InCharge™

MPLS/VPN Manager User's Guide

Version 1.0
November 2003

Cisco Part Number: OL-6052-01

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 PARITES 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 (c) 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>>

Contents

Preface

This guide provides detailed information about InCharge MPLS/VPN Manager. InCharge MPLS/VPN Manager, in conjunction with InCharge IP Availability Manager, automatically diagnoses failures in MPLS/VPN networks and sends the results of its analysis to InCharge Service Assurance Manager.

Intended Audience

This guide is intended to be read by IT managers seeking to better understand the value of InCharge MPLS/VPN Manager, and by system administrators configuring and using InCharge MPLS/VPN Manager.

Prerequisites

It is assumed that both InCharge IP Availability Manager and InCharge Service Assurance Manager are installed. The Global Console is required to configure Polling Groups and Threshold Groups, when applicable. For information on installing these products, refer to the *InCharge Installation Guide*.

Document Organization

This guide consists of the following chapters:

1. INTRODUCTION	Provides brief introductions to MPLS and VPN, and provides an overview of the InCharge MPLS/VPN Manager.
2. MPLS/VPN ELEMENTS AND THEIR FAILURES	Describes the elements monitored by the InCharge MPLS/VPN Manager, and the faults diagnosed.
3. MPLS/VPN MAPS	Provides a brief discussion on how to use the MPLS/VPN maps.
A. MPLS MIBS POLLED	Identifies the MIBs used by the InCharge MPLS/VPN Manager to diagnose connectivity problems.
B. CLI COMMANDS	Discusses the CLI commands used by the InCharge MPLS/VPN Manager.

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
keyword	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
/InCharge	Indicates directory path names in italics
yourDomain	Indicates a user-specific or user-supplied value in bold, italics
File > Open	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.

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 Installation Guide*
- *InCharge System Administration Guide*
- *InCharge Global Console Guide*

InCharge IP Management Documentation

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

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

InCharge Service Assurance Manager Documentation

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

- *An Introduction to InCharge Service Assurance Manager*
- *InCharge Service Assurance Manager Configuration Guide*
- *InCharge Service Assurance Manager Failover System User's Guide*
- *InCharge Service Assurance Manager User's Guide for Business Impact Manager*

The following SMARTS documents are relevant to InCharge Service Assurance Manager adapters.

- *InCharge Service Assurance Manager Notification Adapters User's Guide*
- *InCharge Service Assurance Manager Adapter Platform User's Guide*
- *InCharge XML Adapter User's Guide*
- *InCharge Service Assurance Manager User's Guide for Remedy Adapter*
- *InCharge Service Assurance Manager User's Guide for Concord eHealth Adapter*
- *InCharge Service Assurance Manager User's Guide for InfoVista Adapter*

Abbreviations and Acronyms

The following lists common abbreviations and acronyms that are used in this InCharge guide.

BGP	Border Gateway Protocol
CE	Customer Edge Router
FEC	Forwarding Equivalence Class
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
LDP	Label Distribution Protocol
LSP	Label Switched Path
LSR	Label Switched Router
MBGP	Multiprotocol (extensions of) BGP
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
OSPF	Open Shortest Path First
P	MPLS-Enabled Provider Core Router
PE	MPLS-Enabled Provider Edge Router
RSVP	Resource Reservation Protocol
VPN	Virtual Private Network
VRF	VPN Routing and Forwarding

1

Introduction

This chapter provides brief introductions to Multiprotocol Label Switching (MPLS) and Virtual Private Networks (VPNs). It also provides an overview of the InCharge MPLS/VPN Manager, and describes the domains that the InCharge MPLS/VPN Manager monitors.

Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS), a network technology that separates packet forwarding from packet routing, brings to Internet Protocol (IP) the features, reliability, and predictability of traditional carrier networks, while preserving the dynamic characteristics, flexibility, and cost effectiveness of IP, the world's dominant network protocol.

MPLS technology achieves its versatility through the use of two components: a packet forwarding component, and a routing control component. The packet forwarding component switches at wire speeds using short, fixed-length packet labels. The control component implements sophisticated traffic engineering policies to deliver predictable and reliable performance over different classes of service, and to support the most rigorous transport and bandwidth requirements.

Among its many benefits, MPLS dramatically simplifies the deployment, management, scalability, and flexibility of Virtual Private Networks (VPNs). MPLS VPNs offer the security to conduct private communications over a public infrastructure, the scalability to support hundreds of thousands of users, and the flexibility to accommodate any-to-any traffic patterns.

Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs), which usually include at least several remote sites, are networks that share a common infrastructure, yet provide separate interconnections between the related sites which provide secure communications between those sites.

MPLS implementations of IP VPNs commonly consist of sets of Customer Edge (CE) routers, each of which is attached to one or more Provider Edge (PE) routers that are members of a service provider's network. The CE routers take no active part in the MPLS protocol, and use standard IP policies to exchange data and control information with other subscribers of their respective VPNs.

The PE routers maintain VPN membership and topology information. With this information, the PE routers delegate connections between VPN members by establishing Border Gateway Protocol (BGP) peer relationships with other PE routers attached to members of the same VPNs. Label Switched Paths (LSPs) are established between the BGP peers, and can carry traffic associated with multiple VPNs.

