

HP OpenView Reporting and Network Solutions

MPLS VPN Smart Plug-in to Network Node Manager

User's Guide

Software Version: 3.0

for HP-UX, Solaris, and Windows® operating systems



i n v e n t

Manufacturing Part Number: None

November 2004

© Copyright 2004 Hewlett-Packard Development Company, L.P.

Legal Notices

Warranty.

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

©Copyright 2004 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

Trademark Notices.

Windows[®] is a U.S. registered trademark of Microsoft Corporation.

UNIX[®] is a registered trademark of The Open Group.

1. Introducing the MPLS VPN Smart Plug-in

Introduction	10
Features and Benefits of the MPLS VPN SPI	12
Behavior of the MPLS VPN SPI	13
User Interaction with the MPLS VPN SPI	14
MPLS VPN Events	14
MPLS VPN Views	17
Launching MPLS VPN Views	17
RAMS Integration	19
Reports from OVPI	19
Cross-Launching OVPI from the NNM Alarms Browser	19
Cross-Launching OVPI from the NNM GUI (ovw)	20
Cross-Launching OVPI from the MPLS VPN View	20
Related Documentation	21

2. Installing the MPLS VPN Smart Plug-in

Preparing for Installation	24
Hardware Requirements	24
Software Requirements	24
Supported Operating Systems	24
Network Node Manager	24
Optional Software	25
MIB Dependencies	25
Router Requirements	26
Updating from a Previous Version of the MPLS VPN SPI	28
Preserving Trap Customizations	28
Preserving SAA Test Definitions	28
Installing the MPLS VPN SPI	33
Installing the MPLS VPN SPI on a UNIX Operating System	33
Installing the MPLS VPN SPI on a Windows Operating System	34
Installation Options	36
Removing the MPLS VPN SPI	39
Removing the MPLS VPN SPI on a UNIX Operating System	39
Removing MPLS VPN SPI on a Windows Operating System	39
Initial Configuration	40
Configuring SNMP Polling Access	40
Configuration SNMP Polling Access for APA	40
Configuring SNMP Polling Access for netmon	41

Contents

Configuring SNMP Read/Write Access on Juniper Routers	42
Configuring SNMP Access	43
Configuring SNMP Trap Forwarding	43
MPLS VPN SPI Configuration File	44
3. Understanding MPLS VPN Discovery	
Discovery Process	48
VPN Naming Algorithm	50
Changing VPN Names in the MPLS VPN SPI Configuration	53
Ignoring Management Route Targets	55
4. Understanding Events from the MPLS VPN Smart Plug-in	
MPLS VPN Status Manager	60
Router Status Events	61
Network Core Status Events	65
Reachability Status Change Events	67
Cisco Router Reachability Tests	69
Juniper Router Reachability Tests	69
OVPI Report Pack Threshold Events	71
5. Configuring Reachability Tests	
Reachability Tests	74
Reachability Test Definitions	76
Special Considerations for CE-CE Reachability Tests	76
Non-Supported CE Type	77
Multiple CE Routers Connected to One PE Router	77
Reachability Test Definitions File Format	78
Changing Reachability Test Definitions	84
Reachability Test Configuration	85
Setting Reachability Test Configuration Parameters	85
Configuring Reachability Tests Using the MPLS VPN SPI	86
Configuring SAA Using the Cisco IOS Commands	88
6. Troubleshooting the MPLS VPN Smart Plug-in	
Troubleshooting Checklist	92
Verifying Proper Installation of Network Node Manager Advanced Edition	96

Contents

Determining Which Version of NNM is Installed	97
Setting the NNM Environment Variables	98
Verifying That the NNM Services Are Operating on the Management Station.....	99
Verifying That the MPLS VPN SPI Is Operating	100
Verifying That MIBs Are Loaded	101
Verifying That MPLS VPN Discovery Has Occurred.....	102
Verifying Reachability Test Definitions	103
Recreating the saa_tag.xml File.....	104
Recreating the saa.conf File.....	105
Recreating the ping_mib.conf File	105
Handling Other Problems	106
Rebooting an Edge Router Removes the SAA Test Definitions from the SAA MIB	106
PE Router Symbols Show Red in NNM.....	106
The PE Router Symbol Has a Square Shape, Not a Diamond Shape	107
VPN Names Are Confusing	107
A Change to the MPLS VPN Configuration Does Not Appear.....	107
Collecting Information for HP Support.....	108
Index	111

Contents

Support

Please visit the HP OpenView web site at:

<http://www.managementsoftware.hp.com/>

This web site provides contact information and details about the products, services, and support that HP OpenView offers.


You can also go directly to the support web site at:


<http://support.openview.hp.com/>


HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Throughout the site, access levels are indicated by the following icons:

 HP Passport

 Active contract

 Premium contract

To find more information about access levels, go to the following URL:

http://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to the following URL:

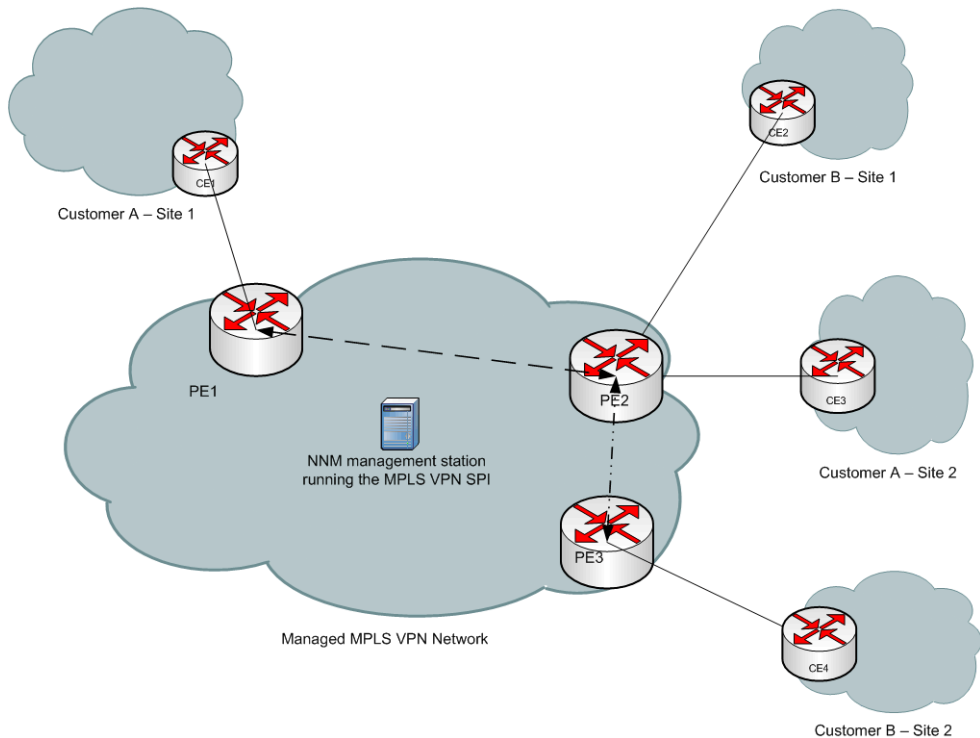
<https://passport.hp.com/hpp2/newuser.do>

Introduction

An internet service provider with an IP backbone may provide virtual private network (VPN) service to its customers using Multi Protocol Label Switching (MPLS) as defined in RFC2547bis. Two sites within a customer network have IP connectivity over the common backbone only if there is some VPN that contains both of them. Two sites with no VPN in common have no connectivity over the backbone.

An MPLS VPN is defined by the presence of a virtual routing and forwarding table (VRF) on an edge router in the service provider network. A VRF represents an instance of a VPN supported by one or more routers. The collection of customer sites from all network devices comprises the actual VPN. Figure 1-1 shows an example of an MPLS VPN network.

Figure 1-1 Example of an MPLS VPN Network



In an MPLS VPN network, the provider edge (PE) routers sit on the perimeter of the service provider's network. They communicate with two other kinds of routers: routers inside the MPLS VPN cloud that belong to the service provider and customer edge (CE) routers that are located and managed at customer sites. The HP OpenView Network Node Manager Smart Plug-in for MPLS VPN (MPLS VPN SPI) discovers VPN network topology and monitors the connectivity between the PE routers taking part in the MPLS VPNs. It uses this information to map raw nodes, PE interfaces, and related traps to VPN service-affecting events.

The MPLS VPN SPI identifies relationships between events and generates new events with the same or more detailed information. These enriched events help you quickly understand and react to a problem on your network. This faster reaction time reduces the mean time to repair (MTTR) the problems within your MPLS VPN network and improves the quality of service to your customers.

For a list of the edge router devices that the MPLS VPN SPI supports, see "Router Requirements" on page 26.

In addition to using the MPLS VPN SPI to diagnose problems affecting the PE and CE router infrastructure in near real-time, you can use the the MPLS VPN SPI to configure reachability tests of the connections between two PE routers taking part in a VPN. This testing gives real-time monitoring of the PE-PE connections and generates an SNMP event if a failure occurs. The MPLS VPN SPI also supports user-configured end-to-end reachability testing between two CE routers.

When HP OpenView Route Analytics Management System (RAMS) is integrated into NNM, the MPLS VPN SPI monitors changes to the best-effort label switch paths between the pairs of routers that are on the RAMS watch list. The MPLS VPN SPI does not support traffic-engineered label switch paths.

When the HP OpenView Performance Insight (OVPI) and NNM servers are integrated and the MPLS VPN Report Pack is running on the OVPI server, you can launch a series of VPN reports directly from the MPLS VPN views. These reports provide hourly, daily, and weekly analysis of performance trends, thus significantly enhancing your problem diagnostic capability.

Features and Benefits of the MPLS VPN SPI

The following list outlines the features of the MPLS VPN SPI and its benefits to you:

- The MPLS VPN SPI monitors the status of the PE routers in MPLS VPN networks and reports device outages.
- For each CE router to which the service provider has access, the MPLS VPN SPI monitors the status of the CE router and the PE-CE connection.
- By enriching network status events, the MPLS VPN SPI generates new, more meaningful events for display in the NNM Alarms Browser.
- Optionally, the MPLS VPN SPI automatically configures reachability tests for valid PE-PE router pairs within a VPN.
- The MPLS VPN SPI allows users to configure various types of PE- and CE-specific reachability tests and generates events to indicate changes in the tested connections.
- When applicable, the MPLS VPN SPI generates new events that relate changes in the label switch paths monitored by RAMS to MPLS VPN performance.
- When applicable, the MPLS VPN SPI provides cross-launching to MPLS VPN-specific OVPI reports.

Behavior of the MPLS VPN SPI

The MPLS VPN SPI detects and reports problems in your MPLS VPN network. The types of traps and events that the MPLS VPN SPI detects and analyzes include:

- Node and interface status change traps for PE routers
- Node and interface status change traps for CE routers
- Network core status events sent from a RAMS appliance within the managed network.
- Reachability status events for PE-PE, PE-CE, and CE-CE reachability tests
- OVPI threshold exceeded traps for MPLS VPN, SAA, and CAR threshold breaches

The MPLS VPN SPI enriches these traps and translates them into events regarding the VPN services they affect. These events identify the impacted VRFs in the VPN services.

User Interaction with the MPLS VPN SPI

Users can monitor the health of the MPLS VPN network in several ways:

- Monitor alarms in the MPLS VPN alarms category to observe status changes in one or more VPNs. See “MPLS VPN Events” on page 14.
- Examine graphical and tabular representations of the MPLS VPN network through the windows available in the MPLS VPN Views. See “MPLS VPN Views” on page 17.
- When RAMS is installed and integrated with NNM, monitor the status of the label switch paths in the MPLS VPN Views. See “MPLS VPN Views” on page 17.
- When OVPI and the MPLS VPN Report Pack are installed, create reports about the activity on the MPLS VPN network by cross-launching to OVPI. See “Reports from OVPI” on page 19.

MPLS VPN Events

The events that the MPLS VPN SPI generates appear in the MPLS VPN category of the NNM Alarms Browser. Double-click the MPLS VPN category to open the MPLS VPN browser.

When the MPLS VPN SPI detects an MPLS VPN fault, it generates one of the following events:

- MPLS/VPN: VPN:VRF [*VPN:VRF*] Down due to [*interface*] IF down on node [*node*].
- MPLS/VPN: VPN:VRF [*VPN:VRF*] Down due to [*interface*] IF Admin down on node [*node*].
- MPLS/VPN: VPN:VRF [*VPN:VRF*] Degraded due to [*interface*] IF down on node [*node*].
- MPLS/VPN: VPN:VRF(s) [*VPN1:VRF1,VPN2:VRF2,...*] Down due to node [*node*] down.
- MPLS/VPN: VPN:VRF(s) [*VPN1:VRF1,VPN2:VRF2,...*] Down due to Board [*board*] down.
- MPLS/VPN: VPN:VRF(s) [*VPN1:VRF1,VPN2:VRF2,...*] Unknown status due to node [*node*] unknown status

- MPLS/VPN: VPN:VRF [*VPN:VRF*] Down due to connection down between [*source_node:interface*] and [*destination_node:interface*]
- MPLS/VPN: SAA test failed between [*node1-node2*] affected VPN/VRF(s): [*VPN1:VRF1,VPN2:VRF2,...*]. Root cause is *cause*.
- MPLS/VPN: [*VPN:VRF*] Path Worse between [*node1*] and [*node2*].
- MPLS/VPN: [*VPN:VRF*] Path Better between [*node1*] and [*node2*].
- MPLS/VPN: SAA test cleared between [*node1-node2*] affected VPN/VRF(s): [*VPN1:VRF1,VPN2:VRF2,...*]
- MPLS/VPN: PingMib test failed between [*node1-node2*] affected VPN/VRF(s): [*VPN1:VRF1,VPN2:VRF2,...*]. Root cause is *cause*.
- MPLS/VPN: PingMib test cleared between [*node1-node2*] affected VPN/VRF(s): [*VPN1:VRF1,VPN2:VRF2,...*]

Some sample messages follow:

```
MPLS/VPN: VPN:VRF [Red_: Red_West] Down due to [Se0/0] IF down on node  
[mplspe04.cnd.hp.com]
```

```
MPLS/VPN: VPN:VRF [Red_: Red_West Blue:Blue] Down due to node  
[mplspe04.cnd.hp.com] down
```

```
MPLS/VPN: VPN:VRF [Red_: Red_West Blue:Blue] Down due to card [card1] down
```

```
MPLS/VPN: SAA test failed between [mplspe04.cnd.hp.com-mplspe01.cnd.hp.com]  
affected VPN/VRF:[Red_:Red_West-Red_East]. Root cause is Connectivity Failure  
between mplspe04.cnd.hp.com and mplspe01.cnd.hp.com.
```

```
MPLS/VPN: VPN:VRF [Red_: Red_West] Down due to [Se0/0] IF ADDRESS down on node  
[mplspe04.cnd.hp.com]
```

```
MPLS/VPN: VPN:VRF [Red_: Red_West] Down due to connection down between  
[mplspe04.cnd.hp.com:Se0/0] and [mplspe01.cnd.hp.com:Se0/0]
```

```
MPLS/VPN: VPN:VRF [Red_: Red_West] Unknown status due to node  
[mplspe04.cnd.hp.com] unknown status
```

The message field of an MPLS VPN alarm indicates the nature of the MPLS VPN fault that has occurred. It also contains these additional pieces of information:

- The list of affected VRFs in each VPN affected by the outage. An interface down condition affects only one VRF. A node down condition can impact multiple VRFs.

