HP OpenView Network Node Manager Smart Plug-in

MPLS VPN Smart Plug-in

For the HP-UX, Solaris, and Windows® Operating Systems

Software Version: 3.2

Administrator's Guide

Document Release Date: August 2006
Software Release Date: August 2006

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Adobe® Acrobat® are trademarks of Adobe Systems Incorporated.

Java™ is a US trademark of Sun Microsystems, Inc.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

This manual's title page contains the following identifying information:

- Software version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

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

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Please visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

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

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 enhancement requests online
- Download software patches
- 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. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

Contents

1 Introducing the MPLS VPN Smart Plug-in

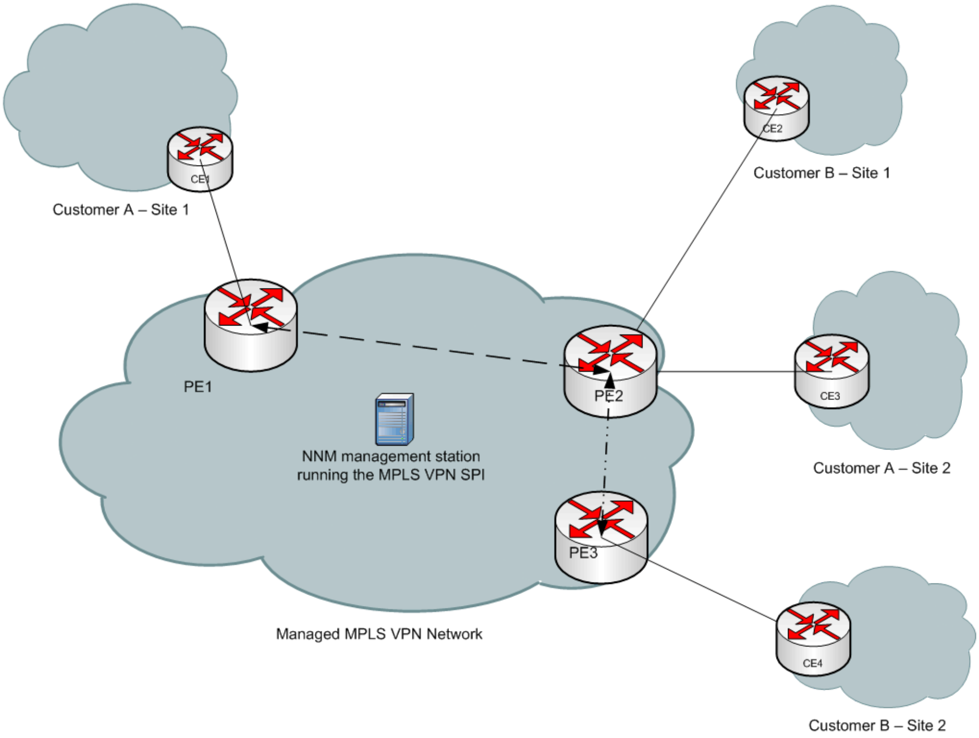
Introduction

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 on page 10 shows an 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 (P routers) 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.

Figure 1 Example of an MPLS VPN Network.



What Can You Achieve with the MPLS VPN SPI?

Manage Traffic and Management VPNs

Management VPNs are part of the network management system in the service provider environment that are able to communicate with the CE routers in order to manage them. The MPLS VPN SPI distinguishes between the Management VPNs and the customer VPNs (referred to as Traffic VPNs in this documentation). The distinction is made in the MPLS VPN views by displaying the Traffic VPNs and the Management VPNs independently.

The MPLS VPN SPI automatically discovers management route targets, which can belong to several or all of the VPNs. Only those Management VPNs that follow a hub-and-spoke topology and whose route targets' occurrence among VRFs is high (at least 3.5 times the occurrence count of the highest occurrence route target in the Traffic VPN) are discovered.

Alternatively, you can configure the management route targets after installation. Use the Management VPN configuration GUI to configure management route targets.

Manage Faults

The MPLS VPN SPI identifies relationships between events and generates new, enriched events that include 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 the *MPLS VPN Smart Plug-in Installation and Configuration Guide*.

Perform Reachability Tests

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 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 label switch paths 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.

Supports VRF-Lite and Shadow Routers

The MPLS VPN SPI supports shadow routers (Cisco refers to them as SLA routers) and VRF-Lite routers. A shadow router is a low-end router that off loads router testing work from the PE router, so that the PE is not overloaded with the same. A VRF-Lite router is basically a traffic classifier that is achieved on the CE by defining multiple VRFs.