The backbone of the service provider's network also includes Provider Core (P) routers that transport various types of data between the sites of the VPNs.

Figure 1 illustrates an MPLS/VPN managed domain.

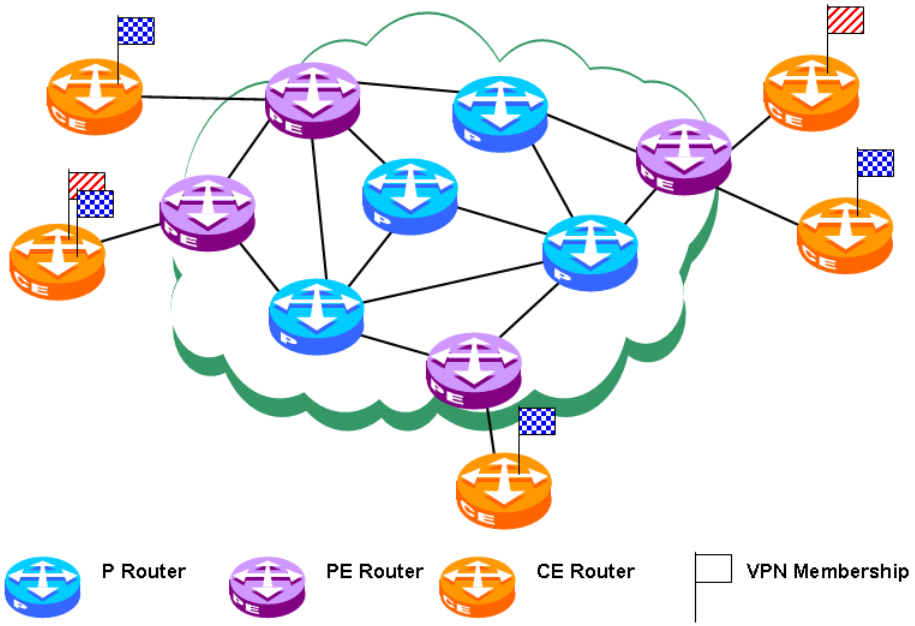

Figure 1: The Managed Domain

InCharge MPLS/VPN Manager

InCharge MPLS/VPN Manager is an InCharge solution that, along with InCharge IP Availability Manager and InCharge Service Assurance Manager (release 6.0 and later), manages MPLS networks and VPNs configured and provisioned over them, in accordance with IETF RFC 2547bis. It provides management capabilities for both the MPLS and the VPN domains of an MPLS/VPN network. It also provides for the mapping and correlation among the domains, and between the MPLS/VPN domains and the underlying transport domain, by means of cross domain correlation and cross domain impact analysis.

InCharge MPLS/VPN Manager Architecture

InCharge MPLS/VPN Manager must be implemented in conjunction with InCharge IP Availability Manager and InCharge Service Assurance Manager. Figure 2 illustrates its position within the framework of a total solution, as well as the flow of information between the components of the solution.

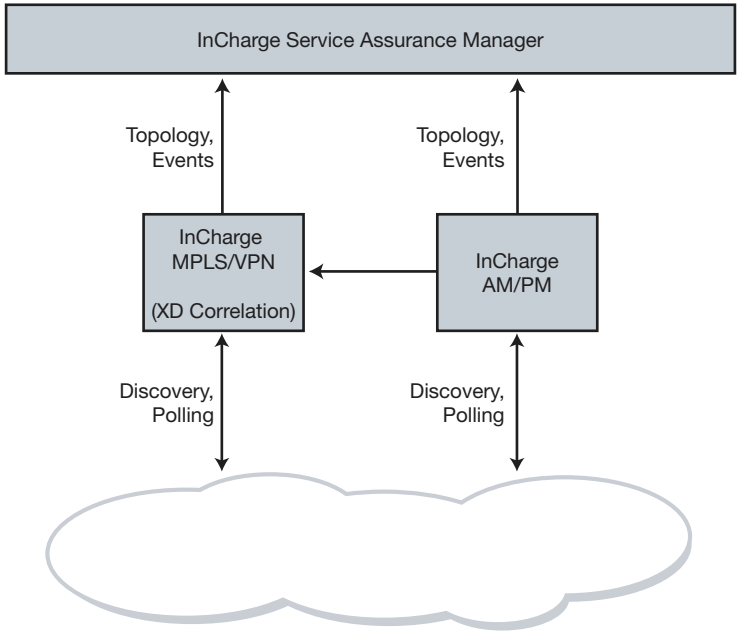

Figure 2: InCharge MPLS/VPN Solution Architecture

In the figure:

- InCharge MPLS/VPN Manager discovers and manages the MPLS and VPN domains, and performs cross-domain correlation (XD Correlation).
- InCharge IP Availability Manager (AM) discovers and manages the underlying transport domain.
- InCharge Service Assurance Manager (SAM) consolidates information from the managed domains, correlates and aggregates notifications from the underlying analysis servers, and provides end-to-end impact analysis. Its Global Console offers comprehensive graphical presentations of all network elements and their relationships.

