to SNMP requests.
AUTHFAILURE	Indicates an authentication failure to SNMP request.
TIMEDOUT	Indicates that the agent is not responding.
UNREACHABLE	Indicates that the agent is not responding to SNMP requests but that the host system is responding to ICMP pings.
OTHER	Indicates an unspecified failure occurred.
UNKNOWN	Default value before the agent is polled.

**Table 40:** SNMPStatus Attribute

## IP Attributes

Attributes for IP protocol endpoints include IPStatus. Table 41 lists the values of the IPStatus attribute.

VALUE	DESCRIPTION
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.

VALUE	DESCRIPTION
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.

**Table 41:** IPStatus Attribute

## Redundancy Group Attributes

Attributes for redundancy groups include:

- AtRiskThreshold
- IsAnyComponentDown
- IsEveryComponentDown

Table 42 lists the value of the AtRiskThreshold attribute:

VALUE	DESCRIPTION
1	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.

**Table 42:** AtRiskThreshold Attribute

Table 43 lists the values of the IsAnyComponentDown attribute.

VALUE	DESCRIPTION
TRUE	Indicates that at least one member of the redundancy group is not operational.
FALSE	Indicates that all the members of the redundancy group are operational.

**Table 43:** IsAnyComponentDown Attribute

Table 44 lists the values of the IsEveryComponentDown attribute.

VALUE	DESCRIPTION
TRUE	Indicates that all the members of the redundancy group are not operational.
FALSE	Indicates that at least one member of the redundancy group is operational.

**Table 44:** IsEveryComponentDown Attribute

## HSRP Group Attributes

Attributes for HSRP groups include all the attributes of the redundancy group. In addition, HSRP groups include the following attributes:

- HsrpEpStateChanged
- IsAnyHSRPEndpointActive
- IsEveryHSRPEndpointReady

Table 45 lists the values of the HsrpEpStateChanged attribute.

VALUE	DESCRIPTION
TRUE	Indicates that one or more members of the redundancy group are not operational.
FALSE	Indicates that all the members of the redundancy group are operational.

**Table 45:** HsrpEpStateChanged Attribute

Table 46 lists the values of the IsAnyHSRPEndpointActive attribute.



VALUE	DESCRIPTION
TRUE	Indicates that at least one endpoint in the HSRP group is active.
FALSE	Indicates that no endpoint in the HSRP group is active.

**Table 46:** IsAnyHSRPEndpointActive Attribute

Table 47 lists the values of the IsEveryHSRPEndpointReady attribute.

VALUE	DESCRIPTION
TRUE	Indicates that all endpoints in the HSRP group responded to polls.
FALSE	Indicates that all endpoints in the HSRP group did not respond to polls.

**Table 47:** IsEveryHSRPEndpointReady Attribute

## HSRP Endpoint Attributes

Attributes for HSRP endpoints include:

- IsSwitchOverActive
- StateChange
- State

Table 48 lists the values of the IsSwitchOverActive attribute.

VALUE	DESCRIPTION
TRUE	Indicates that the endpoint has switched over to the active state.
FALSE	Indicates that the endpoint is in the standby state.

**Table 48:** IsSwitchOverActive Attribute

Table 49 lists the values of the StateChange attribute.

VALUE	DESCRIPTION
0	Indicates that the endpoint has not changed state.
Any other value	Indicates that the endpoint has changed state.

**Table 49:** IsSwitchOverActive Attribute

Attributes for HSRP endpoints include Status. Table 50 lists the values of the Status attribute.

VALUE	DESCRIPTION
ACTIVE_HSRP	Indicates that the interface is active.
ERROR_HSRP	Indicates that an error was encountered during polling.
INITIAL_HSRP	This is the starting state and indicates that HSRP is not running. This state is entered via a configuration change or when an interface first comes up
LEARN_HSRP	The router has not determined the virtual IP address, and not yet seen an authenticated Hello message from the active router. In this state the router is still waiting to hear from the active router.
LISTEN_HSRP	The router knows the virtual IP address, but is neither the active router nor the standby router. It listens for Hello messages from those routers.
SPEAK_HSRP	The 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 standby state.
UNKNOWN_HSRP	Indicates the HSRP state was not polled.