In particular, the MPLS VPN SPI extends the following functionality to a CE connected to a PE:

- VRF-Lite router

  With VRF-Lite, multiple customers share one CE, but only one physical link exists between the CE and the PE. The shared CE maintains separate VRF tables for each VPN. This functionality extends the privacy and security of VPNs to the branch offices.

  VRF-Lite routers can be configured to classify the CE-based site traffic.

  In the case where a VRF-Lite device is a low-end router or a router where the MIBs are properly supported on that IOS, VRF-Lite devices can be provisioned by providing the loopback IP address of the VRF-Lite router in the VRF-Lite configuration file, `$OV_CONF/VrfLite.cfg`. For example, if the MPLS VPN SPI failed to discover two routers (let's say with IP addresses `a.b.c.d` and `w.x.y.z`) as VRF-Lite routers, the `VrfLite.cfg` file would need to contain the following:

  ```
  a.b.c.d
  w.x.y.z
  ```

  During discovery the MPLS VPN SPI excludes them from treating as a CE and includes them in the VRF-Lite list.

- Shadow router

  Like VRF-Lite, shadow routers are connected to the PE and perform limited work load capabilities. Shadow routers can be configured to perform reachability tests. By offloading the reachability tests to the shadow router, the PE can focus on the LSP-based traffic, or multiple label switched packet traffic.

The MPLS VPN SPI discovers Cisco devices acting as VRF-Lite or shadow routers only.

The MPLS VPN SPI discovers shadow and VRF-Lite routers, and displays a VRF-Lite router icon in the MPLS VPN views to represent this functionality. The VRF-Lite router is shown connected to the PE in the MPLS VPN views, irrespective of the VPN in which the PE router participates. The MPLS VPN SPI, however, will not classify the VRF-Lite or shadow routers as CE extensions or PE extensions.

Integration with Route Analytics Management System (RAMS)

When HP OpenView Route Analytics Management System (RAMS) for OSPF or IS-IS 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 monitor traffic-engineered label switch paths.

When HP OpenView Route Analytics Management System (RAMS) for mBGP is integrated into NNM, the MPLS VPN SPI shares configuration information with the RAMS appliance. This sharing automates a lengthy manual process for RAMS configuration.

Integration with HP OpenView Performance Insight (OVPI)

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.
- The MPLS VPN SPI supports VRF-Lite routers and shadow routers.
- 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.
- When CDP is enabled, the MPLS VPN SPI discovers PE-CE connections in a duplicate IP address environment.
- The MPLS VPN SPI automatically discovers management route targets, and displays them separately in the MPLS VPN view as Management VPNs.

- By enriching network status events, the MPLS VPN SPI generates 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 lets you configure various types of site-to-site reachability tests and generates events to indicate changes in the tested connections.
- The MPLS VPN SPI supports Cisco routers that function as shadow routers, performing reachability tests for the connected PE.
- When applicable, the MPLS VPN SPI performs management of the network core by generating enriched events that relate changes in the label switch paths monitored by RAMS to MPLS VPN performance.
- When applicable, the MPLS VPN SPI synchronizes VPN names with the RAMS appliance.
- 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, CE-CE, and shadow router reachability tests.
- OVPI threshold exceeded traps for MPLS VPN, IP SLA, 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 affected 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 15.
- Examine graphical and tabular representations of the MPLS VPN network through the windows available in the MPLS VPN Views. See Available MPLS VPN Views on page 17.
  - Configure Management VPNs by using the MPLS VPN views. See Launching Management VPN Configuration Tool on page 24.
  - Rename VPNs according to your preferences. See Launching the VPN Rename Tool on page 22.
- When RAMS is installed and integrated with NNM, monitor the status of the label switch paths in the MPLS VPN Views. See RAMS Integration on page 20.
- 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 20.

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 Alarms 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 [*VPN:VRF*] Down due to connection down between [*source_node:interface*] and [*destination_node:interface*]
- 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 Path Down between [*node1*] and [*node2*].
- MPLS/VPN: VPN:VRF [*VPN:VRF*] Path Worse between [*node1*] and [*node2*].
- MPLS/VPN: VPN:VRF [*VPN:VRF*] Path Better between [*node1*] and [*node2*].
- MPLS/VPN: IPSLA test failed between [*node1-node2*] affected VPN/VRF(s):[*VPN1:VRF1,VPN2:VRF2,*...]. Root cause is cause.
- MPLS/VPN: IPSLA 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: IPSLA 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 source and destination node names of the edge routers 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]`.

Available MPLS VPN Views

The MPLS VPN SPI has several views available:

- `MPLS VPN View`—High level information about the routers and VPNs in the MPLS VPN network. VPNs are grouped as into Management VPNs and Traffic VPNs. For a sample, see MPLS VPN View on page 18.