InCharge MPLS/VPN Manager Features

Along with InCharge IP Availability Manager and InCharge Service Assurance Manager, the features of InCharge MPLS/VPN Manager include:

- Automatic discovery of LSPs in an MPLS network
- Monitoring of LSP status and performance
- Diagnostic analysis of failures in the MPLS domain
- Automatic discovery of VRF instances in a network
- Monitoring of VRF status and performance
- Automatic discovery of VPN membership
- Automatic discovery of VPN topologies
- Diagnostic analysis of failures in the VPN domain
- Correlation of failures in the MPLS, VPN, and transport domains
- Impact analysis in the MPLS and VPN domains

InCharge MPLS/VPN Manager and the Managed Domains

In the MPLS domain, InCharge MPLS/VPN Manager discovers and monitors MPLS Label Switched Paths (LSPs) in the MPLS network (on both Provider Core and Provider Edge routers), and infers LSP traces from MPLS forwarding tables.

Figure 3 illustrates the MPLS domain that InCharge MPLS/VPN Manager monitors.

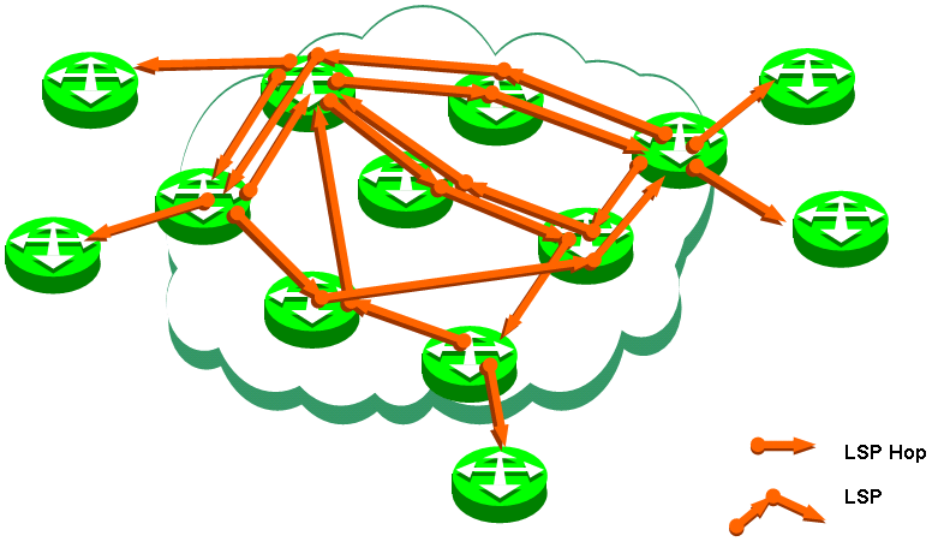

Figure 3: The MPLS Domain

In the VPN domain, InCharge MPLS/VPN Manager discovers and monitors VPN Routing and Forwarding (VRF) tables in the PE routers, determines VPN topology and membership in post processing, and monitors the status and performance of VRFs.

Figure 4 illustrates the VPN domain that InCharge MPLS/VPN Manager monitors.

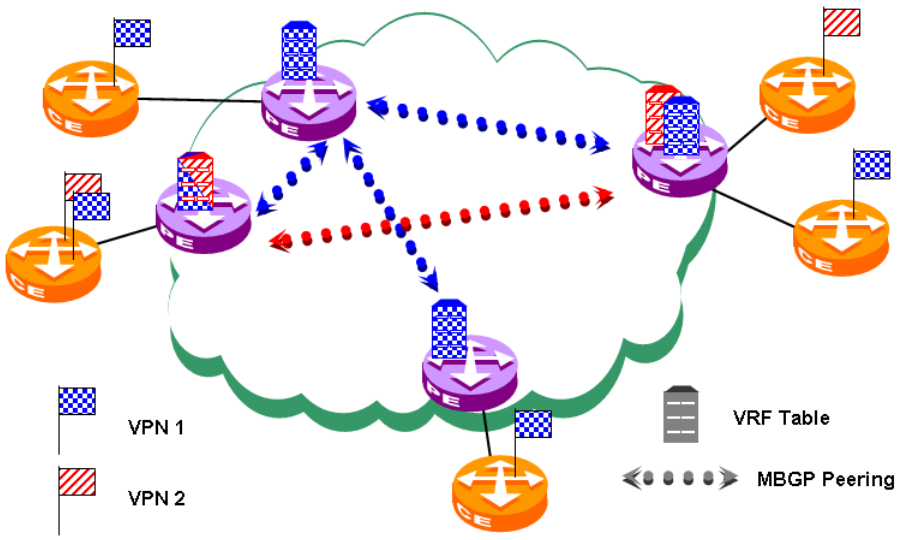

Figure 4: The VPN Domain

InCharge IP Availability Manager discovers and monitors the underlying infrastructure, and correlates the alarms that are generated as a result of any failures in the infrastructure. It then pinpoints the failed element, and identifies all managed elements affected by the failure. The results of its processes are forwarded to the MPLS/VPN Manager and the Global Manager.

Figure 5 illustrates the Transport domain (underlying infrastructure) that InCharge IP Availability Manager monitors.