For example, [Red_: Red_West Blue:Blue] indicates that the outage affects the Red_West VRF on the Red_VPN and the Blue VRF on the Blue VPN.

- The node name of the edge router in outage. For example, [mplspe04.cnd.hp.com].

Or

The names of the edge router nodes for a reachability test. For example, [mplspe04.cnd.hp.com-mplspe01.cnd.hp.com].

- If applicable, the name of the interface in outage on the edge router. For example, [Se0/0].

MPLS VPN Views

The MPLS VPN SPI has several views available:

- **MPLS VPN View**—A list of the VPNs in the MPLS VPN network.
- **MPLS VPN Router Inventory**—A list of the MPLS VPN routers in the MPLS VPN network.
- **MPLS VPN Details**—Graph and table views of all accessible PE and CE routers in a specific VPN.
- **PE Details**—Descriptive information about the VRFs defined for a specific PE router, including the VPN in which each VRF participates.
- **VRF Details**—Descriptive information about the PE and CE routers in a specific VRF.

For information about the functionality available in each view and navigation among the views, see the online help installed with the MPLS VPN SPI.

Launching MPLS VPN Views

There are several ways to reach the MPLS VPN View:

- To open the MPLS VPN View from Home Base, select **MPLS VPN View** in the list, and then click **Launch**.
- To open the MPLS VPN View from any view, click **Tools:Views->MPLS VPN**.
- To open the MPLS VPN View from the NNM Alarms Browser, select an alarm in the MPLS VPN category, and then click **Action->Views:MPLS VPN**.

Many of the alarms that the MPLS VPN SPI generates connect to a specific view. Table 1-1 lists the alarms that provide context for launching a related view. To open a view that shows status information for the device or interface listed in an alarm, select that alarm in the Alarms Browser, and then click **Actions:Views->view_name**.

Table 1-1 Views Associated with MPLS VPN Alarms

Alarm	Available Views
OV_MPLS_VPN_IF_Down	VRF Details View
OV_MPLS_VPN_Node_Down	PE Details View for PE routers MPLS VPN Details view for CE devices
OV_MPLS_VPN_Node_Unknown	PE Details View for PE routers MPLS VPN Details view for CE devices
OV_MPLS_VPN_SAA_Fail	MPLS VPN View MPLS VPN Details Table PE Details
OV_MPLS_VPN_Addr_Down	VRF Details View
OV_MPLS_VPN_Conn_Down	VRF Details View
OV_MPLS_VPN_Board_Down	PE Details View
OV_MPLS_VPN_IFAdmin_Down	VRF Details View
OV_MPLS_VPN_PingMib_Fail	MPLS VPN View MPLS VPN Details Table PE Details
OV_MPLS_VPN_HSRP_IF_Down	VRF Details View
OV_MPLS_VPN_RAMC_Path_Down	RAMC Path History View
OV_MPLS_VPN_RAMC_Path_Become_Worse	RAMC Path History View

RAMS Integration

If you have deployed a RAMS appliance into the managed network and have installed the NNM / RAMS Integration Module, the MPLS VPN SPI can receive traps regarding PE-PE label switch path changes from the RAMS appliance.

There are multiple ways to cross-launch to the RAMS Path History View for a given PE-PE router pair:

- In the MPLS VPN Details graph, select two PE router symbols, right-click, and then click Show LSP.
- In the MPLS VPN Details graph, select one connection symbol (between two PE routers), right-click, and then click Show LSP.
- In the MPLS VPN Details table, select a row containing two PE router names, right-click, and then click Show LSP.

Reports from OVPI

If you have the MPLS VPN and SAA Report Packs installed on your OVPI server and you have installed the NNM / OVPI Integration Module, there are several ways in which you can launch OVPI from the MPLS VPN information in NNM. The following sections describe these ways.

Cross-Launching OVPI from the NNM Alarms Browser

To start OVPI from the NNM Alarms Browser, follow these steps:

1. Select an alarm in the MPLS VPN Alarms Browser, and then click Actions->Additional Actions.
2. In the Action list, click OVPI Report.
3. Click OK.

A web browser window appears containing an OVPI report, pre-filtered for the object that generated the alarm.

Cross-Launching OVPI from the NNM GUI (ovw)

To start OVPI from the NNM GUI (ovw), follow these steps:

1. On the NNM map, select a node or interface symbol for a router in the MPLS VPN network, and then click `Actions->Additional Actions`.
2. In the Action list, click `OVPI Report`.
3. Click `OK`.

A web browser window appears containing the `Report Launchpad`.

4. In the `Report Launchpad`, click the report to view.

Cross-Launching OVPI from the MPLS VPN View

To start OVPI from the MPLS VPN View, follow these steps:

1. In the MPLS VPN View, select `OVPI Report` in the list, and then click `Launch`.

A web browser window appears containing the `Report Launchpad`, in which you can select the report to view.

Related Documentation

Refer to the following documents for more information:

- *Managing Your Network with HP OpenView Network Node Manager*
- *Using Extended Topology*
- *Network Node Manager / Route Analytics Management System Integration Module User's Guide*
- *MPLS VPN Report Pack User Guide*
- *SAA Report Pack User Guide*

These documents are provided in Adobe Acrobat (.pdf) format, and can be found in the following places:

- NNM and NNM Smart Plug-in user guides and the release notes are copied to `$OV_WWW/htdocs/$LANG/` or `%OV_WWW%\htdocs\%LANG%\` on your NNM management station.
- OVPI and OVPI Report Pack user guides and the release notes are copied to the `/OVPI/Docs` directory on your OVPI server.
- All documents can be downloaded from the HP documentation web site located at:

`http://ovweb.external.hp.com/lpe/doc_serv/`

In the select product list, select one of the following names:

- reporting and network solutions
- nnm smart plug-in for mpls
- nnm and rams integration module
- performance insight
- network node manager

For more instructions, see the “Support” section of the *Release Notes for Reporting and Network Solutions*, which can be found in `$OV_WWW/htdocs/` or `%OV_WWW%\htdocs` on your NNM management station.

Introducing the MPLS VPN Smart Plug-in

Related Documentation

Preparing for Installation

Before installing the MPLS VPN Smart Plug-in (SPI), verify that your computer meets the hardware and software requirements, and that the prerequisite software has been set up properly.

Hardware Requirements

Verify that the following disk space settings are configured prior to installing the MPLS VPN SPI:

Table 2-1

Recommended Disk Space Settings

Location	Size
<i>UNIX:</i> \$OV_MAIN_PATH	15 MB
<i>Windows:</i> %OV_MAIN_PATH%	

Software Requirements

Supported Operating Systems

The following operating systems are supported:

- HP-UX 11.0 or HP-UX 11.11
- Solaris 2.8 or Solaris 2.9
- Microsoft® Windows® 2000 with service pack 3, Windows® XP, or Windows® 2003

Network Node Manager

Verify that the following software and all of its prerequisites and patches are installed on all systems in the managed environment:

- HP OpenView Network Node Manager Advanced Edition, version 7.5 with Consolidated Patch 2 or higher

Refer to the *Network Node Manager Installation Guide* for instructions on how to install the NNM product.

Optional Software

The MPLS VPN SPI integrates with the following optional software:

- HP OpenView Performance Insight (OVPI) version 5.0, installed on a separate server and meeting the following requirements:
 - Integrated with NNM using the NNM / OVPI Integration Module.
 - Includes one or more of the MPLS VPN and SAA Report Packs.
- HP OpenView Route Analytics Management System (RAMS) version 2.51, meeting the following requirements:
 - Integrated with NNM using the NNM / RAMS Integration Module.
 - Supports one or more of the OSPF and IS-IS protocols.

MIB Dependencies

The following MIBs must be loaded before the MPLS VPN SPI can function properly:

- Cisco SMI MIB—Shipped with NNM and installed to the following location:
UNIX: \$OV_SNMP_MIBS/Vendor/Cisco/CISCO-SMI.my
Windows: %OV_SNMP_MIBS%\Vendor\Cisco\CISCO-SMI.my
- Standard DISMAN PING MIB—Shipped with NNM and installed to the following location:
UNIX:
\$OV_SNMP_MIBS/Standard/rfc2925-DISMAN-PING-MIB.my
Windows:
%OV_SNMP_MIBS%\Standard\rfc2925-DISMAN-PING-MIB.my
- Cisco RTTMON MIB—Shipped with the MPLS VPN SPI and installed to the following location:
UNIX: /opt/OV/newconfig/MPLS/CISCO-RTTMON-MIB.my
Windows: %OV_CONF%\MPLS\CISCO-RTTMON-MIB.my

- Juniper SMI MIB—Shipped with the MPLS VPN SPI and installed to the following location:

UNIX: \$OV_NEWCONF/MPLS/jnx-smi.mib

Windows: %OV_CONF%\MPLS\jnx-smi.mib

- Juniper VPN MIB—Shipped with the MPLS VPN SPI and installed to the following location:

UNIX: \$OV_NEWCONF/MPLS/jnx-vpn.mib

Windows: %OV_CONF%\MPLS\jnx-vpn.mib

- Juniper Ping MIB—Shipped with the MPLS VPN SPI and installed to the following location:

UNIX: \$OV_NEWCONF/MPLS/jnx-ping.mib

Windows: %OV_CONF%\MPLS\jnx-ping.mib

If the Cisco SMI MIB is loaded onto the NNM management station before you install the MPLS VPN SPI, the MPLS VPN SPI installation process loads all other required MIBs. Otherwise, you must manually load all required MIBs. For information, see “Verifying That MIBs Are Loaded” on page 101.

NOTE

On the Windows operating system, the Typical NNM installation option does not load the Cisco SMI MIB. You can choose the Custom NNM installation option and specify to load the SNMP MIBs. Alternatively, you can load this MIB as described in “Verifying That MIBs Are Loaded” on page 101.

Router Requirements

This release of the MPLS VPN SPI discovers and manages the following types of router devices:

- Cisco routers with Internetwork Operating System (IOS) version 12.2(15)T that support MplsVpnMIB.
- Juniper M and T series routers with Juniper Operating System (JunOS) version 6 that support jnx-smi.mib, jnx-vpn.mib, and jnx-ping.mib.

- Any CE router with SNMP access that supports MIB-II. Configuration of Cisco SAA tests on a CE router requires that the CE router runs IOS version 12.2(15)T. Configuration of Juniper Ping tests on CE router requires that the CE runs JunOS version 6 or above.
- For optional core management through RAMS, each PE router must have a loopback address that participates in OSPF or IS-IS.

Updating from a Previous Version of the MPLS VPN SPI

If you have customized a previous version of the MPLS VPN SPI, read the sections appropriate to your installation before installing the current version of the MPLS VPN SPI.

Preserving Trap Customizations

If you have customized any of the trap definitions in the trapd.conf file, save a copy of this file. The MPLS VPN SPI overwrites the trapd.conf file.

After installing the MPLS VPN SPI, re-enter your customizations into the trapd.conf file. This file is located at:

- *UNIX*:
`$OV_CONF/$LANG/trapd.conf`
- *Windows*:
`%OV_CONF%\%LANG%\trapd.conf`

Preserving SAA Test Definitions

If you have defined SAA tests using a previous version of the MPLS VPN SPI, follow these steps to preserve your test configuration:

1. Delete the existing SAA test definitions from the managed routers:

a. Export all existing SAA tests into a file:

- *UNIX*:
`$OV_BIN/reachability_config.ovpl -e /tmp/saa_test_A`
- *Windows*:
`%OV_BIN%\reachability_config.ovpl -e C:\temp\saa_test_A`

For more information, see “Changing Reachability Test Definitions” on page 84.

- b. Using any text editor, in the `saa_test_A` file, change the `OP` parameter for each test definition to `DELETE`.

For more information, see “Configuring Reachability Tests Using the MPLS VPN SPI” on page 86.

- c. Import the updated SAA test definitions to the MPLS VPN SPI:

- *UNIX:*

```
$OV_BIN/reachability_config.ovpl -i  
/tmp/saa_test_A
```

- *Windows:*

```
%OV_BIN%\reachability_config.ovpl -i  
C:\temp\saa_test_A
```

For more information, see “Changing Reachability Test Definitions” on page 84.

- d. Save the `saa_test_A` file for future reference.

2. Back up the `VpnNames.txt` file:

- *UNIX:*

```
cp $OV_CONF/VpnNames.txt /tmp/VpnNames-A.txt
```

- *Windows:*

```
copy %OV_CONF%\VpnNames.txt C:\temp\VpnNames-A.txt
```

3. Remove the MPLS VPN SPI.

For instructions, see “Removing the MPLS VPN SPI” on page 39.