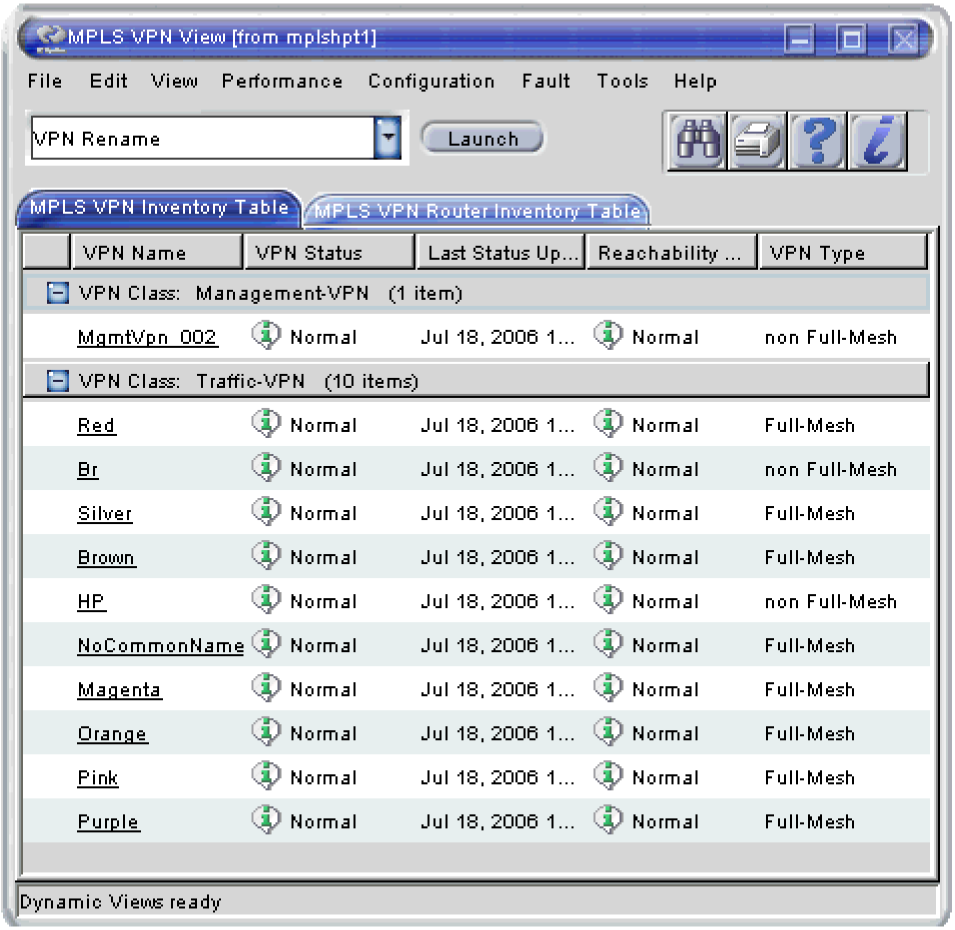
- `MPLS VPN Details`—Descriptive information about the accessible PE and CE routers and the VRFs in a specific VPN. Shadow routers and VRF-Lite routers are displayed as VRF-Lite routers in the graph view. A shadow router is displayed for all VPNs in which the connected PE participates.

- `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 and the VRF neighbors of a PE. When a VRF belongs to more than one VPN, all of the VPN names are listed, separated by commas. The VRF neighbor tab lists adjacent VRFs, and are grouped by the VPN to which they belong.

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

Figure 2 MPLS VPN View



	VPN Name	VPN Status	Last Status Up...	Reachability ...	VPN Type
⊟ VPN Class: Management-VPN (1 item)					
	MgmtVpn_002	Normal	Jul 18, 2006 1...	Normal	non Full-Mesh
⊟ VPN Class: Traffic-VPN (10 items)					
	Red	Normal	Jul 18, 2006 1...	Normal	Full-Mesh
	Br	Normal	Jul 18, 2006 1...	Normal	non Full-Mesh
	Silver	Normal	Jul 18, 2006 1...	Normal	Full-Mesh
	Brown	Normal	Jul 18, 2006 1...	Normal	Full-Mesh
	HP	Normal	Jul 18, 2006 1...	Normal	non Full-Mesh
	NoCommonName	Normal	Jul 18, 2006 1...	Normal	Full-Mesh
	Magenta	Normal	Jul 18, 2006 1...	Normal	Full-Mesh
	Orange	Normal	Jul 18, 2006 1...	Normal	Full-Mesh
	Pink	Normal	Jul 18, 2006 1...	Normal	Full-Mesh
	Purple	Normal	Jul 18, 2006 1...	Normal	Full-Mesh

Dynamic Views ready

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 View`.
- 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 View`.