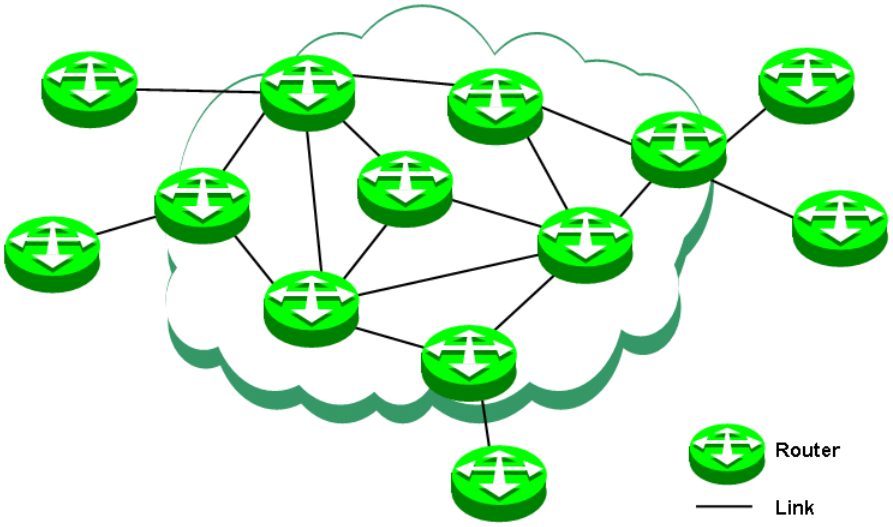

Figure 5: The Transport Domain

InCharge Service Assurance Manager imports topology and event information from the underlying managed domains, consolidates the information, and interprets the severity of the problems in the context of services and businesses. Service Assurance then provides operations personnel with meaningful information with which automated corrective actions can be associated.

2

MPLS/VPN Elements and Their Failures

This chapter describes the MPLS/VPN elements discovered and managed by InCharge MPLS/VPN Manager and the failures diagnosed for each element. The diagnosis identifies root-cause failures in the MPLS/VPN domain, indicating problems that require immediate attention. InCharge MPLS/VPN 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.

The chapter also describes the elements that the InCharge MPLS/VPN Manager uses when it monitors the managed elements and diagnoses failures.

Note: In addition to the processes that InCharge MPLS/VPN Manager performs, InCharge IP Availability Manager discovers and monitors the MPLS/VPN network infrastructure elements, and diagnoses connectivity failures between those elements. See the *InCharge IP Availability Manager User's Guide* for information about the elements that it monitors, along with descriptions of their failures.

Summary of Elements Monitored and Faults Diagnosed

The following table summarizes the MPLS/VPN elements monitored and faults diagnosed.

ELEMENT	DIAGNOSIS	EXPLANATION
VPN	Impacted	Connectivity between VPN peers (peer VRFs hosted by PEs) has been impaired by connectivity failures in the transport layer.
VRF	Impacted	Connectivity between this VRF and one or more of its VPN peers has been impaired by connectivity failures in the transport layer.
LSP	Impacted	Connectivity for this path has been impaired by connectivity failures in the transport layer.
LSPHop	Impacted	Connectivity for this LSP Hop has been impaired by connectivity failures in the transport layer.
VRF	MidRoutesExceeded	The mid threshold of VRF routes has been crossed. (See explanation below.)
VRF	HighRoutesExceeded	The high threshold of VRF routes has been crossed. (See explanation below.)
VRF	MaxRoutesExceeded	The maximum number of VRF routes has been reached. (See explanation below.)
VPN	MidRoutesExceeded	The mid threshold of VRF routes for one or more VRFs that are members of this VPN has been crossed. (See explanation below.)
VPN	HighRoutesExceeded	The high threshold of VRF routes for one or more VRFs that are members of this VPN has been crossed. (See explanation below.)
VPN	MaxRoutesExceeded	The maximum number of VRF routes for VRFs that are members of this VPN has been reached. (See explanation below.)

Table 3: Summary of Elements Monitored and Faults Diagnosed

Each VRF (hosted by a PE) has its own routing table where it holds routing information for routes it learned either from its attached CE(s), or from peer VRFs in the same VPN. In addition to routing information, each VRF also maintains three attributes: MidRouteThreshold, HighRouteThreshold and MaxRoutes. The size of the routing table, namely the number of routes it holds, is compared against these attributes. If the device supports the MPLS-VPN MIB and the VRF is SNMP instrumented, then InCharge will monitor the number of routes in each VRF and will generate events when the mid-level and high-level thresholds are crossed. The maximum level denotes the maximum number of routes which this VRF is configured to hold. When set to zero, these values are ignored.

MPLS Elements

The following MPLS elements are used by the InCharge MPLS/VPN Manager when it monitors the managed elements and diagnoses failures.

LSP

An LSP (Label Switched Path) is a concatenation of LSPHops which represents the label-switched path taken by labeled packets across an MPLS network. In some cases (when not all the devices of the MPLS network are managed by InCharge) an LSP will only contain part of the entire path.

LSPHop

An LSPHop (Label Switched Path Hop) represents a uni-directional logical link between two devices in an MPLS network across which MPLS-labeled packets are sent and no processing of the label occurs. An exception to this definition is the last hop of an LSP (see LSP definition) across which the packet that is sent may be un-labeled due to penultimate label popping. In that case, the Label attribute of the LSPHop is 3, although the packet is, in fact, un-labeled.