4. Install the newest version of the MPLS VPN SPI.

For instructions, see “Installing the MPLS VPN SPI” on page 33.

5. Verify that NNM has been configured with the SNMP set community string for each edge router that is the source of one or more SAA tests.

For instructions, see “Configuring SNMP Access” on page 43.

6. Trigger Extended Topology discovery to discover your network and perform MPLS VPN discovery. By default the MPLS VPN SPI configures all possible PE-PE VRF-unaware SAA tests for your network.

For instructions, see “Discovery Process” on page 48.

7. Update the newly-defined SAA test definitions to match the previous SAA test definitions:

- a. Export the automatically configured SAA tests into a file:

- *UNIX*:

```
$OV_BIN/reachability_config.ovpl -e  
/tmp/saa_test_B
```

- *Windows*:

```
%OV_BIN%\reachability_config.ovpl -e  
C:\temp\saa_test_B
```

For more information, see “Changing Reachability Test Definitions” on page 84.

NOTE

If there are no automatically configured SAA tests, the `saa_test_B` file will be empty. In this case, you can work directly in the `saa_test_A` file for steps b and c.

- b. As necessary, update the SAA test definitions file.

Using any text editor, compare the SAA tests defined in the `saa_test_B` file with those defined in the `saa_test_A` file (from step 1):

- Modify the tests in the `saa_test_B` file to match the corresponding tests in the `saa_test_A` file. Change the `OP` parameter for each test definition to `MODIFY`
- Add any additional tests defined in the `saa_test_A` file to the `saa_test_B` file. Change the `OP` parameter for each test definition to `ADD`.

NOTE

The MPLS VPN SPI version 2.0 (and later) allows for more SAA test types than does the MPLS VPN SPI version 1.0. It also uses hexadecimal numbers for identifying SAA tests. This is a change from the previous release. You will see these changes as you compare test definitions, but they do not affect this effort:

- The `saa_test_B` file includes a `TEST_TYPE` element. You do *not* need to add this element to the version 1.0 test definitions.
- The `OV_TAG` element uses hexadecimal notation in the `saa_test_B` file and decimal notation in the `saa_test_A` file. You do *not* need to change the tag value for version 1.0 test definitions.

For more information, see “Configuring Reachability Tests Using the MPLS VPN SPI” on page 86.

- c. Import the updated SAA test definitions to the MPLS VPN SPI:

- *UNIX*:

```
$OV_BIN/reachability_config.ovpl -i  
/tmp/saa_test_B
```

- *Windows*:

```
%OV_BIN%\reachability_config.ovpl -i  
C:\temp\saa_test_B
```

For more information, see “Changing Reachability Test Definitions” on page 84.

8. Verify that the VPN names used in the previous version are retained for the new version:

- a. Compare the backup file `VpnNames-A.txt` (from step 2) with the new VPN names file:

- *UNIX*: `$OV_CONF/VpnNames.txt`
- *Windows*: `%OV_CONF%\VpnNames.txt`

Updating from a Previous Version of the MPLS VPN SPI

- b. As necessary, edit the `VpnNames.txt` file to match the VPN names from the previous version. Change *only* the VPN names.

For more information, see “Changing VPN Names in the MPLS VPN SPI Configuration” on page 53.

Installing the MPLS VPN SPI

If you encounter problems while performing any of these installation steps, see Chapter 6, “Troubleshooting the MPLS VPN Smart Plug-in,” on page 91 or the *NNM Smart Plug-in for MPLS VPN Release Notes* for possible assistance.

IMPORTANT

If you are installing the MPLS VPN SPI for the first time, enable NNM Extended Topology before attempting to install the MPLS VPN SPI. For specific instructions, see the guide *Using Extended Topology* that was included with NNM Advanced Edition.

NOTE

If you are installing the MPLS VPN SPI over an existing installation of the MPLS VPN SPI, see “Updating from a Previous Version of the MPLS VPN SPI” on page 28 for specific instructions.

Installing the MPLS VPN SPI on a UNIX Operating System

To install the MPLS VPN SPI on a UNIX[®] operating system, follow these steps:

1. Log on to the NNM management station as user `root`.
2. Verify that the `LANG` environment variable is set to an appropriate value:

```
echo $LANG
```

The response should be `C` (for English) or another value appropriate to your locale.

3. Verify that the NNM environment variables are sourced properly.

For instructions, see “Setting the NNM Environment Variables” on page 98.

4. If you are using an Oracle database for the NNM data warehouse, follow these steps to configure Oracle for the MPLS VPN SPI:
 - a. `cd $OV_CONF/nmnet/topology/extensibility`
 - b. `cp UpdateColumn.xslt UpdateColumn.xslt.orig`
 - c. Using any text editor, delete the word `COLUMN` from line 36 of the `UpdateColumn.xslt` file.
5. Mount the Reporting and Network Solutions CD-ROM.
6. From the Reporting and Network Solutions CD-ROM directory, start setup

The installation script verifies that the target system has the correct version of NNM installed. If NNM is not installed, the installation script exits with an error. See “Handling Other Problems” on page 106 for more information.
7. Follow the instructions on the screen to install the MPLS VPN SPI.

For a list of the decisions you will be asked to make during the installation process, see “Installation Options” on page 36.

Installing the MPLS VPN SPI on a Windows Operating System

To install the MPLS VPN SPI on a Windows operating system, follow these steps:

1. Log on to the NNM management station as user administrator.
2. Verify that the `LANG` environment variable is set to an appropriate value:

```
echo %LANG%
```

The response should be `C` (for English) or another value appropriate to your locale.

3. Verify that the NNM environment variables are sourced properly.

For instructions, see “Setting the NNM Environment Variables” on page 98.

4. If you are using an Oracle database for the NNM data warehouse, follow these steps to configure Oracle for the MPLS VPN SPI:
 - a. **cd %OV_CONF%\nnmet\topology\extensibility**
 - b. **copy UpdateColumn.xslt UpdateColumn.xslt.orig**
 - c. Using any text editor, delete the word `COLUMN` from line 36 of the `UpdateColumn.xslt` file.
5. Insert the Reporting and Network Solutions CD-ROM into the CD-ROM drive.
6. The CD-ROM should start automatically. If it does not, go to the Reporting and Network Solutions CD-ROM directory, and then double-click `setup.bat`.

The installation script verifies that the target system has the correct version of NNM installed. If NNM is not installed, the installation script exits with an error. See “Handling Other Problems” on page 106 for more information.
7. Follow the instructions on the screen to install the MPLS VPN SPI. For a list of the decisions you will be asked to make during the installation process, see “Installation Options” on page 36.

Installation Options

Table 2-2 lists the decisions you will be asked to make during the installation process.

Table 2-2 **Installation Options for the MPLS VPN SPI**

Option	Description
List of product types to install	Select to install the NNM Smart Plug-ins.
List of SPIs to install	Select to install the MPLS VPN SPI.
Start MPLS VPN discovery?	<p>Type yes to initiate Extended Topology discovery including MPLS VPN discovery at the end of the installation.</p> <p>Type no to leave the MPLS VPN network undiscovered. If you enter no, The MPLS VPN network is not discover until the next time you run Extended Topology discovery. See “Discovery Process” on page 48.</p>
Configure SAA tests at the end of each MPLS VPN discovery cycle?	<p>Type yes to have the MPLS VPN SPI automatically update the SAA MIB on each managed Cisco PE router with the SAA test definitions after MPLS VPN discovery completes. If you enter yes, ensure that the SNMP configuration database contains the set community string for each Cisco PE router. See “Initial Configuration” on page 40.</p> <p>Type no to prevent automatic updates to the SAA MIBs. If you enter no, the MPLS VPN SPI updates the SAA MIB upon explicit command only. See “Reachability Test Configuration” on page 85.</p> <p>You can change the automatic configuration setting. See “MPLS VPN SPI Configuration File” on page 44.</p>
SAA test frequency	<p>Type the number of seconds between SAA test executions. The default value is 600 seconds (10 minutes).</p> <p>You can change the SAA test frequency. See “MPLS VPN SPI Configuration File” on page 44.</p>

Table 2-2 Installation Options for the MPLS VPN SPI (Continued)

Option	Description
SAA test timeout	<p>Type the number of milliseconds before an SAA test times out. The default value is 100 milliseconds.</p> <p>You can change the SAA test timeout value. See “MPLS VPN SPI Configuration File” on page 44.</p>
Configure PingMIB tests at the end of each MPLS VPN discovery cycle?	<p>Type yes to have the MPLS VPN SPI automatically update the ping MIB on each managed Juniper PE router with the ping MIB test definitions after MPLS VPN discovery completes. If you enter yes, ensure that the SNMP configuration database contains the set community string for each Juniper PE router. See “Initial Configuration” on page 40.</p> <p>Type no to prevent automatic updates to the ping MIBs. If you enter no, the MPLS VPN SPI updates the ping MIB upon explicit command only. See “Reachability Test Configuration” on page 85.</p> <p>You can change the automatic configuration setting. See “MPLS VPN SPI Configuration File” on page 44.</p>
PingMIB test frequency	<p>Type the number of seconds between ping MIB test executions. The default value is 600 seconds (10 minutes).</p> <p>You can change the ping MIB test frequency. See “MPLS VPN SPI Configuration File” on page 44.</p>
PingMIB test timeout	<p>Type the number of seconds before a ping MIB test times out. The default value is 1 second.</p> <p>You can change the ping MIB test timeout value. See “MPLS VPN SPI Configuration File” on page 44.</p>
PingMIB test poll interval	<p>Type the number of seconds between the polls for results from the ping MIB tests. The default value is 60 seconds (1 minute).</p> <p>You can change the ping MIB test polling interval. See “MPLS VPN SPI Configuration File” on page 44.</p>

Table 2-2 Installation Options for the MPLS VPN SPI (Continued)

Option	Description
Do you have a current license for NNM Advanced Edition (or are you evaluating the product)?	Type yes if NNM Advanced Edition is properly licensed for your scenario. Otherwise, type no .
Administrator User Id and Password	Type the user ID and password for the administrator login to NNM Advanced Edition. If you do not know this information, contact your network administrator.

Removing the MPLS VPN SPI

NOTE

Removing the MPLS VPN SPI does not delete the MPLS VPN alarms from the NNM Alarms Browser. When you no longer need these alarms, delete them manually using the delete functionality in the Alarms Browser.

Removing the MPLS VPN SPI on a UNIX Operating System

To remove the MPLS VPN SPI on a UNIX operating system, follow these steps:

1. Log on to the NNM management station as user `root`.
2. Unconfigure and remove the MPLS VPN SPI:

```
mpls_unconfig.ovpl
```

3. On the Solaris operating system *only*, type the commands:

```
/usr/sbin/pkgrm HPOvMPLS  
/usr/sbin/pkgrm HPOvCisMPLSagt
```

Removing MPLS VPN SPI on a Windows Operating System

To remove the MPLS VPN SPI on a Windows operating system, follow these steps:

1. Log on to the NNM management station as user `administrator`.
2. Unconfigure and remove the MPLS VPN SPI:

```
mpls_unconfig.ovpl
```

Initial Configuration

The MPLS VPN SPI uses NNM Advanced Edition functionality to monitor the health of the virtual private networks in a multiprotocol label switching (MPLS VPN) environment. To ensure smooth SNMP communication between the MPLS VPN SPI and the managed MPLS VPN routers, read each topic in this section and perform the appropriate configuration steps.

Configuring SNMP Polling Access

The MPLS VPN SPI relies on NNM knowing the correct status of the nodes and interfaces of the provider edge (PE) and customer edge (CE) routers in the MPLS VPN network. NNM determines this status information using the active polling analyzer (APA) *or* netmon.

Follow the steps in the topic appropriate for your NNM configuration.

Configuration SNMP Polling Access for APA

The APA must be aware of and able to reach each node and interface.

To configure SNMP polling access to the edge routers, follow these steps:

1. For each interface card, determine the configuration action required:
 - If the interface card has an IP address that can be reached directly from the management station, verify that the interface card is shown in the NNM topology view.

The APA uses ICMP echo requests to determine the status of these interface cards. You do not need to do any additional configuration work.
 - If the interface card has an IP address that is *not* directly reachable from the management station, add the IP address to the APA no polling list as described in step 2.
 - If the interface card does *not* have an IP address, add the IP address of the managed interface to the APA no polling list as described in step 2.

2. As determined in step 1, add IP address information to the APA no polling list. The APA ignores these addresses because it is unable to reach them. The files involved in this configuration are as follows:

- *UNIX:*

```
$OV_CONF/nnet/topology/filter/TopoFilters.xml  
$OV_CONF/nnet/paConfig.xml
```

- *Windows:*

```
%OV_CONF%\nnet\topology\filter\TopoFilters.xml  
%OV_CONF%\nnet\paConfig.xml
```

The following steps present a high level view of the procedure for configuring the APA no polling list. For detailed instructions on this process, see the section “Disable APA from Using ICMP to Poll Specific Addresses” in the chapter “Using the Active Problem Analyzer” of the *Using Extended Topology* guide.

- a. Create a backup copy of the `TopoFilters.xml` file.
- b. Using any text editor, in the `TopoFilters.xml` file, add the IP addresses you do not want APA to poll.
- c. Create a backup copy of the `paConfig.xml` file.
- d. Using any text editor, in the `paConfig.xml` file, uncomment the `NoPingAddresses` section and enter the appropriate values.

Configuring SNMP Polling Access for netmon

netmon must be aware of and able to reach each node and interface.

To configure SNMP polling access to the edge routers, follow these steps:

1. For each interface card, determine the configuration action required:

- If the interface card has an IP address that can be reached directly from the management station, verify that the interface card is shown in the NNM topology view.

netmon uses ICMP echo requests to determine the status of these interface cards. You do not need to do any additional configuration work.

- If the interface card has an IP address that is *not* directly reachable from the management station, add the IP address to the `netmon.snmpStatus` file as described in step 2.