**Table 50:** HSRP Endpoint Status Attribute

# D

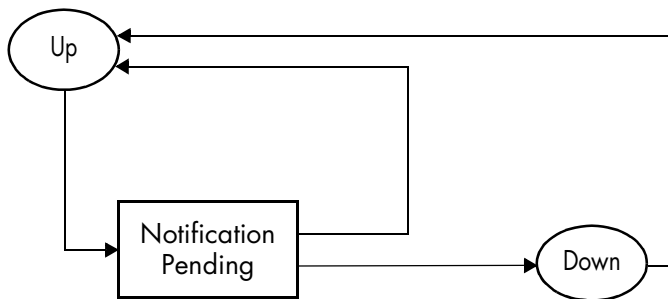
## Polling for Analysis

An InCharge IP Domain Manager uses a cooperative approach to Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) polling to obtain connectivity, fault, and performance data for its correlation analysis. The parameters for controlling ICMP and SNMP polling and for setting thresholds for polled data are accessed through the Polling and Thresholds Console.

### ICMP Poller

InCharge uses a high-performance, asynchronous ICMP poller. The ICMP poller uses two asynchronous threads; one thread sends polls, and the other receives polls. Because the send and receive threads operate separately, slow response times or excessive timeouts do not affect the polling rate. Thus, the ICMP poller performs at a consistent polling rate.

Figure 5 shows the three possible states of a monitored element as determined by its response to an ICMP poll. The states are *up*, *notification pending*, and *down*.



**Figure 5:** Possible States of an Element During an Analysis Polling Cycle

An element is in the *up* state until it fails to respond to an ICMP poll. When it fails to respond, the status of the element changes to the *notification pending* state and stays in that state until InCharge can determine whether the element is *up* or *down*.

If the element responds to an ICMP poll before the maximum failure retry count is exceeded for the element, the status of the element changes back to the *up* state.

If the maximum failure retry count is exceeded for the element, the status of the element changes to the *down* state, and InCharge does not poll the element again until the next scheduled polling cycle. An element stays in the *down* state until it responds to an ICMP poll. When the element responds, InCharge changes the status of the element to the *up* state.

This polling sequence is performed for each IP endpoint that is managed.

## SNMP Poller

InCharge uses a synchronous, multi-threaded SNMP poller. By default, the SNMP poller uses ten synchronous polling threads.

The SNMP poller fully supports the SNMP V1 and V2C protocols, and supports authentication and access control but not data encryption for the SNMP V3 protocol. With SNMP V1, the correlation model uses 32-bit counters in its correlation analysis. With SNMP V2C or V3, the correlation model uses high-capacity 64-bit counters in its correlation analysis. Using 64-bit counters is critical for performance analysis of high-speed data links because using 32-bit counters might result in wrapping (overflow) of the counters between polls.

Polling for devices with multiple IP addresses is supported because the SNMP poller supports multiple IP addresses for each SNMP agent. The SNMP poller automatically switches to an alternate IP address during failures, thereby ensuring the integrity of InCharge's correlation analysis during an outage.

## Just-In-Time Polling

The SNMP poller's MIB variable poll list is driven by a Just-In-Time polling algorithm, which ensures that only those MIB variables needed for correlation are polled. For example, if a port monitored for performance data is disabled, or goes down, the SNMP poller automatically removes the relevant MIB variables from the poll list. If the port is re-enabled, or comes back up, the variables are automatically put back onto the MIB poll list.

## Request-Consolidation Polling

Issuing a single SNMP GET request that requests 10 variables is more efficient than issuing 10 GET requests each requesting a single variable. The SNMP poller consolidates as many variables as possible into a single SNMP GET request. The consolidation is not restricted to variables from the same SNMP table. Polling consolidation continually adapts to changes in the MIB variable poll list.