LSPInSegment

An LSPInSegment (Label Switched Path In Segment) represents an incoming label in the MPLS forwarding table of a device.

LSPOutSegment

An LSPOutSegment (Label Switched Path Out Segment) represents an outgoing label in the MPLS forwarding table of a device.

VPN Elements

The following VPN elements are used by the InCharge MPLS/VPN Manager when it monitors the managed elements and diagnoses failures.

RouteTarget

InCharge MPLS/VPN Manager creates an instance of RouteTarget for each route target used in the network. These are used to identify peering relationships between VRF instances, and for the instantiation of VPN instances. For a complete explanation on how route targets are used to define VPNs in an MPLS/BGP VPN, please refer to Sections 4.3.1 and 4.3.5 of *IETF RFC 2547bis*.

VRF

A VRF represents a VPN Routing and Forwarding instance on a PE (Provider Edge) router. For a complete explanation on how VRFs are used to isolate VPN traffic between different VPN customers in an MPLS/BGP VPN, please refer to Chapter 3 of *IETF RFC 2547bis*.

VPN

A VPN represents a collection of VRFs configured in the network that are all members of the same Virtual Private Network.

3

MPLS/VPN Maps

This chapter briefly describes how to use the MPLS/VPN maps that can be displayed on the Global Console to learn more about the source, impact and causes of MPLS/VPN events.

Note: See the *InCharge Operator's Guide* for detailed information about the use of the Global Console.

Using the MPLS/VPN Maps

Maps provide a graphical representation of your topology. As you monitor your managed domain, you might need to examine the elements of your maps and investigate the active events that affect them. Maps for MPLS/VPN elements display the LSPs and routers that comprise VPNs and VRFs. There are three types of maps that focus on MPLS elements:

- LSP Map
- LSP Hops Map
- VPN Map

There are several ways to launch maps that display MPLS topology elements from the Global Console:

- From the **Show Map** option: This appears in the Event menu or the pop-up menu if you right-click on a selected MPLS-related notification. It also appears in the pop-up menu of an MPLS instance in the Topology Browser or the Map Browser.

- From a node in a map: You can right-click on an MPLS node (such as a VPN, VRF, router, or LSP) in an existing map and select LSP Map from the submenu.
- From the **Show Map** button: This appears in the Find Instance and Find System dialog boxes. (The button is activated when you select a row in the table.) An LSP Map can be launched when you find and MPLS node.

LSP Map

The LSP map displays connectivity between Provider Edge (PE) routers. The edges in the LSP map represent LSP instances in the repository. They are displayed as solid lines with directional arrows signifying the destination end of the LSP.

Note: The detailed hops of the LSPs are not shown in this map. They can be viewed in the LSP Hops maps. The only routers shown in the LSP map are PE routers that are either the source or destination of each LSP displayed in the map.

- When launched from an LSP, this map displays the LSP and the two PE routers associated with it.
- When launched from a VPN, the LSP map displays the PE routers and LSPs belonging to the VPN in either the Hub and Spoke or the Full Mesh configuration.
- When launched from a PE router, the LSP map displays all the LSPs that either originate or terminate at that PE router.
- When launched from a VRF, this map shows all of the LSPs utilized by the VRF to communicate with its peer VRFs.

Figure 6 provides an example of an LSP map.