- If the interface card does *not* have an IP address, add the IP address of the managed node to the `netmon.snmpStatus` file as described in step 2.
2. As determined in step 1, add IP address information to the `netmon.snmpStatus` file. `netmon` uses SNMP requests of the `ifIndex`, `ifOperStatus`, and `ifAdminStatus` MIB objects to determine the status of these interface cards.

The `netmon.snmpStatus` file is located in the following directory:

UNIX: `$OV_CONF`

Windows: `%OV_CONF%`

- a. If the `netmon.snmpStatus` file does not exist, create it in the specified directory.
- b. If possible, add IP address wildcards to cover multiple IP addresses that cannot be reached directly from the NNM management station.

Use a single line for each IP address wildcard entry.

- c. As needed, add specific IP addresses for interface cards and managed nodes that are not part of the specified IP address wildcards.

Use a single line for each specific IP address entry.

- d. See `netmon.snmpStatus` in the UNIX manpages or the Windows online help for more information on this file.

Configuring SNMP Read/Write Access on Juniper Routers

All remote operation MIBs that the JunOS software supports require that the SNMP clients have read-write privileges. The default SNMP configuration of Juniper routers is read-only. For information on enabling read-write access to the JunOS MIBS, see:

<http://www.juniper.net/techpubs/software/junos/junos64/swconfig64-net-mgmt/html/snmp-remote-operations4.html>

Configuring SNMP Access

The MPLS VPN SPI requires SNMP access to the managed devices in the MPLS VPN environment

NOTE

This access is a requirement for automatic configuration of PE-PE VRF-unaware reachability tests. If you do not specify the set community string for an edge router, you must specify it for each test definition in the reachability test definitions file and run a command line tool to configure these tests on the router. For instructions, see “Configuring Reachability Tests Using the MPLS VPN SPI” on page 86.

Alternatively, on Cisco routers, you can directly configure the SAA echo tests for that router. For instructions, see “Configuring SAA Using the Cisco IOS Commands” on page 88.

To configure the SNMP configuration database with SNMP set community strings for all edge routers, follow these steps:

1. Start the SNMP configuration utility:

- *UNIX:* `$OV_BIN/xnmsnmpconf`
- *Windows:* `%OV_BIN%\xnmsnmpconf`

2. In the SNMP Configuration window, specify the set community string for each edge router.

See `xnmsnmpconf` in the UNIX manpages or the Windows online help for more information.

Configuring SNMP Trap Forwarding

The MPLS VPN SPI must receive traps from the managed edge devices in order to determine the operational and reachability status for these routers.

Configure each edge router to include the NNM management station as one of the SNMP trap recipients. For information about how to perform this configuration, see the documentation that came with your routers.

MPLS VPN SPI Configuration File

The MPLS VPN SPI installation process sets the values of several parameters that control the product's behavior. These parameters are stored in the file:

- *UNIX*: `$OV_CONF/mpls.conf`
- *Windows*: `%OV_CONF%\mpls.conf`

Figure 2-1 shows a sample `mpls.conf` file.

Figure 2-1

Sample `mpls.conf` File

```
SAA_TRIG=true
FREQUENCY=600
TIMEOUT=100
PINGMIB_TRIG=true
PINGMIBFREQ=600
PINGMIBTIMEOUT=1
PINGMIBPOLLINTERVAL=60
HANDLE_ADDR_EVENTS
```

The parameters in the `mpls.conf` file are as follows:

- `SAA_TRIG`—Determines whether the SAA reachability configuration process runs after MPLS VPN discovery completes. Possible values are `true` and `false`.
- `FREQUENCY`—Sets the default frequency (in seconds) for SAA reachability tests to run. If a reachability test definition for a Cisco router does not specify a frequency, the MPLS VPN SPI configures that reachability test with this frequency value.
- `TIMEOUT`—Sets the default timeout value (in milliseconds) for SAA reachability tests. If a reachability test definition for a Cisco router does not specify a timeout, the MPLS VPN SPI configures that reachability test with this timeout value.
- `PINGMIB_TRIG`—Determines whether the PingMIB reachability configuration process runs after MPLS VPN discovery completes. Possible values are `true` and `false`.

- `PINGMIBFREQ`—Sets the default frequency (in seconds) for ping MIB reachability tests to run. If a reachability test definition for a Juniper router does not specify a frequency, the MPLS VPN SPI configures that reachability test with this frequency value.
- `PINGMIBTIMEOUT`—Sets the default timeout value (in seconds) for ping MIB reachability tests. This value must be in the range of 1-15 seconds. If a reachability test definition for a Juniper router does not specify a timeout, the MPLS VPN SPI configures that reachability test with this timeout value.
- `PINGMIBPOLLINGINTERVAL`—Sets the time (in seconds) between polls of the ping MIB on Juniper routers to determine the current status of configured ping MIB tests.
- `HANDLE_ADDR_EVENTS`—Determines whether the MPLS VPN SPI handles the `OV_APA_ADDR_DOWN` and `OV_APA_ADDR_UP` events. By default, the MPLS VPN SPI ignores the address down and address up events. To enable the MPLS VPN SPI for receiving the address down and address up events, include the `HANDLE_ADDR_EVENTS` parameter in the `mpls.conf` file. This parameter takes no arguments.

To change the values of the MPLS VPN SPI configuration parameters:

- Using any text editor, edit the `mpls.conf` file to contain the desired values.

The MPLS VPN SPI reads the `mpls.conf` file each time it performs reachability test configuration and each time it receives an `OV_APA_ADDR_DOWN` or `OV_APA_ADDR_UP` event.

NOTE

Changing the value of the `FREQUENCY` or `TIMEOUT` parameters affects new or modified reachability test definitions only. Existing reachability test definitions do not change.

Installing the MPLS VPN Smart Plug-in
MPLS VPN SPI Configuration File

Discovery Process

The MPLS VPN Smart Plug-in (SPI) determines which routers in the Network Node Manager (NNM) topology support virtual private networks using multiprotocol label switching (MPLS VPN). The MPLS VPN SPI performs SNMP queries of the router devices to determine the provider edge (PE) router configuration and virtual route forwarding (VRF) groupings. Additionally, it uses subnet information in the Extended Topology database to identify the interfaces in each customer network that are connected to the PE routers in the managed network and identifies these as customer edge (CE) routers.

NOTE

If the CE routers are not included in the NNM management domain, the MPLS VPN SPI cannot determine the PE-CE relationships.

The MPLS VPN SPI generates the information that the MPLS VPN views use to display a model of the MPLS VPN network. This model contains the following information:

- Details about the PE routers:
 - VRF details
 - Interface-to-VRF relationships
 - Route target import/export lists
- Details about the outward-facing interface cards on the PE routers:
 - The interface number
- Details about the outward-facing interfaces on the CE routers that connect to one or more PE routers:
 - The interface number
- Details about the VRF/VPN configurations:
 - The relationships among the VRFs

MPLS VPN discovery is integrated with the Extended Topology discovery of NNM Advanced Edition. The MPLS VPN discovery agent processes are `ovet_daCiscoMplsVpn` and `ovet_daJunMplsVpn`. These processes run whenever the Extended Topology discovery runs.

To modify the Extended Topology discovery configuration, or to initiate Extended Topology, use the Configure Extended Topology window in NNM Advanced Edition. For more information, see the guide *Using Extended Topology* that was included with NNM Advanced Edition.

VPN Naming Algorithm

Each VRF object includes a list of import and export route targets that identify other VRFs in the MPLS VPN network. The MPLS VPN SPI reads the route targets in these import and export lists to identify groups of VRF neighbors. These relationships determine which routes through the MPLS VPN network must be tested to assure adequate service for your intranet customers.

VRFs that can be linked directly or indirectly by their neighbor relationships are considered to be in the same VPN. This approach enables the MPLS VPN SPI to correctly discover simple network topologies that are fully meshed as well as complex network topologies that are of a hub and spoke design.

The MPLS VPN SPI stores the VRF grouping relationships and the VPN names in the `VpnNames.txt` file. This file is described in “Changing VPN Names in the MPLS VPN SPI Configuration” on page 53.

The MPLS VPN SPI attempts to assign a meaningful VPN name to each discovered VRF group according to the following rules:

1. If the discovered VRF group matches a VRF group stored in the `VpnNames.txt` file, then continue to use the VPN name for the stored VRF group.

A discovered VRF group matches a stored VRF group if one or more VRFs exists in both VRF lists.

2. If the discovered VRF group does not match a VRF group stored in the `VpnNames.txt` file, then examine the individual VRF names for each VRF in the group to create a new VPN name:
 - If at least 65 percent of the VRFs in the group have the same name and that name would be a unique VPN name, then assign that text string as the VPN name for the VRF group.
 - If at least 65 percent of the VRFs in the group have the same name and that name is already a VPN name for another VRF list, then assign the VPN name as the VRF name appended with an underscore followed by the VPN internal identification number for this VRF group.

3. If at least the first three characters of each name in the VRF group match, then set the VPN name to be the string formed by the maximum number of initial matching characters.

This rule assumes that this name is not already assigned to a different VRF group.

4. If none of the preceding rules applies, set the VPN name to be the string `NoCommonName_` followed by the VPN internal identification number.

To change a VPN name, manually edit the `VpnNames.txt` file to change the VPN name to something meaningful for your network as described in “Changing VPN Names in the MPLS VPN SPI Configuration” on page 53.

NOTE

The MPLS VPN SPI does not identify or support any VPN that contains only one VRF.

Table 3-1 shows several applications of the VPN naming algorithm.

Table 3-1 Sample VPN Naming Applications

VRFs in the VPN	Selected VPN Name	Explanation
Blue Blue	Blue	All VRF names are the same; choose that name
Blue Green Green Green	Green	75 percent match among VRF names; choose the majority name
Red_East Red_West	Red_	The common initial characters

Table 3-1 **Sample VPN Naming Applications (Continued)**

VRFs in the VPN	Selected VPN Name	Explanation
Red_North Red_South	Red_5	The common initial characters with underscore and the VPN internal identifier appended for uniqueness
Blue Green Yellow	NoCommonName_1	VRF names cannot be matched or formed into a meaningful name

Changing VPN Names in the MPLS VPN SPI Configuration

The MPLS VPN SPI stores the VRF grouping relationships and their associated VPN names in the file:

- *UNIX*: `$OV_CONF/VpnNames.txt`
- *Windows*: `%OV_CONF%\VpnNames.txt`

You can modify this file to customize the VPN names. The format of the `VpnNames.txt` file is as follows:

```
VpnName VPN_Internal_Id VrfList
```

The separator between entries is a single tab. No additional white space is allowed.

The `VrfList` may contain multiple entries. Each entry specifies the name of a PE router and a VRF on that router. Each entry in the `VrfList` is in the following format:

```
DeviceName<<>>VrfName DeviceName<<>>VrfName
```

The separator between the router and VRF names is the string `<<>>`. The separator between entries in the `VrfList` is a single tab.

The `DeviceName` can be an IP address or a hostname. The value of the `DeviceName` comes from NNM's topology database.

Figure 3-1 shows a sample `VpnNames.txt` file.

Figure 3-1 Sample `VpnNames.txt` file

```
Blue 1 Device1<<>>Blue Device2<<>>Blue Device3<<>>Blue
NoCommonName_2 2 Device3<<>>Red Device4<<>>Green
Device5<<>>Purple
Cust 3 Device6<<>>CustEast Device7<<>>CustWest
Device8<<>>CustNorth Device9<<>>CustSouth
```

To change an assigned VPN name:

- Using any text editor, edit the `VpnNames.txt` file:
 1. Change each VPN name that contains the string `NoCommonName_` to a meaningful name for that network.
 2. Change other VPN names as desired.

WARNING

Modify the values for the `vpnName` field only. Changes to other fields in this file result in the entire file being discarded.

Ignoring Management Route Targets

Some network administrators include a management route target that touches most or all of the VPNs in the network. This management route target allows management traffic to flow within the MPLS VPN network and appears to the MPLS VPN SPI to be a single, large VPN.

You can configure a list of route targets that comprise the management route. The MPLS VPN SPI ignores the listed management routes when computing VPN relationships.

The following configuration file includes a list of management routes that the MPLS VPN SPI should ignore during discovery:

- *UNIX*: \$OV_CONF/nmet/agents/MplsVpn.cfg
- *Windows*: %OV_CONF%\nmet\agents\MplsVpn.cfg

Figure 3-2 shows the section of the `MplsVpn.cfg` file that creates a list of management routes to be ignored.

Figure 3-2

Default MPLS Route Target Ignore Table Configuration Script

```
create table mplsStore.mplsRTIgnore
(
    m_vrfrtIgnore    text not null,
    unique(m_vrfrtIgnore)
);

insert into mplsStore.mplsRTIgnore
(
    m_vrfrtIgnore
)
values
(
    '12345:10003'
);
```

To configure one or more route targets that the MPLS VPN SPI should ignore during discovery:

1. Using any text editor, edit the `MplsVpn.cfg` file:
 - a. Uncomment the `mplsStore.mplsRTIgnore` section by deleting the `//` at the beginning of each row.
 - b. Replace the sample text `12345:1003` with the route target identifier for the management route. The route target identifier must be contained within single quotations marks.
 - c. To include multiple route targets that should be ignored, insert additional route target identifier insert statements. Each route target identifier must be in a separate statement as shown in Figure 3-3.

Figure 3-3 Example of Multiple Route Target Configurations

```
create table mplsStore.mplsRTIgnore
(
    m_vrfrtIgnore    text not null,
    unique(m_vrfrtIgnore)
);

insert into mplsStore.mplsRTIgnore
(
    m_vrfrtIgnore
)
values
(
    '29975:10002'
);

insert into mplsStore.mplsRTIgnore
(
    m_vrfrtIgnore
)
values
(
    '29975:10003'
);
```


2. Remove the `VpnNames.txt` file from the following directory:

- *UNIX*: `$OV_CONF`
- *Windows*: `%OV_CONF%`

The MPLS VPN SPI will recreate the `VpnNames.txt` file at the next discovery process.

3. Run the Extended Topology discovery. For more information, see the guide *Using Extended Topology* that was included with NNM Advanced Edition.