Upon encountering a non-fatal error during polling consolidation, the SNMP poller responds differently to an SNMP V1 agent than to an SNMP V2C or V3 agent for the following reason: Where an SNMP V1 agent *stops* processing a request upon encountering an error, an SNMP V2C or V3 agent *continues* processing a request upon encountering an error. An SNMP V2C or V3 agent handles errors on a per OID basis.

If a non-fatal error is encountered by an SNMP V1 agent during a GET request seeking multiple variables, the SNMP poller suspends the polling of the affected variable because continuing to poll that variable would require the resending of the remainder of the request after receiving the error, which would probably impact the performance of the SNMP V1 agent; the SNMP poller continues to poll the unaffected variables. (An example of an affected variable is one that has become unavailable due to a configuration change.) This behavior enables the SNMP poller to operate efficiently with an SNMP V1 agent during unexpected changes to a device's configuration.

In contrast, if a non-fatal error is encountered by an SNMP V2C or V3 agent during a GET request seeking multiple variables, the SNMP poller continues the polling of the affected variable as well as the unaffected variables.

## ICMP and SNMP Polling Coordination

InCharge links its ICMP and SNMP pollers so that the SNMP poller does not send requests to any SNMP agent address that the ICMP poller determines to be unreachable. IP addresses that are unresponsive to ICMP polls are added to a *do not poll* list, which the SNMP poller checks before sending SNMP requests.

If an SNMP agent address is on the *do not poll* list, the SNMP poller does not send a request to that address. If an SNMP agent has multiple IP addresses, the SNMP poller checks for each address in the *do not poll* list. For an address that does *not* appear in the list, the SNMP poller sends a request to that address. If all addresses for an agent are on the list, the SNMP poller deems the agent as unreachable and temporarily suspends sending SNMP requests to that agent. As soon as an agent's IP address becomes responsive, as determined by the ICMP poller, the address is removed from the list, and SNMP polling resumes.

# Index

## Numerics

- 1 Gb Ethernet access ports threshold group 50
- 1 Gb Ethernet interface threshold group 49
- 1 Gb Ethernet trunk ports threshold group 50
- 10/100 Mb Ethernet access ports threshold group 50
- 10/100 Mb Ethernet interface threshold group 49
- 10/100 Mb Ethernet trunk ports threshold group 50

## A

- Access
  - Port 50
  - Port group 49
- Adding or removing a setting 60
- Adding or removing matching criteria 61
- AdminStatus attribute 15, 28, 74
- Aggregate event 2
- All components down 24
- Analysis mode
  - Connectivity polling 47
  - Connectivity polling - external poller 48
- At risk 24
- ATM access ports threshold group 50
- ATM interface group 49
- ATM trunk ports threshold group 50
- AtRiskThreshold 24, 79
- Attribute
  - AdminStatus 15, 28, 74
  - AtRiskThreshold 24, 79
  - Certification 74
  - DiscoveryErrorInfo 10
  - HsrpEpStateChanged 80
  - IPStatus 28, 78
  - IsAnyComponentDown 80
  - IsAnyHSRPEndpointActive 80
  - IsEveryComponentDown 80
  - IsEveryHSRPEndpointReady 81
  - IsFlapping 4, 13, 15, 76
  - IsNetworkAdapterDown 76
  - IsNetworkAdapterFlapping 4, 17, 76
  - IsSwitchOverActive 81
  - IsUnresponsive 73
  - List of 73
  - OperStatus 28, 75

- SNMPStatus 78
- StandbyStatus 77
- Status 77, 82

## B

- Backup interface support setting 51
  - Maximum uptime 51
  - Unstable notification 33
- Backup interface threshold group 49
- BASEDIR xi
- Bridge 7

## C

- Cable 16
- Card 19
  - Down 4, 19
    - Symptoms of 19
  - Operationally down 6, 20
  - Redundancy group 23
  - Switch over 6, 20
- Certification attribute 74
- Changing matching criteria 62
- Changing priority of a group 60
- Changing setting parameters 62
- Chassis 19
  - Down 4, 19
    - Symptoms of 19
- Connection 16
  - Cable 16
  - Down 4, 16
    - Symptoms of 17
  - Down or flapping 6, 17
  - Network connection 16
  - Trunk cable 16
  - Unstable 4, 17
    - Symptoms of 17
- Connectivity exception
  - System 9
  - VLAN 18
- Connectivity polling
  - Analysis mode 47
  - Polling interval 47