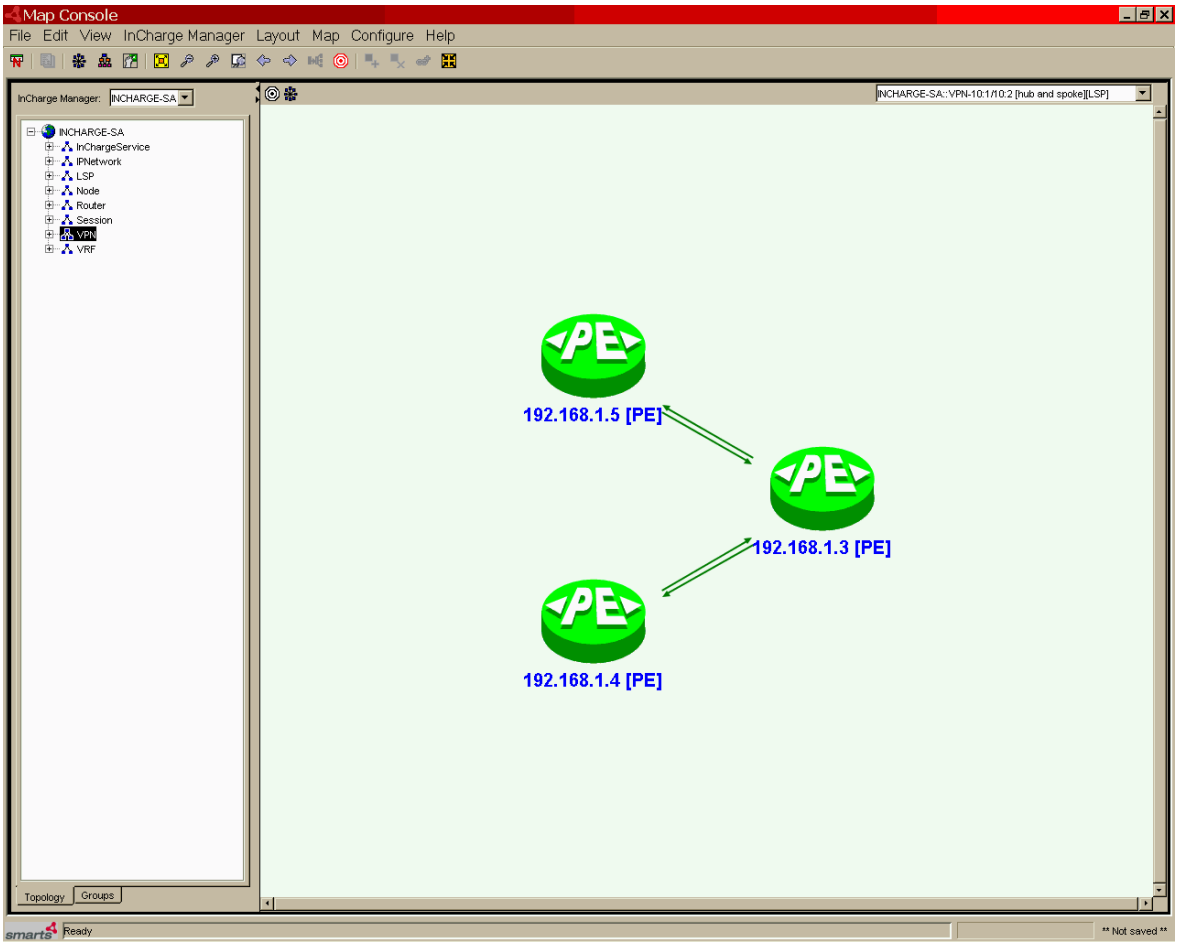

Figure 6: LSP Map

LSP Hops Map

The LSP Hops map displays similar information to the LSP map except that instead of displaying just the endpoint PE routers of an LSP, it includes all of the transit, or intermediate, Provider Core (P) routers as well. The LSP Hops map can be accessed by right-clicking on a router node or an LSP connection edge in an LSP map and choosing LSP Hops from the list of maps in the menu.

Additionally, the LSP Hops map contains a **Highlight LSP** button to identify all of the hops in one LSP. Click this button to bring up a list of LSPs displayed in the map. Select the appropriate LSP from the list to highlight all of the LSP Hops that comprise that LSP. The map edges appear in bold to represent the LSP Hops in the selected LSP.

Figure 7 provides an example of an LSP Hops map.