MPLS VPN Status Manager

The status manager for the MPLS VPN Smart Plug-in (SPI) receives specific SNMP events from the HP OpenView event subsystem. It then generates new, enriched SNMP events that relate the situation in the event to the virtual private networks (VPNs) in the network. The status manager configures the Pairwise correlation in Network Node Manager (NNM) to clear enriched events from the NNM Alarms Browser when appropriate.

The MPLS VPN SPI status manager processes (`MPLS_sm` and `MPLS_pp`) are NNM services managed by `ovspmd`. They log status messages into the standard NNM log file:

- *UNIX*: `$OV_LOG/System.txt`
- *Windows*: `%OV_LOG%\System.txt`

For information about the enriched events that the MPLS VPN SPI generates, see the following sections:

- “Router Status Events” on page 61
- “Network Core Status Events” on page 65
- “Reachability Status Change Events” on page 67
- “OVPI Report Pack Threshold Events” on page 71

Router Status Events

This section describes the events that the MPLS VPN SPI generates regarding the proper functioning of an edge router in a virtual private network in a multiprotocol label switching (MPLS VPN) environment.

The MPLS VPN SPI connects to the HP OpenView event subsystem to receive events about status changes of the provider edge (PE) and customer edge (CE) routers in the managed MPLS VPNs. When the MPLS VPN SPI receives an event regarding a status change of a CE-facing interface on a PE router or a PE-facing interface on a CE router, it generates a new event that describes the root cause of the change. The MPLS VPN SPI also listens for each event describing a change in status of PE or CE router interface cards or nodes and generates an event for each of these changes.

The MPLS VPN SPI generates new device status events that are enriched with information specific to the MPLS VPN network. The NNM Alarms Browser displays these enriched events in the MPLS VPN category.

By default, the MPLS VPN SPI receives events from the netmon process only. If you configure NNM to receive events from the active problem analyzer (APA), the MPLS VPN SPI receives events from the APA instead of from the netmon process. To change the input event source for NNM, use the `ovet_apaConfig.ovpl` command. For more information, see the guide *Using Extended Topology* that was included with NNM Advanced Edition.

Table 4-1 lists and describes the device status events that the MPLS VPN SPI generates. The format of these events is described in “MPLS VPN Events” on page 14. For information about the variable bindings associated with an event, see the `trapd.conf` file in the following directory:

```
UNIX: $OV_CONF/C  
Windows: %OV_CONF%\C
```

Router Status Events

Table 4-1 Enriched Router Status Events Generated by the MPLS VPN SPI

Enriched Event Name/ HP OpenView Event OID	Meaning	Input Event Name/ HP OpenView Event OID	Input Event Source
OV_MPLS_VPN_IF_Down/ 70001000	A CE-facing interface configured for the MPLS VPN on a PE router is down.	OV_APA_IF_DOWN/ 5893012	APA
		OV_IF_Down/ 58916867	netmon
OV_MPLS_VPN_IFAdmin_Down/ 70001014	A CE-facing interface configured for the MPLS VPN on a PE router is down for administrative purposes.	OV_APA_IF_Admin_Down/ 40000088	APA
OV_MPLS_VPN_HSRP_IF_Down/ 70001017	A CE-facing interface configured for the MPLS VPN on a PE router has been switched to the PE router's HSRP backup device.	OV_APA_IF_DOWN/ 5893012	APA
		OV_IF_Down/ 58916867	netmon
None; clears the OV_MPLS_VPN_IF_Down, OV_MPLS_VPN_IFAdmin_Down, or OV_MPLS_VPN_HSRP_IF_Down event from the Alarms Browser	A CE-facing interface configured for the MPLS VPN on a PE router is back up.	OV_APA_IF_UP/ 5893002	APA
		OV_IF_Up/ 58916866	netmon
OV_MPLS_VPN_Node_Down/ 70001002	A PE router is down.	OV_APA_NODE_DOWN/ 58983013	APA
		OV_Node_Down/ 58916865	netmon

Table 4-1 Enriched Router Status Events Generated by the MPLS VPN SPI

Enriched Event Name/ HP OpenView Event OID	Meaning	Input Event Name/ HP OpenView Event OID	Input Event Source
None; clears the OV_MPLS_VPN_Node_ Down event from the Alarms Browser	A PE router is back up.	OV_APA_NODE_UP/ 58983003	APA
		OV_Node_Up/ 58916864	netmon
OV_MPLS_VPN_Board_ Down/ 70001013	A card with a VRF-enabled interface in the affected VPN is down. This interface might be on a PE or a CE within the VPN.	OV_APA_CARD_DOWN/ 58983035	APA
None; clears the OV_MPLS_VPN_Board_ Down event from the Alarms Browser	A card with a VRF-enabled interface is back up.	OV_APA_CARD_UP/ 58983034	APA
OV_MPLS_VPN_Conn_ Down/ 70001011	The connection between two interface cards on devices in the affected VPN is not functioning correctly.	OV_APA_CONNECTION_DOWN/ 58983014	APA
None; clears the OV_MPLS_VPN_Conn_ Down event from the Alarms Browser	The connection between two interface cards is now functioning correctly.	OV_APA_CONNECTION_UP/ 58983004	APA

Router Status Events

Table 4-1 Enriched Router Status Events Generated by the MPLS VPN SPI

Enriched Event Name/ HP OpenView Event OID	Meaning	Input Event Name/ HP OpenView Event OID	Input Event Source
OV_MPLS_VPN_Node_Unknown/ 70001004	The status of an intermediate device in the VRF path cannot be determined.	OV_TOPOLOGY_Status_Change_Notification/ 60001101	netmon
OV_MPLS_VPN_Addr_Down/ 70001009 NOTE: This alarm is <i>off</i> by default. See “MPLS VPN SPI Configuration File” on page 44 for more information.	An interface card on a device in the affected VPN is not responding to a ping request of its IP address.	OV_APA_ADDR_DOWN/ 58983011	APA
None; clears the OV_MPLS_VPN_Addr_Down event from the Alarms Browser	An interface card is now responding to a ping request of its IP address.	OV_APA_ADDR_UP/ 58983001	APA

Network Core Status Events

The HP OpenView Route Analytics Management System (RAMS appliance) monitors the status of the label switch paths between PE router pairs within the core of the managed network and sends a `rexRouteChange` trap each time the status of a monitored path changes. When RAMS is integrated with NNM and the RAMS watch list is correctly configured, the MPLS VPN SPI receives the SNMP trap and sends a new, enriched trap describing the change in status to NNM.

The watch list for the `rexRouteChange` event defines the source and destination router pairs for which NNM receives traps from RAMS. NNM ignores any source and destination router pair that is not included in a watch list. Thus, to effectively monitor the paths between PE routers, each PE-PE router pair must be included in the watch list for the `rexRouteChange` event. This configuration must be bilateral. For example, for the PE-PE router pair PE1 and PE2, the watch list for the `rexRouteChange` event must be configured as shown in Table 4-2.

Table 4-2

Sample `rexRouteChange` Watch List Configuration

Source Router	Destination Router
PE1	PE2
PE2	PE1

Acceptable values for the router identification are hostname and IP address. All PE routers in the watch list must have loopback addresses that participate in OSPF or IS-IS. For specific information about configuring a watch list, click the “Solutions” icon (building blocks) in the the web-based online help for NNM (URL:

`http://nnm_mgmt_station:3443/OvCgi/OvWebHelp.exe`).

Table 4-3 lists and describes the device status events that the MPLS VPN SPI generates. The format of these events is described in “MPLS VPN Events” on page 14. For information about the variable bindings associated with an event, see the `trapd.conf` file in the following directory:

UNIX: `$OV_CONF/C`
Windows: `%OV_CONF%\C`

Table 4-3 **Enriched Network Core Status Events Generated by the MPLS VPN SPI**

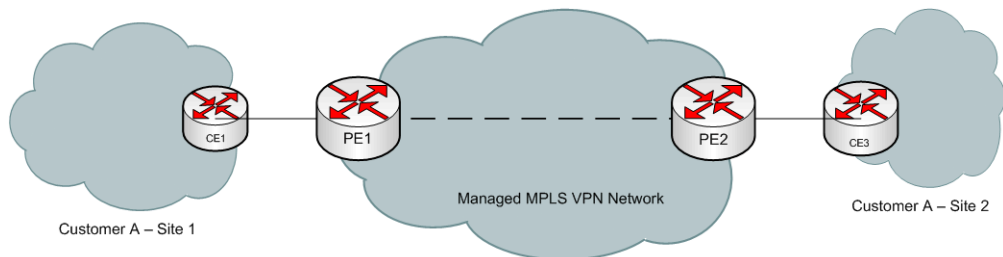
Enriched Event Name/ HP OpenView Event OID	Meaning
OV_MPLS_VPN_RAMs_Path_Down/ 70001018	The path between two PE routers is down.
None; clears the OV_MPLS_VPN_RAMs_Path_Down event from the Alarms Browser	The path between two PE routers is back up.
OV_MPLS_VPN_RAMs_Path_Worse/ 70001020	The status of the path between two PE routers is more severe than last reported.
OV_MPLS_VPN_RAMs_Path_Better/ 70001021	The status of the path between two PE routers is less severe than last reported.

Reachability Status Change Events

The MPLS VPN SPI generates new reachability status change events that are enriched with information specific to the MPLS VPN network. The NNM Alarms Browser displays these enriched events in the MPLS VPN category.

The MPLS VPN SPI configures reachability tests between routers in the MPLS VPN network and listens for the resulting SNMP traps. When one of these traps indicates a change to the reachability status, the MPLS VPN SPI generates a reachability status change event. Figure 4-1 shows an example of a path through an MPLS VPN network.

Figure 4-1 **Reachability Test Path Example**



The MPLS VPN SPI supports reachability tests of the following paths:

- PE router to PE router (for example, PE1 to PE2)
- PE router to the near CE router (for example, PE1 to CE1)
- CE router to CE router (for example CE1 to CE3)

Reachability Status Change Events

Table 4-4 lists the enriched events that the MPLS VPN SPI generates for reachability test conditions. The format of these events is described in “MPLS VPN Events” on page 14. For information about the variable bindings associated with an event, see the `trapd.conf` file in the following directory:

UNIX: \$OV_CONF/C

Windows: %OV_CONF%\C

Table 4-4 Enriched Reachability Status Events Generated by the MPLS VPN SPI

Enriched Event Name/ HP OpenView Event OID	Meaning	Notes
OV_MPLS_VPN_SAA_FAIL/ 70001006	The connection between two devices is down	Received the <code>rttMonTimeout Notification trap</code> with <code>rttMonCtrlOperTimeoutOccurred/.1.3.6.1.4.1.9.9.42.1.2.9.1.6 = TRUE</code>
OV_MPLS_VPN_SAA_PASS/ 70001007 Clears the OV_MPLS_VPN_SAA_FAIL event from the Alarms Browser	The connection between two devices is back up	Received the <code>rttMonTimeout Notification trap</code> with <code>rttMonCtrlOperTimeoutOccurred/.1.3.6.1.4.1.9.9.42.1.2.9.1.6 = FALSE</code>
OV_MPLS_VPN_PingMib_Fail/ 70001015	The connection between two devices is down.	The MPLS VPN SPI status manager noted a test failure in the ping MIB on the router
OV_MPLS_VPN_PingMib_Pass/ 70001016 Clears the OV_MPLS_VPN_PingMib_Fail event from the Alarms Browser.	The connection between two devices is back up.	The MPLS VPN SPI status manager noted a test success replacing a failure in the ping MIB on the router

Cisco Router Reachability Tests

For Cisco routers, the MPLS VPN SPI uses the Cisco Internetwork Operating System (IOS) Service Assurance Agent (SAA) for reachability tests. Each test is an ICMP echo request from one PE or CE router to another PE or CE router in the VPN. The SAA calculates the round trip time of its echo request. If the round trip time exceeds the timeout value for that test, the SAA indicates the test failure by sending a copy of the `rttMonTimeoutNotification` trap with the value of the `rttMonCtrlOperTimeoutOccurred` variable binding set to `TRUE`. The MPLS VPN SPI receives the SNMP trap and sends a new, enriched trap describing the SAA test failure to NNM.

If the failed SAA test was a test of the entire path between two CE routers, the MPLS VPN SPI triggers NNM to poll the interfaces on the affected VRF to determine the point of failure within that path. It then sends a new, enriched trap that identifies the specific failure to NNM.

If the SAA test succeeds, the SAA indicates the test success by sending a copy of the `rttMonTimeoutNotification` trap with the value of the `rttMonCtrlOperTimeoutOccurred` variable binding set to `FALSE`. The MPLS VPN SPI receives the SNMP trap and, if this trap follows an SAA failure trap, sends a new, enriched trap describing the reachability change in status to NNM. This new event clears the SAA failure event from the NNM Alarms Browser.

Juniper Router Reachability Tests

For Juniper routers, the MPLS VPN SPI uses the Juniper ping MIB for reachability tests. Each test is configured as a row in the `pingCtlTable` of the ping MIB. The Juniper operating system runs the ping MIB tests and stores the test results in the `pingCtlTable`. The MPLS VPN SPI status manager (MPLS_pp process) periodically polls the `pingCtlTable` on each Juniper router to determine the status of the ping MIB tests. For each failed ping MIB test, the MPLS VPN SPI sends a trap describing the ping MIB test failure to NNM.

If the failed ping MIB test was a test of the entire path between two CE routers, the MPLS VPN SPI triggers NNM to poll the interfaces on the affected VRF to determine the point of failure within that path. It then sends a new, enriched trap that identifies the specific failure to NNM.

Reachability Status Change Events

For each successful ping MIB test that follows a failed ping MIB test, the MPLS VPN SPI sends a trap describing the reachability change in status to NNM. This new event clears the ping MIB failure event from the NNM Alarms Browser.

OVPI Report Pack Threshold Events

When OVPI and the MPLS VPN Report Pack are installed, the MPLS VPN SPI receives several threshold events from OVPI. The MPLS VPN SPI posts these events to the MPLS VPN Performance category in the NNM Alarms Browser. It does not add any information to these events.