- Retries 47
- Timeout 47
- Connectivity polling - external poller
  - Analysis mode 48
  - Initial status 48
  - Instrument card 48
  - Instrument IP 48
  - Instrument network adapters 48
  - Instrument SNMP agents 48
- Connectivity setting 32
  - Correlation use bridging mode 52
  - Number of bridged via threshold 52
  - Number of bridges threshold 52
  - Restart trap threshold 8, 23, 52
  - Restart trap window 8, 23, 53
  - Testing notification mode 12, 53
- Console
  - Domain Manager Administration Console 56
  - Polling and Thresholds Console 57
- Copying a group 63
- Correlation use bridging mode 52
- Creating a group 64

## D

- Dial-on-demand interface setting 49
  - Maximum uptime 53
  - Unstable notification 33
- Disabled
  - Network adapter 14
- Discovery error 10
- DiscoveryErrorInfo attribute 10
- Domain Manager Administration Console 56
- Down
  - Card 19
  - Chassis 19
  - Connection 16
  - IP 28
  - Network adapter 12
  - Partition 21
  - System 8
- Duplicate 29
- Duplicate IP 29
  - Duplicate 6

## E

- Edge
  - Table of 37
- Element
  - Assigning to groups 59

- Exception
  - Definition of 2
  - Summary table 5
  - System
    - Connectivity 5, 9
    - Operational 5, 9
  - VLAN
    - Connectivity 5
    - Operational 5, 18

## F

- FDDI interfaces threshold group 49
- Firewall 7

## G

- Global Console 35
  - Map Console view 36
  - Notification Log Console view 36

## Group

- Assigning members 59
- Changing priority 60
- Copying 63
- Creating 64
- Properties 59

## Groups

- Definition of 45
- Polling
  - Hubs and Bridges 46
  - Other Systems 46
  - Routers 46
  - Switches 46

- Systems resource groups 54

## Threshold

- 1 Gb Ethernet access ports 50
- 1 Gb Ethernet interface 49
- 1 Gb Ethernet trunk ports 50
- 10/100 Mb Ethernet access ports 50
- 10/100 Mb Ethernet interface 49
- 10/100 Mb Ethernet trunk ports 50
- ATM access ports 50
- ATM interface 49
- Backup interfaces 49
- Dial-on-demand interfaces 49
- FDDI interfaces 49
- Hubs and bridges system resources 50
- Other Ports access ports 50
- Other Ports trunk ports 50
- Other Systems system resource 50
- Routers system resources 50



---

- Serial interfaces group 49
- Switches system resource 50
- Token Ring interfaces group 49
- Trunk ports 49

## H

- Host 7
- HSRP Group 25, 28
- Hub 7
- Hubs and Bridges polling group 46
- Hubs and Bridges threshold group 50

## I

- ICMP polls 2, 45
- Initial status 48
- Instrument card 48
- Instrument IP 48
- Instrument network adapters 48
- Instrument SNMP agents 48
- Interface 12
- Interface management policy
  - Description 54
  - Parameters 55
- Interface/port flapping setting 32
  - Link trap threshold 13, 54
  - Link trap window 13, 54
- IP
  - Down 6, 28
  - Duplicate 29
  - Unresponsive 6, 28
- IP network 40
  - Connectivity map 41
  - Membership map 41
- IPStatus attribute 28, 78, 82
- IsAnyComponentDown attribute 80
- IsEveryComponentDown attribute 80
- IsFlapping attribute 4, 13, 15, 76
- IsNetworkAdapterDown attribute 76
- IsNetworkAdapterFlapping attribute 4, 17, 76
- IsUnresponsive attribute 73

## L

- Link trap threshold 13, 32, 54
- Link trap window 13, 32, 54
- Logical connection down 14