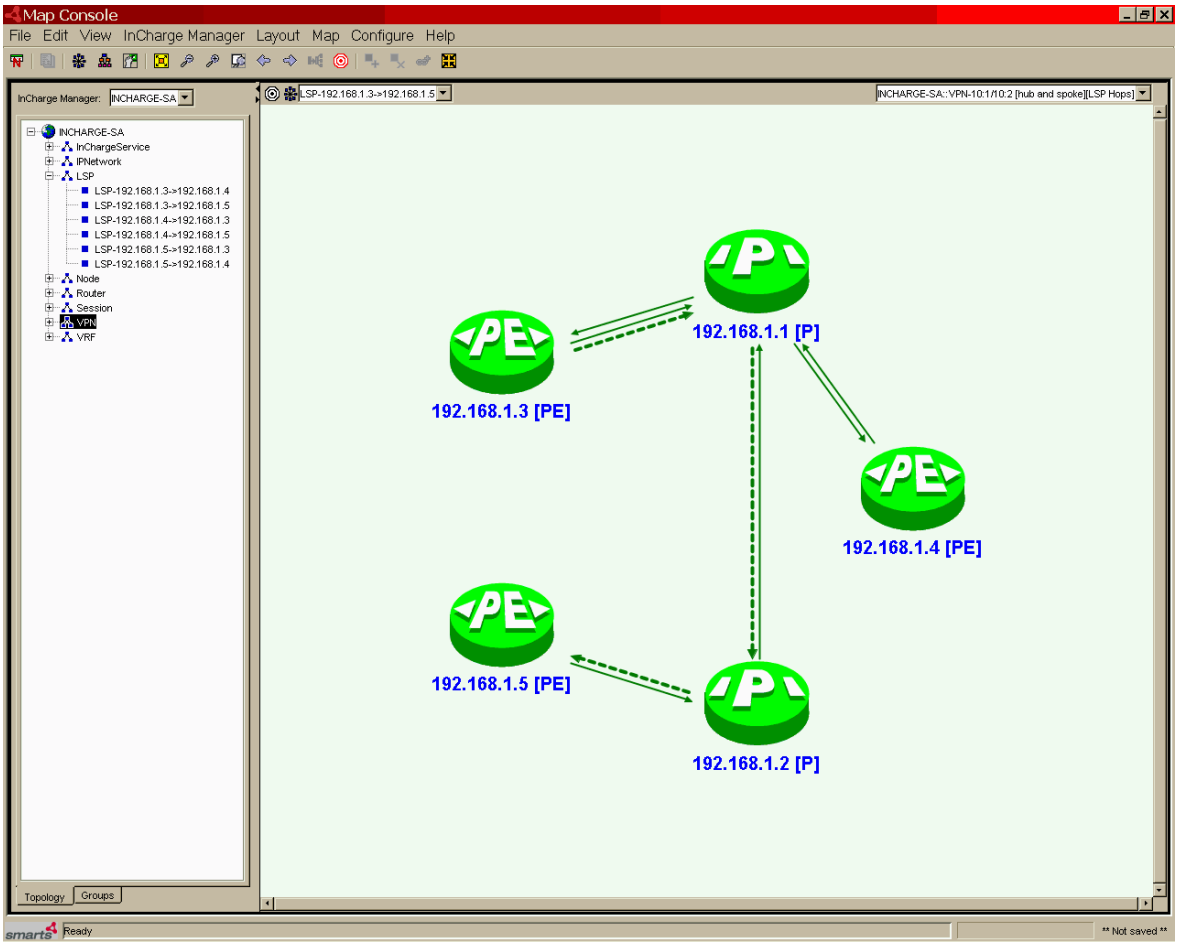

Figure 7: LSP Hops Map

VPN Map

The VPN map displays icons for VPNs, VRFs, Customer Edge routers (CEs) and Provider Edge routers (PEs). Whenever a VRF is displayed, the PE that hosts the VRF, as well as the CEs attached to the VRF, are also displayed.

- When launched from a VPN, the map displays all of the VRFs that are part of this VPN (and their CEs and PEs).
- When launched from a PE, the map displays all of the VRFs hosted by the PE.
- When launched from a VRF, the map displays that VRF.
- When launched from a CE, the map displays all the VRFs to which this CE is attached.

If an icon has a plus sign (+) next to it, it can be expanded. For example, if a plus sign appears next to a PE, then it hosts additional VRFs which are not currently displayed in the map. Right click the PE and choose Expand Node to display those VRFs.

You can also right click the background of the VPN map to display two menu items called "Show PEs" and "Show CEs." Both show check marks next to them. If you uncheck Show PEs, then the PEs are removed from the map. Click it again to re-display the PEs. This also applies to the CEs. Removing displayed icons can make the map easier to read.

Figure 8 provides an example of a VPN map.

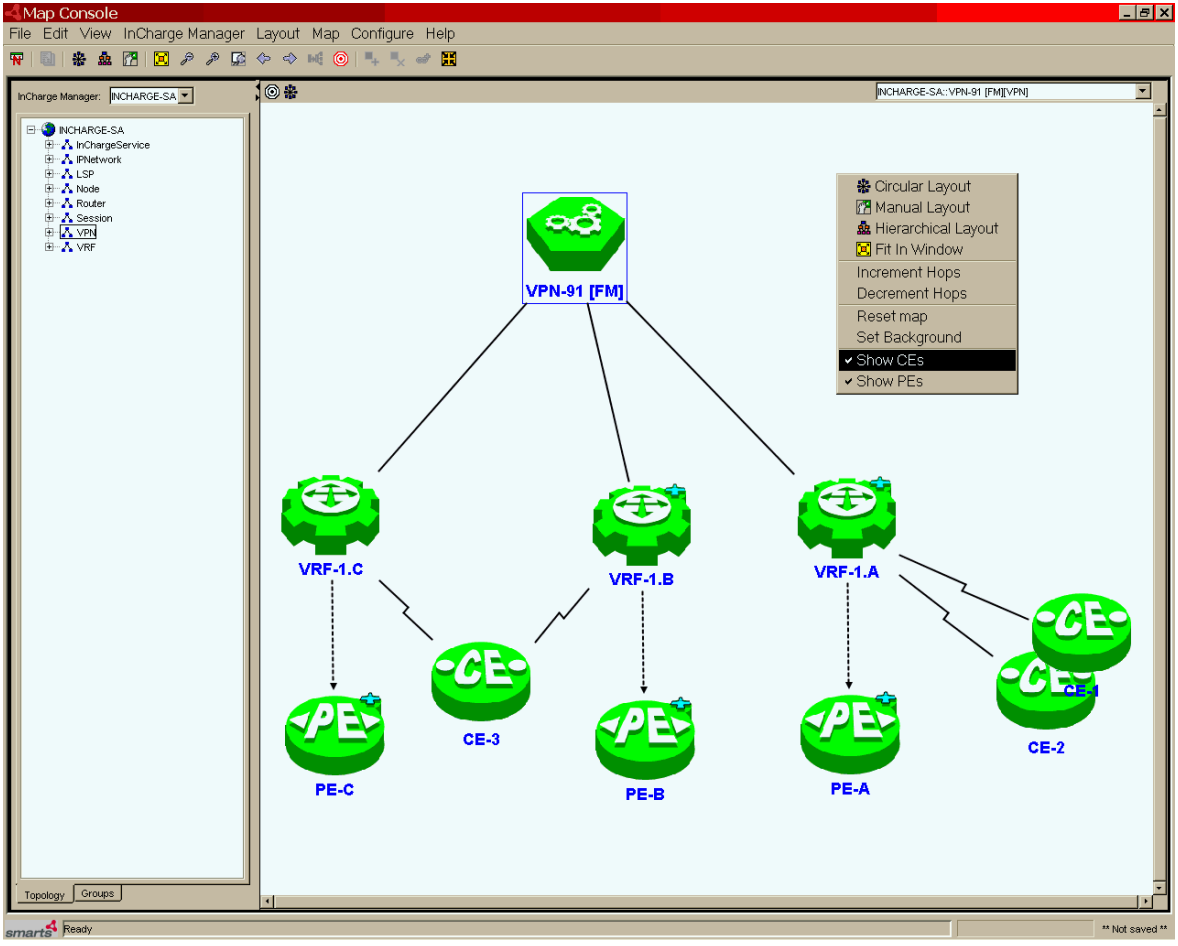

Figure 8: VPN Map

A

MPLS MIBs Polled

This appendix lists the MIBs polled by InCharge MPLS/VPN Manager.