Table 4-5 lists and describes the threshold events that the MPLS VPN SPI receives from OVPI.

Table 4-5 **MPLS VPN Threshold Events from OVPI**

OVPI Event Name	Meaning
VPN_INTERFACEAVAIL_PCT	The average availability of all interfaces in the VPN is below the acceptable threshold.
VPN_DISCARD_PCT	The average packet discard percentage of all interfaces in the VPN is above the acceptable threshold.
VPN_ERROR_PCT	The average packet error percentage of all interfaces in the VPN is above the acceptable threshold.
VPN_SNMPRESPONSE	The average SNMP response from OVPI to the device/interface of all interfaces in the VPN is above the acceptable threshold.
VRF_OPERSTATUS	A VRF is in a non-operational status.

5 **Configuring Reachability Tests**

Reachability Tests

Some routers embed an SNMP agent to perform active monitoring of network health and to verify that service level agreements are being met. The values of the agent's test MIB determine the monitoring configuration for that device. You can configure the agent to perform differently on each router in the network.

The MPLS VPN SPI configures the router agents to test the reachability of each provider edge-provider edge (PE-PE) router pair in a virtual private network in a multiprotocol label switching (MPLS VPN) environment. If a reachability test times out, the router agent sends an SNMP trap to Network Node Manager (NNM). The MPLS VPN SPI receives this trap from the HP OpenView event subsystem, enriches it with information about the MPLS VPN network, and displays the event in the NNM Alarms Browser.

“Reachability Status Change Events” on page 67 describes how the MPLS VPN SPI processes these traps.

The MPLS VPN Smart Plug-in (SPI) integrates with the SNMP agents to configure reachability tests on the following types of routers:

- Cisco—Each Cisco router has an embedded Service Assurance Agent (SAA) that uses the values of the Cisco RTTMON MIB (SAA MIB) to determine the reachability test configuration for that device. For a description of Cisco's reachability test mechanism, see “Cisco Router Reachability Tests” on page 69.
- Juniper—Each Juniper router uses the values of the Juniper ping MIB to determine the reachability test configuration for that device. For a description of Juniper's reachability test mechanism, see “Juniper Router Reachability Tests” on page 69.

The MPLS VPN SPI maintains a list of PE-PE router pairs and configures bilateral tests of the reachability between each pair. For example, the MPLS VPN SPI configures the agent on PE1 to send a query from PE1 to PE2. The MPLS VPN SPI also configures the agent on PE2 to send a query from PE2 to PE1.

The MPLS VPN SPI supports the following types of reachability tests:

- A *PE-PE VRF-unaware reachability test* checks the connectivity between the PE routers as black boxes. By default, the MPLS VPN SPI configures these tests for every PE-PE pair in the MPLS VPN network.
- A *PE-PE VRF-aware reachability test* checks the connectivity between two PE routers over a pre-defined VRF path in a VPN.
- A *PE-CE VRF-aware reachability test* checks the connectivity between a PE router and a specific local CE router in a VPN.
- A *CE-CE end-to-end reachability test* checks the connectivity along a specific CE-PE-PE-CE path in a VPN.

Reachability Test Definitions

Reachability test definitions are stored in an MPLS VPN SPI internal file. The MPLS VPN SPI processes this file and configures each router's agent in the MPLS VPN network. Use the appropriate command to access the current reachability test definitions. For information, see "Changing Reachability Test Definitions" on page 84.

To configure a reachability test, create a new test definitions file and import that file into the MPLS VPN SPI reachability test definitions file. You can export the current reachability test definitions to a file and edit that file with your changes, or you can create a new text file containing only the tests you want to configure. Then import the updated reachability test definitions to the MPLS VPN SPI. Whenever the reachability test definitions file changes, the MPLS VPN SPI updates the reachability test configurations on each managed PE router and each Cisco (for SAA) or Juniper (for ping MIB) CE router.

NOTE

The pingCtlTable in the Juniper ping MIB allows up to 100 rows. Therefore, the MPLS VPN SPI supports up to 100 reachability tests per Juniper router.

Special Considerations for CE-CE Reachability Tests

The CE-CE end-to-end reachability test looks at the connectivity from the source CE router to the near PE router, then to the far PE router, and finally to the far CE router. For example, the reachability test for router CE1 to router CE3 in Figure 4-1 on page 67 follows the path: CE1-PE1-PE2-CE3.

The following sections discuss situations that apply to some CE-CE end-to-end reachability tests.

Non-Supported CE Type

If the source CE router (CE1) is not a Cisco or Juniper device, the MPLS VPN SPI breaks the CE-CE test into multiple segments that can be configured on a PE router. For example, consider the following network path:

CE1-PE1-PE2-CE3

If CE1 is not a Cisco or Juniper device, then the MPLS VPN SPI splits the test into a PE1-CE1 reachability test and a PE1-CE3 reachability test. It configures these tests on the PE1 device without intervention.

Multiple CE Routers Connected to One PE Router

The MPLS VPN SPI can discover multiple CE routers connected to a single PE router through a layer 2 switch but does not manage the switch directly. Instead, the VPN topology shows these multiple CE routers as directly connected to the PE router.

CE-CE end-to-end reachability tests are not supported in this environment. For example, consider the following path:

CE4-Sw1-PE3-PE4-CE6

To test the connections from router CE4 to router CE6, configure three separate reachability tests:

- PE3-CE4 VRF aware
- PE3-PE4 VRF aware
- PE4-CE6 VRF aware

Reachability Test Definitions File Format

The reachability test definitions file is a flat text file that defines the queries for each router to perform. The file contains one or more `BEGIN/END` pairs, each of which defines a specific test. Table on page 82 shows sample reachability test definitions.

The elements within a reachability test definition are as follows:

- `BEGIN`—The element that starts the definition of a reachability test.
- `TEST_TYPE`—The type of reachability test to be defined.

Possible values are `PE-PE`, `PE-CE`, and `CE-CE`:

- Use `PE-PE` for a `PE-PE` VRF-unaware test or for a `PE-PE` VRF-aware test.
- Use `PE-CE` for a `PE-local CE` VRF-aware test.
- Use `CE-CE` for an end-to-end `CE-CE` test.

- `SOURCE`—The selection name of the source router for the reachability test.

This value must match the selection name in the NNM topology database. The source router is the initiator of the reachability test. If the source router is Cisco, the MPLS VPN SPI configures an SAA test. If the source router is Juniper, the MPLS VPN SPI configures a ping MIB test.

- `DEST`—The selection name of the destination router for the reachability test.

This value must match the selection name in the NNM topology database. The destination router is the device that is verified by the reachability test.

- `VRF`—Optional. The name of a VRF that exists on both the source and destination routers.

This name is available in the router configuration files on the source edge router and in the file:

- *UNIX*: `$OV_CONF/VpnNames.txt`
- *Windows*: `%OV_CONF%\VpnNames.txt`

This value applies to `PE-PE` VRF-aware and `PE-CE` VRF-aware tests only.

- **OP**—The operation to be performed when this file is imported into the reachability test configuration tool.

Possible values are `ADD`, `DELETE`, and `MODIFY`.

The `MODIFY` operation examines the values of the `SOURCE`, `DEST`, and `VRF` elements to determine which test definition to change. If there is no test definition that matches the combination of these keys, the `MODIFY` operation adds the test definition as a new reachability test.

- **CONFIG_TYPE**—Optional. The configuration method to be used.

If this element is not included in the reachability test definition, the MPLS VPN SPI determines the correct value based on the type of router specified with the `SOURCE` parameter. The MPLS VPN SPI uses `SAA_TEST_CONFIG` for SAA tests and `TEST_CONFIG` for ping MIB tests.

Possible values are `SAA_TEST_CONFIG`, `TEST_CONFIG`, and `SAA_TEST_SYNC`:

- Use `SAA_TEST_CONFIG` to cause the MPLS VPN SPI reachability test configuration process to configure this test in the SAA MIB on the source router when you import this file.
- Use `TEST_CONFIG` to cause the MPLS VPN SPI reachability test configuration process to configure this test in the ping MIB on the source router when you import this file.
- Use `SAA_TEST_SYNC` to prevent the reachability test configuration process from changing the configuration of this test in the SAA on the source router. If you use this value, you must explicitly configure this reachability test in the SAA MIB on the source router using the Cisco IOS commands.

NOTE

There is no counterpart to `SAA_TEST_SYNC` for Juniper routers. All ping MIB test configuration must be done using the MPLS VPN SPI.

- **SRC_ADDR**—Optional. The IP address of the source interface card on the router for the reachability test.

This value applies to standard VRF-*unaware* tests only.

- For a PE-PE VRF-*unaware* test, this value can be any IP address on the source router.
- For a CE-CE end-to-end test, this value must be a private IP address within the VPN.

- **SAA_SRC_ADDR**—Deprecated. Use **SRC_ADDR** in new test definitions.
- **DEST_ADDR**—Optional. The IP address of the destination interface card on a router for the reachability test.

The address must be within the VPN address range that is reachable through the specified destination router for this reachability test.

- For a PE-PE VRF-*unaware* test, this value can be any IP address on the destination router.
- For a PE-PE VRF-*aware* test, a PE-CE VRF-*aware* test, or a CE-CE end-to-end test, this value must be a private IP address within the VPN.

- **SAA_DEST_ADDR**—Deprecated. Use **DEST_ADDR** in new test definitions.
- **SET_COMM**—Optional. The SNMP set community string of the source PE router.

If the community string for the source PE router is configured in the SNMP configuration database, you do not need to supply it in the reachability test definition. This value applies only when the value of the **CONFIG_TYPE** parameter is **SAA_TEST_CONFIG** or **TEST_CONFIG**.

- **FREQUENCY**—Optional. The time interval between instances of this test. Specify the number of seconds for the time interval.

If this element is not included in the reachability test definition, the value of the **FREQUENCY** parameter (for SAA tests) or **PINGMIBFREQ** parameter (for ping MIB tests) in the `mpls.conf` file when this reachability test is configured will be used for this test. For information on the `mpls.conf` file, see “MPLS VPN SPI Configuration File” on page 44.

- **TIMEOUT**—Optional. The length of time allowed for the response to a query before considering that the test failed.

Specify the number of milliseconds (for SAA tests) or seconds (for ping MIB tests), as appropriate, for the timeout value. For ping MIB tests, this value must be in the range of 1-15 seconds.

If this element is not included in the reachability test definition, the value of the `TIMEOUT` parameter (for SAA tests) or `PINGMIBTIMEOUT` parameter (for ping MIB tests) in the `mpls.conf` file when this reachability test is configured will be used for this test. For information on the `mpls.conf` file, see “MPLS VPN SPI Configuration File” on page 44.

- **TAG**—The identifier for this reachability test.
This value is determined by the MPLS VPN SPI and is valid for the export mode only. For a new test definition, leave this parameter undefined.
- **END**—The element that completes the definition of a reachability test.

Table 5-1 shows example reachability test definitions. The values of the `SOURCE` and `CONFIG_TYPE` parameters determine whether each test is an SAA or ping MIB reachability test.

Table 5-1 Sample Reachability Test Definitions

SAA Test Definitions	Ping MIB Test Definitions
PE-PE VRF-Unaware Reachability Test Samples	
<pre>BEGIN TEST_TYPE=PE-PE SOURCE=mplspe01 DEST=mplspe04 VRF= OP=ADD CONFIG_TYPE=SAA_TEST_CONFIG SAA_SRC_ADDR= SAA_DEST_ADDR= SET_COMM=ntcprivate FREQUENCY=600 TIMEOUT=100 TAG= END</pre>	<pre>BEGIN TEST_TYPE=PE-PE SOURCE=mplspe05 DEST=mplspe06 VRF= OP=ADD CONFIG_TYPE=TEST_CONFIG SRC_ADDR= DEST_ADDR= SET_COMM=remote-community FREQUENCY=600 TIMEOUT=1 TAG= END</pre>
PE-PE VRF-Aware Reachability Test Samples	
<pre>BEGIN TEST_TYPE=PE-PE SOURCE=mplspe01 DEST=mplspe04 VRF=Red_East OP=ADD CONFIG_TYPE=SAA_TEST_CONFIG SAA_SRC_ADDR= SAA_DEST_ADDR=10.97.255.27 SET_COMM=ntcprivate FREQUENCY=600 TIMEOUT=100 TAG= END</pre>	<pre>BEGIN TEST_TYPE=PE-PE SOURCE=mplspe05 DEST=mplspe06 VRF=brown-west-vpn OP=ADD CONFIG_TYPE=TEST_CONFIG SRC_ADDR= DEST_ADDR=10.97.255.29 SET_COMM=remote-community FREQUENCY=600 TIMEOUT=1 TAG= END</pre>

Table 5-1 Sample Reachability Test Definitions (Continued)

SAA Test Definitions	Ping MIB Test Definitions
PE-CE Local VRF-Aware Reachability Test Samples	
<pre> BEGIN TEST_TYPE=PE-CE SOURCE=mplspe01 DEST=mplsce01 VRF=Red_East OP=ADD CONFIG_TYPE=SAA_TEST_CONFIG SAA_SRC_ADDR= SAA_DEST_ADDR=10.10.20.1 SET_COMM=ntcprivate FREQUENCY=600 TIMEOUT=100 TAG= END </pre>	<pre> BEGIN TEST_TYPE=PE-CE SOURCE=mplspe05 DEST=mplsce06 VRF= brown-west-vpn OP=ADD CONFIG_TYPE=TEST_CONFIG SRC_ADDR= DEST_ADDR=10.97.255.3 SET_COMM=remote-community FREQUENCY=600 TIMEOUT=1 TAG= END </pre>
CE-CE End-to-End Reachability Test Samples	
<pre> BEGIN TEST_TYPE=CE-CE SOURCE=mplsce02 DEST=mplsce04 VRF= OP=ADD CONFIG_TYPE=SAA_TEST_CONFIG SAA_SRC_ADDR= SAA_DEST_ADDR= SET_COMM=ntcprivate FREQUENCY=600 TIMEOUT=100 TAG= END </pre>	<pre> BEGIN TEST_TYPE=CE-CE SOURCE=mplsce06 DEST=mplsce61 VRF= OP=ADD CONFIG_TYPE=TEST_CONFIG SRC_ADDR= DEST_ADDR= SET_COMM= remote-community FREQUENCY=600 TIMEOUT=1 TAG= END </pre>

Changing Reachability Test Definitions

You can view and change the current reachability test definitions:

- To view the current reachability test definitions:

```
reachability_config.ovpl -e filename
```

The MPLS VPN SPI exports the test definitions to the specified *filename*. These test definitions come from the reachability test configuration information stored by the MPLS VPN SPI, not from the devices themselves.