## M

- Map

- Background 39
- Icons and indicators 37
- Type of 39
  - IP network connectivity 41
  - IP network membership 41
  - Physical connectivity 40, 42
  - VLAN connectivity 41
  - VLAN membership 42

### Map Console

- Icons and indicators 37
- Type of map 39
  - IP network connectivity 41
  - IP network membership 41
  - Physical connectivity 40, 42
  - VLAN connectivity 41
  - VLAN membership 42

### Maps

- Opening 36

### Matching criteria

- 1 Gb Ethernet access ports threshold group 50
- 1 Gb Ethernet interface threshold group 49
- 1 Gb Ethernet trunk ports threshold group 50
- 10/100 Mb Ethernet access ports threshold group 50
- 10/100 Mb Ethernet interface threshold group 49
- 10/100 Mb Ethernet trunk ports threshold group 50
- Adding or removing 61
- ATM access ports threshold group 50
- ATM interface threshold group 49
- ATM trunk ports threshold group 50
- Backup interfaces threshold group 49
- Changing 62
- Dial-On-Demand interfaces threshold group 49
- FDDI interfaces threshold group 49
- Hubs and Bridges polling group 46
- Hubs and Bridges system resource threshold group 50
- Other Systems polling group 46
- Other Systems system resource threshold group 50
- Routers polling group 46
- Routers system resource threshold group 50
- Serial interfaces threshold group 49
- Switches polling group 46
- Switches system resource threshold group 50
- Token Ring interfaces threshold group 49

### Maximum uptime 51

- Backup interface support setting 51
- Dial-on-Demand interface support setting 53

- moduleStandbyStatus 20
- Multilayer switch feature card (MSFC) 7

### N

- Network adapter
  - Administratively down 6, 15
  - Backup activated 6, 15
  - Disabled 4, 14
    - Symptoms of 14
  - Down 4, 12
    - Symptoms of 12
  - Down or flapping 6, 15
  - Exceeded maximum uptime 6, 15
  - Interface 12
  - Logical connection down 4, 14
    - Symptoms of 14
  - Port 11
  - Redundancy group 23
  - Sub-interface 12
  - Unstable 4, 13
    - Symptoms of 13
- Network connection 16
  - Redundancy group 24
- Node 7
  - Table of 37
- Not responding
  - SNMP agent 22
- Notification
  - Aggregate 2
  - Display of 2
  - Types 2
  - Exception
    - see Exception
  - Root-cause
    - see Root-cause
  - Symptomatic
    - see Symptomatic event
- Number of bridged via threshold 52
- Number of bridges threshold 52

### O

- Opening a Map 36
- Operational exception
  - System 9
  - VLAN 18
- OperStatus attribute 28, 75
- Other Ports threshold group 50
- Other Systems polling group 46
- Other Systems threshold group 50

### P

- Partition 20

- Down 4, 21
  - Symptoms of 21
- partition.conf 21
- Permanent Virtual Circuit (PVC) 38
- Physical connectivity map 40, 42
- Polling
  - ICMP 2, 45
  - SNMP 2, 45, 85
- Polling and Thresholds Console 56
  - Layout 57
  - Polling tab 57
  - Thresholds tab 57
  - Toolbar buttons 58
- Polling interval 47
- Polling tab 57
- Port 11
  - Access 50
  - Trunk 50
- Priority
  - Changing 60
- Probe 7

### R

- Redundancy group 23, 38
  - All components down 6, 24
  - At risk 6, 24
  - AtRiskThreshold 24
  - Reduced redundancy 6, 24
- Removing or adding a setting 60
- Removing or adding matching criteria 61
- Restart trap threshold 8, 23, 32, 52
- Restart trap window 8, 23, 32, 53
- Restoring default values of a setting 63
- Retries
  - Connectivity polling 47
- Root cause 2
  - Card down 4, 19
  - Chassis down 4, 19
- Connection
  - Down 4, 16
  - Unstable 4, 17
- Network adapter
  - Disabled 4, 14
  - Down 4, 12
  - Logical connection down 4, 14
  - Unstable 4, 13
- Partition down 4, 21
- SNMP agent not responding 4, 22
- Summary table 3