MPLS MIBs

The following MIBs are used by InCharge MPLS/VPN Manager.

- MPLS-LSR-MIB: This is available on Cisco 7200 and 7500 series devices, and on 12000 series devices.
- MPLS-VPN-MIB: This is available on Cisco 7200 and 7500 series devices.

MPLS-LSR-MIB

MPLS-LSR-MIB (IETF version *draft-ietf-mpls-lsr-mib-05.txt*.) The OIDs used are:

- mplsInterfaceConfTable

  mplsInterfaceLabelParticipationType (1.3.6.1.3.96.1.1.1.10)
- mplsInSegmentTable

  mplsInSegmentXCIndex (1.3.6.1.3.96.1.3.1.5)
- mplsOutSegmentIndexNext (1.3.6.1.3.96.1.5)
- mplsOutSegmentTable

  mplsOutSegmentIfIndex (1.3.6.1.3.96.1.6.1.2)

  mplsOutSegmentTopLabel (1.3.6.1.3.96.1.6.1.4)

mplsOutSegmentNextHopIpv4Addr (1.3.6.1.3.96.1.6.1.6)

- mplsXCTable

  mplsXCLspId (1.3.6.1.3.96.1.9.1.2)

MPLS-VPN-MIB

MPLS-VPN-MIB (IETF version *draft-ietf-ppvpn-mpls-vpn-mib-03. txt.*) The OIDs used are:

- mplsVpnConfiguredVrfs (1.3.6.1.3.118.1.1.1)
- mplsVpnIfConfTable (1.3.6.1.3.118.1.2.1)
- mplsVpnVrfTable (1.3.6.1.3.118.1.2.2)
- mplsVpnVrfRouteTargetTable (1.3.6.1.3.118.1.2.3)
- mplsVpnVrfPerfCurrNumRoutes (1.3.6.1.3.118.1.3.1.1.3)
- mplsVpnVrfRouteNextHop (1.3.6.1.3.118.1.4.1.1.6)

B

CLI Commands

This appendix details the Command Line Interface (CLI) Commands used by InCharge MPLS/VPN Manager.

InCharge MPLS/VPN Manager CLI Commands

InCharge MPLS/VPN Manager uses specific CLI commands to obtain information regarding MPLS-enabled interfaces on devices, the MPLS forwarding tables, VRFs configured on the devices, and MP-BGP sessions between the devices and other MPLS-enabled devices. The CLI commands are invoked automatically during the discovery process using a CLI discovery probe. The set of commands invoked for the devices depend on the type of device (for example, MPLS-enabled router) and the availability of topological information through SNMP on that device. InCharge MPLS/VPN Manager will first attempt to obtain the information using SNMP. If the requested MIBs are not available on the device (either because the version of the device operating system does not support them or the vendor does not support them), it will use the CLI probe.

CLI Environment Variables

The CLI automates a telnet session with the network devices. The commands used by InCharge MPLS/VPN Manager require 'enable' privileges on the device. The user needs to specify three environment variables on the shell on which the InCharge MPLS/VPN Manager is running. The environment variables are:

- EXPECT_USERID
- EXPECT_PASSWORD
- EXPECT_ENABLE

The CLI uses EXPECT to automatically start a telnet session. EXPECT_USERID is the user login name; EXPECT_PASSWORD is the user password for the telnet session; and EXPECT_ENABLE is the enable password for the telnet session. These need to be specified only once before starting InCharge MPLS/VPN Manager. If the user name is already granted enable privileges (without having to type the enable password in the login phase) then the EXPECT_ENABLE variable can be given a dummy value (but needs to be specified). All MPLS-enabled devices in the network are required to be configured with the same user name and passwords.

CLI Commands for Cisco Devices.

MPLS

InCharge MPLS/VPN Manager checks whether the MPLS-LSR MIB exists on the device. If so, it obtains information about the MPLS forwarding tables and MPLS-enabled interfaces from that MIB. Otherwise it adds the commands "show mpls forwarding" and "show mpls interfaces" to the list of commands to be invoked.

VPN

InCharge MPLS/VPN Manager checks whether the MPLS-VPN MIB exists on the device. If so, it obtains information about VRFs from that MIB. Otherwise it adds the commands "show ip vrf detail" and "show ip bgp vpnv4 all tags" to the list of commands to be invoked.

CLI Commands for Juniper ERX Devices

Variants of the preceding commands are used for Juniper ERX devices.

Initally, InCharge MPLS/VPN Manager uses the "virtual-router" command to log into a specific virtual router on an ERX device.

Then, when applicable, the system uses the following commands:

- show mpls interface brief
- show mpls forwarding brief
- show ip vrf detail
- show ip bgp vpnv4 all fields best rd out-label peer next-hop extended-communities

Index

T

V