- To create new or modified reachability test definitions:

```
reachability_config.ovpl -i filename
```

The MPLS VPN SPI reads the reachability test definitions from the specified *filename* and updates the reachability test configurations on the appropriate PE routers.

See “Configuring Reachability Tests Using the MPLS VPN SPI” on page 86 for step-by-step instructions on how to change reachability test definitions.

Reachability Test Configuration

By default, the MPLS VPN SPI updates its reachability test definitions at the completion of MPLS VPN discovery. It then configures the agent MIB on each managed router with any changes to the existing reachability test definitions. See “Setting Reachability Test Configuration Parameters” on page 85.

Because the MPLS VPN SPI communicates with a router using SNMP, unassisted configuration of reachability tests requires access to the SNMP set community string for each router. See “Configuring Reachability Tests Using the MPLS VPN SPI” on page 86.

If you do not want to supply the SNMP set community string for a Cisco router, you can configure the SAA MIB on the router using the Cisco IOS commands. See “Configuring SAA Using the Cisco IOS Commands” on page 88.

There is no mechanism for manual configuration of the ping MIB on Juniper routers. All ping MIB test configuration must be done using the MPLS VPN SPI as described in “Configuring Reachability Tests Using the MPLS VPN SPI” on page 86.

Setting Reachability Test Configuration Parameters

The MPLS VPN SPI installation process sets the values of several parameters that control unassisted reachability test configuration.

To change the parameters for reachability test configuration via the MPLS VPN SPI:

- Using any text editor, edit the `mpls.conf` file.

The MPLS VPN SPI reads the `mpls.conf` file each time it performs reachability test configuration.

NOTE

Changing the value of any of the `FREQUENCY`, `TIMEOUT`, `PBMBIFREQ`, or `PINGMIBTIMEOUT` parameters affects new or modified reachability test definitions only. Existing reachability test definitions do not change.

For information on the contents of the `mpls.conf` file, see “MPLS VPN SPI Configuration File” on page 44.

Configuring Reachability Tests Using the MPLS VPN SPI

Unassisted reachability test configuration requires access to the SNMP set community string for a router. There are two supported ways to provide the SNMP set community string:

- Use the command `xnmssnmpconf` to store the community string in NNM’s SNMP configuration database. This method gives NNM access to the router for all of its management functions.
- Supply the community string in the imported reachability test definitions file. This method gives router access to the MPLS VPN SPI for reachability test configuration only.

By default, the MPLS VPN SPI creates VRF-unaware reachability tests for each PE-PE router pair in each VPN in the managed network after the MPLS VPN discovery process completes. If the list of PE-PE router pairs changes, the MPLS VPN SPI deletes the reachability tests that it configured without direct input from a reachability test definition file and configures new VRF-unaware reachability tests between all known PE-PE router pairs. (The list of PE-PE router pairs changes if MPLS VPN discovery identifies a new PE-PE router pair or removes an existing PE-PE router pair from the topology.)

To configure VRF-aware reachability tests or additional VRF-unaware reachability tests using the MPLS VPN SPI, follow these steps:

1. Create a reachability test definitions file:

```
reachability_config.ovpl -e filename
```

filename contains the current reachability test definitions.

2. Using any text editor, in *filename*, define the reachability tests to be performed:
 - a. As needed, modify the existing definitions:
 - To change an existing test definition, make the appropriate edits to the test definition, and then set the `OP` parameter to `MODIFY`.

- To delete an existing test definition, set the `OP` parameter to `DELETE`.

NOTE

If you delete a test definition that was created by the MPLS VPN SPI, the SPI will not re-add this test definition. If you later decide to perform this reachability test, you must write and import this test definition into the reachability configuration.

- b. As needed, add new test definitions:
 - Follow the format of the test definitions file.
For CE-CE end-to-end reachability tests, note the information in “Special Considerations for CE-CE Reachability Tests” on page 76.
 - Set the `OP` parameter to `ADD`.
- c. As needed, supply the SNMP set community string for each reachability test definition:
 - If the set community string for the source PE router is stored in the SNMP configuration database, ignore the `SET_COMM` parameter in the reachability test definition.
 - If the set community string for the source PE router is *not* stored in the SNMP configuration database, provide the correct value for the `SET_COMM` parameter in the reachability test definition.

3. Import the updated reachability test definitions:

```
reachability_config.ovpl -i filename
```

The MPLS VPN SPI reads each test definition in *filename* and configures that test in the appropriate MIB for the source router.

NOTE

The `reachability_config.ovpl` tool replaces the `saa_config.ovpl` tool from version 2.1 of the MPLS VPN SPI.

Configuring SAA Using the Cisco IOS Commands

If the SNMP set community string for a router is not available, use the Cisco IOS commands to configure SAA tests on that router.

Each SAA test includes a unique tag name. The MPLS VPN SPI uses this tag name to identify the SAA test in an SNMP trap. You must use the tag names that the MPLS VPN SPI generates. If the MPLS VPN SPI splits a CE-CE end-to-end reachability test into two separate tests, you must include the unique tag value for each test in its configuration.

To configure SAA tests via the Cisco IOS commands, follow these steps:

1. In a new text file, enter the following elements and their values for each SAA test:

- BEGIN
- TEST_TYPE
- SOURCE
- DEST
- VRF (if applicable)
- OP
- CONFIG_TYPE = SAA_TEST_SYNC
- SAA_SRC_ADDR (if applicable)
- SAA_DEST_ADDR (if applicable)
- END

For information about the file format, see “Reachability Test Definitions File Format” on page 78.

2. Generate a unique tag value for each SAA test:

```
saa_config.ovpl -i input_filename -o output_filename
```

The MPLS VPN SPI reads the *input_filename*, the text file you created in step 1, and writes the *output_filename*, a revised SAA test definitions file that includes a tag name for each SAA test definition.

3. Connect to the source router and use the Cisco IOS commands to configure each SAA.

For each test, specify the corresponding tag that the MPLS VPN SPI set in the `OV_TAG` parameter of the `output_filename` generated in step 2.

Figure 5-1 shows an example of a Cisco IOS command sequence for configuring an SAA test. For instructions on configuring your router, see the related Cisco documentation.

Figure 5-1 **Example of Cisco IOS Commands for SAA Configuration**

```
rtr Entry Number
type echo protocol IpIcmp Destination [source-ipaddr Source]
vrf VRF Name
timeout Timeout Value
frequency Frequency
tos 5
tag TagValue
rtr reaction-conf Entry Number threshold-type immediate
action-type trapOnly timeout-enable
rtr schedule Entry Number life 2147483647 start-time now
```

6 Troubleshooting the MPLS VPN Smart Plug-in

Troubleshooting Checklist

NOTE

If you are installing the MPLS VPN Smart Plug-in (SPI) over an existing version, see “Updating from a Previous Version of the MPLS VPN SPI” on page 28 before performing the MPLS VPN SPI installation steps.

Following is a summary of items to consider if you are having difficulties with the MPLS VPN SPI:

- Network Node Manager (NNM) cannot connect to the topology.
The NNM processes are not operating.
 - ❑ Verify that NNM is installed as described in “Verifying Proper Installation of Network Node Manager Advanced Edition” on page 96.
 - ❑ Verify that the NNM environment variables have been sourced properly as described in “Setting the NNM Environment Variables” on page 98.
 - ❑ Verify that the NNM services are operating properly as described in “Verifying That the NNM Services Are Operating on the Management Station” on page 99.
- One or more edge routers is not appearing in the NNM topology or the MPLS VPN views.
NNM has not discovered this device.
 - ❑ Use the `loadhosts` command or a seed file to help NNM locate all edge routers in the network. For instructions, see the guide *Managing Your Network with HP OpenView Network Node Manager*.
 - ❑ Verify that the MPLS VPN discovery has completed successfully as described in “Verifying That MPLS VPN Discovery Has Occurred” on page 102.

- All VRFs appear in one VPN, and this configuration is not what you expected to see.

The network has linked all PE routers because of management routes that touch all VRFs.

- ❑ Implement the `mplsStore.mplsRTIgnore` section of the `MplsVpn.cfg` file as described in “Ignoring Management Route Targets” on page 55.

- No events appear in the MPLS VPN Alarms Browser.

The MPLS VPN SPI is not receiving events about the edge routers.

- ❑ Verify that the required MIBs are loaded as described in “Verifying That MIBs Are Loaded” on page 101.
- ❑ Verify that the managed devices are properly configured to forward traps to the NNM management station:
 - If you use SNMP access-control to limit the computers that can have SNMP access to a router, include the NNM management station in the access list on each edge router.
 - Configure each edge router to include the NNM management station as one of the SNMP trap recipients.
 - For information about these configurations, see the documentation that came with your routers.
- ❑ Verify that the NNM management station is receiving events from the devices:
 - Look in the All Alarms browser for events regarding the edge routers. An easy way to create an event is to temporarily disconnect an interface card from the network.
- ❑ Verify that NNM is able to poll the edge routers for status information as described in “Configuring SNMP Polling Access for netmon” on page 41.
- ❑ Verify that MPLS VPN discovery has occurred as described in “Verifying That MPLS VPN Discovery Has Occurred” on page 102.
- ❑ Verify that the MPLS VPN SPI is operating as described in “Verifying That the MPLS VPN SPI Is Operating” on page 100.

Troubleshooting Checklist

- No network core status events appear in the MPLS VPN Alarms Browser.

The MPLS VPN SPI is not receiving events from the RAMS appliance.

- Verify that RAMS is properly integrated with NNM as described in the *Network Node Manager / Route Analytics Management System Integration Module User's Guide*.
 - Verify that the watch list for the `rexRouteChange` event is configured with all PE-PE router pairs as described in “Network Core Status Events” on page 65.
- The RAMS Path History View is empty.

The view did not correctly receive the PE router information.

- Type the PE router names directly into the `Source Router` and `Destination Router` fields of the RAMS Path History View.
 - For more information, see the documentation that came with the RAMS appliance.
- No reachability test status events appear in the MPLS VPN Alarms Browser.

The MPLS VPN SPI is not receiving reachability events from the edge routers.

- Verify that the managed devices are properly configured to forward traps to the NNM management station:
 - If you use SNMP access-control to limit the computers that can have SNMP access to a router, include the NNM management station in the access list on each edge router.
 - Configure each edge router to include the NNM management station as one of the SNMP trap recipients.
 - For information about these configurations, see the documentation that came with your routers.

- ❑ Verify that the NNM management station is receiving events from the devices:
 - Look in the All Alarms browser for events regarding the edge routers. An easy way to create an event is to temporarily disconnect an interface card from the network.
- ❑ Verify that the reachability test definitions exist. See “Verifying Reachability Test Definitions” on page 103.
- ❑ Verify that the MPLS VPN SPI is operating. See “Verifying That the MPLS VPN SPI Is Operating” on page 100.
- A Juniper router returns a `BAD_VALUE` (SNMPv1) or `RESOURCE_UNAVAILABLE` (SNMPV2) message when I try to configure a reachability test in the ping MIB.

Juniper routers support a maximum of 100 rows in the `pingCtlTable`.
- ❑ Delete unwanted reachability tests and then configure the new test.

For additional troubleshooting information, refer to the latest *NNM Smart Plug-in for MPLS VPN Release Notes* and *Release Notes for Reporting and Network Solutions* available on the Web at http://ovweb.external.hp.com/lpe/doc_serv under the Reporting and Network Solutions product category.

Verifying Proper Installation of Network Node Manager Advanced Edition

To verify that the NNM Advanced Edition product is installed, do the following:

UNIX:

```
/usr/sbin/swlist | grep "OpenView Network Node Manager  
Extended Topology"
```

Windows:

1. From the Start menu, launch the Control Panel.
2. Double-click Add/Remove Programs.
3. Verify that HP OpenView Network Node Manager is present in the list of programs.

Determining Which Version of NNM is Installed

To determine which version of NNM is installed:

UNIX: `/opt/OV/bin/ovnnmversion`

Windows: `install_dir\bin\ovnnmversion`

Setting the NNM Environment Variables

To source the NNM environment variables:

- UNIX using sh or ksh: `. /opt/OV/bin/ov.envvars.sh`
- UNIX using csh: `source /opt/OV/bin/ov.envvars.csh`
- Windows: run `install_dir\bin\ov.envvars.bat` within a command window

This step sets the environment variables required by the MPLS VPN SPI, including:

- *UNIX*: `$OV_BIN`, `$OV_LRF`, `$OV_CONF`, `$OV_MAIN_PATH`
- *Windows*: `%OV_BIN%`, `%OV_LRF%`, `%OV_CONF%`, `%OV_MAIN_PATH%`

Verifying That the NNM Services Are Operating on the Management Station

To verify that the NNM services are operating on the management station, follow these steps:

1. Verify that NNM is installed as described in “Verifying Proper Installation of Network Node Manager Advanced Edition” on page 96.
2. Determine the status of the NNM services:
 - *UNIX*: `$OV_BIN/ovstatus -v`
 - *Windows*: `%OV_BIN%\ovstatus -v`

All of the processes, including PMD, should be running.

3. If NNM and all associated processes are not running, stop and restart the NNM services:
 - *UNIX*:
`$OV_BIN/ovstop -c`
`$OV_BIN/ovstart -c`
 - *Windows*:
`%OV_BIN%\ovstop -c`
`%OV_BIN%\ovstart -c`

Verifying That the MPLS VPN SPI Is Operating

To verify that the MPLS VPN status manager service is operating on the management station, follow these steps:

1. Determine the status of the MPLS VPN SPI status manager:

- *UNIX:*
`$OV_BIN/ovstatus -v MPLS_sm MPLS_pp`
- *Windows:*
`%OV_BIN%\ovstatus -v MPLS_sm MPLS_pp`

The `MPLS_sm` and `MPLS_pp` processes should be running.