---

- System
  - Down 4, 8
  - Unstable 4, 8
- Router 7
- Router switch feature card (RSFC) 7
- Router switch module (RSM) 8
- Routers polling group 46
- Routers threshold group 50

**S**

- Serial interfaces threshold group 49
- serverConnect.conf 56
- Setting
  - Adding or removing 60
  - Changing parameters 62
  - Definition of 45
  - Hubs and Bridges polling group 46
  - Hubs and Bridges system resource threshold group 50
  - Other Systems polling group 46
  - Other Systems system resource threshold group 50
  - Restoring default values 63
  - Router polling group 46
  - Routers system resource threshold group 50
  - Switches polling group 46
  - Switches system resource threshold group 50
- SNMP
  - Polling 85
  - Polls 2, 45
  - Trap 31
    - Cold start 31
    - Link down 31
    - Link up 31
    - List of 67
    - Warm start 31
- SNMP agent 22
  - Not responding 4, 22
  - Symptoms of 22
  - Repeated restarts 6, 23
  - Unresponsive 6, 23
- SNMPStatus attribute 78
- Stable time 32
- StandbyStatus attribute 77
- Status attribute 77
- Sub-interface 12
- Switch 8
- Switches polling group 46
- Switches threshold group 50
- Symptomatic event 2

- Card
  - Operationally down 6, 20
  - Switch over 6, 20
- Connection down or flapping 6, 17
- Duplicate IP
  - Duplicate 6, 29
- HSRP Endpoint
  - Switch over 29
- HSRP group
  - Switch Over 6
  - Switch over failed 6, 24
- IP
  - Down 6, 28
  - Unresponsive 6, 28
- Network adapter
  - Administratively down 6, 15
  - Backup activated 6, 15
  - Down or flapping 6, 15
  - Exceeded maximum uptime 6, 15
- Redundancy group
  - All components down 6, 24
  - At risk 6, 24
  - Reduced redundancy 6, 24
- SNMP agent
  - Repeated restarts 6, 23
  - Unresponsive 6, 23
- System
  - Discovery error 6, 11
  - Might be down 6, 11
  - Unresponsive 6, 11
- System 7
  - Bridge 7
  - Connectivity exception 5, 9
  - Discovery error 6, 10, 11
  - Down 4, 8
    - Symptoms of 8
  - Firewall 7
  - Host 7
  - Hub 7
  - Might be down 6, 11
  - Multilayer switch feature card 7
  - Node 7
  - Operational exception 5, 9
  - Probe 7
  - Router 7
  - Router switch feature card 7
  - Router switch module 8
  - Switch 8
  - Terminal server 8
  - Unresponsive 6, 11

- Unstable 4, 8
  - Symptoms of 8
- Unsupported 8
- System redundancy group 24
- System Resource Groups 50
- Systems Resource Groups
  - Interface Management Policy 54

- Operational exception 5, 18
- Tagging policy 55

## T

- Tagging Policy, VLAN 55
- Technical Support xiv
- Terminal server 8
- Testing notification mode 12, 53
- Threshold
  - AtRiskThreshold 24
  - Interface Management Policy 54
  - Restart trap threshold 8
  - Restart trap window 8, 23
  - Testing notification mode 12
- Timeout
  - Connectivity polling 47
- Token Ring interfaces threshold group 49
- Topology Maps
  - See Maps 35
- Trunk cable 16
- Trunk ports
  - Definition of 50
  - Group 49

## U

- Unresponsive
  - IP 28
  - SNMP agent 23
  - System 11
- Unstable
  - Connection 17
  - Example of diagnosis 32
  - Minimum traps used to diagnose 32
  - Network adapter 13
  - System 8
  - Trap window used to diagnose 32
- Unsupported 8

## V

- Virtual router 7
- VLAN 18, 40
  - Connectivity exception 5, 18
  - Connectivity map 41
  - Membership map 42