2. If the `MPLS_sm` or `MPLS_pp` process is not running, stop and restart the NNM services:

- *UNIX:*
`$OV_BIN/ovstop -c`
`$OV_BIN/ovstart -c`
- *Windows:*
`%OV_BIN%\ovstop -c`
`%OV_BIN%\ovstart -c`

Verifying That MIBs Are Loaded

To verify that the required MIBs are loaded onto the NNM management station, follow these steps:

1. In the NNM GUI (ovw), click Options->Load/Unload MIBs:SNMP.

The Load/Unload MIB:SNMP window appears. This window lists the MIBs that have been loaded onto the NNM management station.

2. Verify that the MIBs named in “MIB Dependencies” on page 25 are loaded.
3. If one or more of the required MIBs is not loaded, add it using this window.

For more information, see the guide *Managing Your Network with HP OpenView Network Node Manager*.

Verifying That MPLS VPN Discovery Has Occurred

If you think that the MPLS VPN SPI has not discovered all routers in the MPLS VPN network, check the status of the MPLS VPN discovery agents:

- *UNIX:*

```
$OV_BIN/ovstatus -v ovet_daCiscoMplsVpn  
$OV_BIN/ovstatus -v ovet_daJunMplsVpn
```
- *Windows:*

```
%OV_BIN%\ovstatus -v ovet_daCiscoMplsVpn  
%OV_BIN%\ovstatus -v ovet_daJunMplsVpn
```

The last message in the status output describes the current state of the MPLS VPN discovery agent:

- If this message describes a step in the discovery process, MPLS VPN discovery is running. Wait for the discovery process to complete, and then look for the expected MPLS VPN devices in the MPLS VPN views.
- If this message is *Awaiting next discovery cycle*, the MPLS VPN discovery agent has completed discovery and is idle until the next discovery cycle. Use the `loadhosts` command or a seed file to help NNM locate all routers in the MPLS VPN network. For more information, see the guide *Managing Your Network with HP OpenView Network Node Manager*.
- If this message shows an error state, restart Extended Topology discovery. For more information, see the guide *Using Extended Topology*.

Verifying Reachability Test Definitions

Several configuration files store the reachability test definitions that the MPLS VPN SPI configures on the PE routers. The `saa.conf` and `ping_mib.conf` files store the SAA and ping MIB test definitions, respectively, in plain text. The `saa_tag.xml` file stores these test definitions in XML format.

To verify that the reachability test definitions exist, check for the existence of the following files:

- *UNIX*:
 - `$OV_DB/saa_tag.xml`
 - `$OV_DB/saa.conf` (optional, for reachability tests on Cisco routers)
 - `$OV_DB/ping_mib.conf` (optional, for reachability tests on Juniper routers)
- *Windows*:
 - `%OV_DB%\saa_tag.xml`
 - `%OV_DB%\saa.conf` (optional, for reachability tests on Cisco routers)
 - `%OV_DB%\ping_mib.conf` (optional, for reachability tests on Juniper routers)

Recreating the saa_tag.xml File

If the `saa_tag.xml` file does not exist or has size 0 and either of both of the `saa.conf` and `pingmib.conf` files does exist but should, follow these steps to recreate the `saa_tag.xml` file:

1. Export the current reachability test definitions to a file:

- *UNIX:*

```
$OV_BIN/reachability_config.ovpl -e  
/tmp/current_tests.txt
```

- *Windows:*

```
%OV_BIN%\reachability_config.ovpl -e  
C:\temp\current_tests.txt
```

2. Edit the `current_tests.txt` file, changing the value of the `OP` parameter for one of the test definitions to `MODIFY`.

3. Import the revised file:

- *UNIX:*

```
$OV_BIN/reachability_config.ovpl -i  
/tmp/current_tests.txt
```

- *Windows:*

```
%OV_BIN%\reachability_config.ovpl -i  
C:\temp\current_tests.txt
```

The `saa_tag.xml` file should now exist.

NOTE

The `saa_tag.xml` file is internal to the MPLS VPN SPI. Do not edit this file.

Recreating the `saa.conf` File

If the `saa.conf` file does not exist or has size 0, follow these steps to recreate the SAA test definitions:

1. Log on to an edge router that is the source for one or more SAA tests.
2. Edit the Cisco RTTMON MIB to remove all SAA test configurations.
3. Repeat steps 1 and 2 for each edge router that is the source for one or more SAA tests in the MPLS VPN network.
4. Ensure that the `SAA_TRIG` parameter in the `mpls.conf` file is set to `true`. See “Setting Reachability Test Configuration Parameters” on page 85.
5. Initiate Extended Topology discovery to rediscover the MPLS VPN topology. After MPLS VPN discovery completes, the NNM generates the `saa.conf` file.

See the guide *Using Extended Topology* for information on initiating discovery.

Recreating the `ping_mib.conf` File

If the `ping_mib.conf` file does not exist or has size 0, follow these steps to recreate the ping MIB test definitions:

1. Log on to an edge router that is the source for one or more ping MIB tests.
2. Edit the Juniper ping MIB to remove all test configurations.
3. Repeat steps 1 and 2 for each edge router that is the source for one or more ping MIB tests in the MPLS VPN network.
4. Ensure that the `PINGMIB_TRIG` parameter in the `mpls.conf` file is set to `true`. See “Setting Reachability Test Configuration Parameters” on page 85.
5. Initiate Extended Topology discovery to rediscover the MPLS VPN topology. After MPLS VPN discovery completes, the NNM generates the `ping_mib.conf` file.

See the guide *Using Extended Topology* for information on initiating discovery.

Handling Other Problems

This section lists errors that you might encounter while using the MPLS VPN SPI and describes remedies to these situations. Read this section if none of the situations in the “Troubleshooting Checklist” on page 92 matches your need.

Rebooting an Edge Router Removes the SAA Test Definitions from the SAA MIB

NOTE

This situation applies to Cisco routers only.

There is no way to protect the SAA test definitions from removal.

To work around this situation:

- Before rebooting the edge router, perform the following IOS command on that router:

```
write mem
```

This command causes the router to reload the SAA tests during the boot sequence.

PE Router Symbols Show Red in NNM

The red color indicates critical status for these devices. This status is managed by NNM, not the MPLS VPN SPI.

If you believe this status indicator to be incorrect, perform a demand poll of this node to ensure that NNM is showing the latest status information:

- *UNIX:* `$OV_BIN/nmdemandpoll nodename`
- *Windows:* `%OV_BIN%\nmdemandpoll nodename`

NNM queries the *nodename* using SNMP and updates the status of the node’s interface cards. The color of the PE router symbol reflects the status of the contained interface cards.

The PE Router Symbol Has a Square Shape, Not a Diamond Shape

The square symbol shape indicates a computer with only one LAN card. The diamond symbol shape indicates a router with multiple LAN cards. If the PE router symbol has a square shape, NNM has information about only one LAN card. SNMP requests for information about additional LAN cards have not been successful. Verify the SNMP connectivity to this router:

- **UNIX:** `$OV_BIN/snmpwalk nodename system`
- **Windows:** `%OV_BIN%\snmpwalk nodename system`

NNM walks the system section of the MIB-2 MIB for the specified node.

- Upon success, `snmpwalk` displays the values of the system variables. If there are multiple LAN cards, the PE router symbol should now be a diamond shape.
- Upon failure, `snmpwalk` displays the message “No response arrived before timeout.”

Set the set community string for the PE router in the SNMP configuration database, and then perform the SNMP walk again.

VPN Names Are Confusing

You can configure VPN names that make sense for your environment. See “Changing VPN Names in the MPLS VPN SPI Configuration” on page 53.

A Change to the MPLS VPN Configuration Does Not Appear

After changing the MPLS VPN structure, delete the `VpnNames.txt` file, and then initiate Extended Topology discovery to update the MPLS VPN information. For more information, see the guide *Using Extended Topology* that was included with NNM Advanced Edition.

Collecting Information for HP Support

If errors occur that are not documented in this guide, follow these steps to collect information about your system and configuration, and then report the problem to your HP support representative.

1. Take note of the error.
2. Verify that NNM is operating. For instructions, see “Verifying That the NNM Services Are Operating on the Management Station” on page 99.
3. Gather the following information for your HP support representative:

- Data and configuration files:

UNIX:

- \$OV_CONF/VpnNames.txt
- \$OV_CONF/mp1s.conf
- \$OV_LOG/ovtopodump.log
- \$OV_LOG/ovet_disco.old.log
- \$OV_LOG/ovet_topoquery_getallIfcs.log

Windows:

- %OV_CONF%\VpnNames.txt
- %OV_CONF%\mp1s.conf
- %OV_LOG%\ovtopodump.log
- %OV_LOG%\ovet_disco.old.log
- %OV_LOG%\ovet_topoquery_getallIfcs.log

- Reachability test export file (`current_tests.txt`):
Create the export file:
 - *UNIX*:

```
$OV_BIN/reachability_config.ovpl -e /tmp/current_tests.txt
```
 - *Windows*:

```
%OV_BIN%\reachability_config.ovpl -e C:\temp\current_tests.txt
```
- The file `ovobjprint.output`:
Create the output file:
 - *UNIX*:

```
$OV_BIN/ovobjprint > /tmp/ovobjprint.output
```
 - *Windows*:

```
%OV_BIN%\ovobjprint > C:\temp\ovobjprint.output
```
- Topology of your MPLS VPN network including:
 - Connectivity information
 - Names, IP addresses
- VPN information:
 - PE router – VRF – Interface relationships
 - VPN details (which VRF on which PE router corresponds to which VPN)
- Screenshots as appropriate:
 - Alarms Browser showing events
(Modify the column widths of the browser to display as much of the event message text as possible.)
 - NNM submaps

Collecting Information for HP Support

- Current status of the network:
 - Is everything operational?
 - Did any interfaces or routers shut down while you were collecting the above data?
- PE router information including:
 - Vendor (e.g., Cisco)
 - Model name (e.g., Catalyst 6509)
 - IOS version

B

- benefits
 - MPLS VPN SPI, 12

C

- CE-CE end-to-end reachability test
 - description, 75
 - sample, 83
- Cisco
 - SAA test definitions deleted at reboot, 106
- configuration
 - initial, 43
- cross-launch of OVPI reports, 19

E

- events
 - reachability test status change, 69
 - router status change, 61

I

- installation
 - hardware requirements, 24
 - on UNIX, 33
 - on Windows, 34
 - software requirements, 24

L

- launch of OVPI reports, 19
- log files
 - System.txt, 60

M

- MIB dependencies
 - list, 25
 - verification, 101
- MPLS VPN Alarms Browser, 14
- MPLS VPN discovery
 - configuration, 49
 - description, 48
 - running, 49
 - verification, 102
- MPLS VPN SPI
 - behavior, 13
 - benefits, 12
 - events
 - reachability test status change, 69
 - router status change, 61
 - user interaction, 14

- installation
 - on UNIX, 33
 - on Windows, 34
 - verification, 100
- removal
 - on UNIX, 39
 - on Windows, 39
- software prerequisites, 24
- uninstall
 - on UNIX, 39
 - on Windows, 39
- MPLS VPN status manager, 60
- mpls_sm, 60
- mpls_unconfig.ovpl, 39

N

- netmon.snmpStatus file, 42
- Network Node Manager
 - prerequisite, 24
- nmdemandpoll, 106
- NNM Alarms Browser
 - MPLS VPN category, 14
- NNM installation
 - environment variables, 98
 - verification, 96
 - version identification, 97
- NNM services
 - verification, 99

O

- operating systems
 - supported, 24
- OVPI report
 - launching, 19

P

- pairwise correlation
 - MPLS VPN status manager, 60
 - ping MIB events, 68
 - router status events, 62, 66
 - SAA events, 68
- PE-CE VRF-aware reachability test
 - description, 75
 - sample, 83
- PE-PE VRF-aware reachability test
 - description, 75
 - sample, 82
- PE-PE VRF-unaware reachability test
 - description, 75

Index

- sample, 82
- ping MIB
 - description, 69
- ping MIB test
 - description, 69
 - events, 69
- ping MIB test definitions
 - changing, 84
- ping_mib.conf file
 - creation, 105

R

- reachability test
 - CE-CE end-to-end, 75
 - configuration, 85
 - MPLS VPN SPI, 86
 - PE-CE VRF-aware, 75
 - PE-PE VRF-aware, 75
 - PE-PE VRF-unaware, 75
- reachability test definitions
 - changing, 84
 - description, 76
 - file format, 78
- reachability_config.ovpl, 84, 86, 87
- removal
 - on UNIX, 39
 - on Windows, 39

S

- SAA
 - description, 69
- SAA test
 - configuration
 - Cisco IOS commands, 88
 - description, 69
 - events, 69
- SAA test definitions
 - deleted at reboot, 106
 - verification, 103
- saa.conf file
 - creation, 105
- saa_config.ovpl, 87
- saa_tag.xml file
 - creation, 104
- Service Assurance Agent, 69
- SNMP configuration database, 43
- SNMP set community string
 - access, 85, 86
 - configuring, 43
 - SET_COMM element, 80

- snmpwalk, 107
- support
 - information needed, 108
- symbols
 - shape, 107
 - status, 106
- System.txt file, 60

T

- trapd.conf file, 61, 65, 68

U

- uninstall
 - on UNIX, 39
 - on Windows, 39

V

- VPN names
 - algorithm, 50
 - changing, 53
- VRF-aware reachability test
 - configuration, 86
 - DEST_ADDR element, 80
 - SAA_DEST_ADDR element, 80
 - VRF element, 78
- VRF-unaware reachability test
 - SAA_SRC_ADDR element, 80
 - SRC_ADDR element, 80

W

- write mem, 106

X

- xnmsnmpconf, 43, 86