Inventory Table Tabs from the MPLS VPN View

There are two tabs on the MPLS VPN view:

- MPLS VPN Inventory View

  From the MPLS VPN view, select the MPLS VPN Inventory Table tab. This table lists the details of the VPNs. VPNs are separated into Traffic VPNs and Management VPNs categories.

- MPLS VPN Router Inventory View

  From the MPLS VPN view, select the MPLS VPN Router Inventory Table tab. This table displays participating provider edge devices (PE), customer edge devices (CE), and shadow routers (VRF-Lite).

Launching VRF Details

From the MPLS VPN view, select the MPLS VPN Inventory Table tab. Select a VPN from the VPN Name column, and then double-click. The VRF Details view displays, which includes two tabs.

First, the VRF Details Table tab provides information about the name of the VPNs the VRF participates in as well as the route target import and export. The inventory table lists the PE interfaces and connected CE interface for the VRF.

Second, the VRF Neighbor Table tab displays VRF details for each VPN in which the VRF participates.

RAMS Integration

HP offers support for several protocols with the RAMS appliance. If you have deployed a RAMS appliance into the managed network and have installed the NNM / RAMS Integration Module, the MPLS VPN SPI has the following possible additional features:

- With RAMS for OSPF or IS-IS, the MPLS VPN SPI can perform core network management by receiving 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, select `Show LSP` from the list, and then click `Launch`.

  — In the `MPLS VPN Details Table`, select two PE router rows, select `Show LSP` from the list, and then click `Launch`.

  — In the `VRF Neighbors Table`, click `Show` in the `LSP` column of the row that includes the remote PE router.

- With RAMS for mBGP, the MPLS VPN SPI can perform VPN name synchronization with the RAMS appliance. For more information, see Synchronizing VPN Names with RAMS on page 41.

Reports from OVPI

If you have the MPLS VPN and Service Assurance 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 Views

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

1. In any MPLS VPN view, and then optionally select an object.
2. Select a report in the list, and then click Launch.

   Some reports require that you select an object in the MPLS VPN view before launching the report (for example, the MPLS VPN Router Report available from the MPLS VPN Details Table). Other reports use data common to the entire view (such as the VPN name for the THIS VPN Report available from the MPLS VPN Details Table).

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

Configuration Tools from the MPLS VPN View

The following configuration tools are available from the MPLS VPN view:

- VPN Rename tool

This view lets you change the name of the discovered VPNs.

- Management VPN Configuration tool

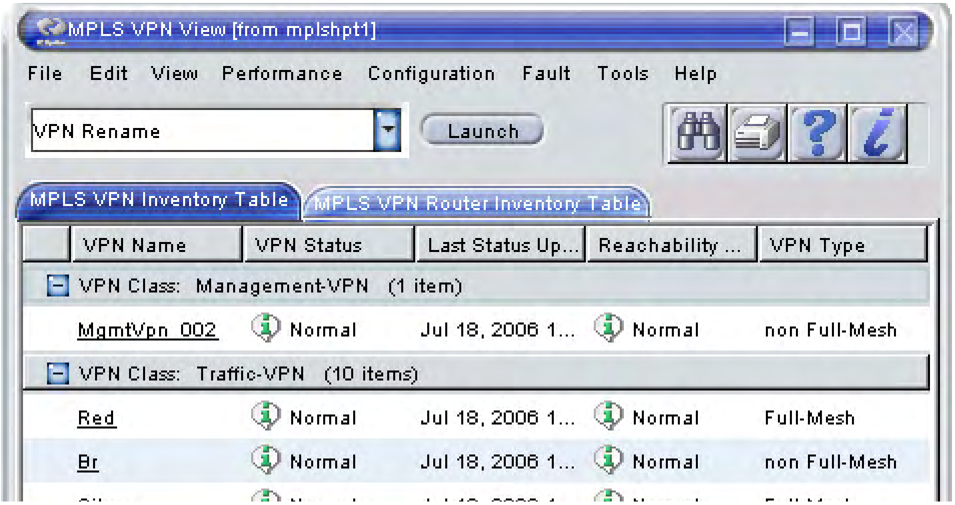
  This view lets you manage the discovery of route targets. You can set the MPLS VPN SPI to automatically discover Management VPNs, include additional route targets, and exclude other route targets.

Launching the VPN Rename Tool

To change the name of VPNs, do the following:

1. From the MPLS VPN view, select `VPN Rename` view from the list box. See Figure 3.

Figure 3 VPN Rename View Selection from the MPLS VPN View

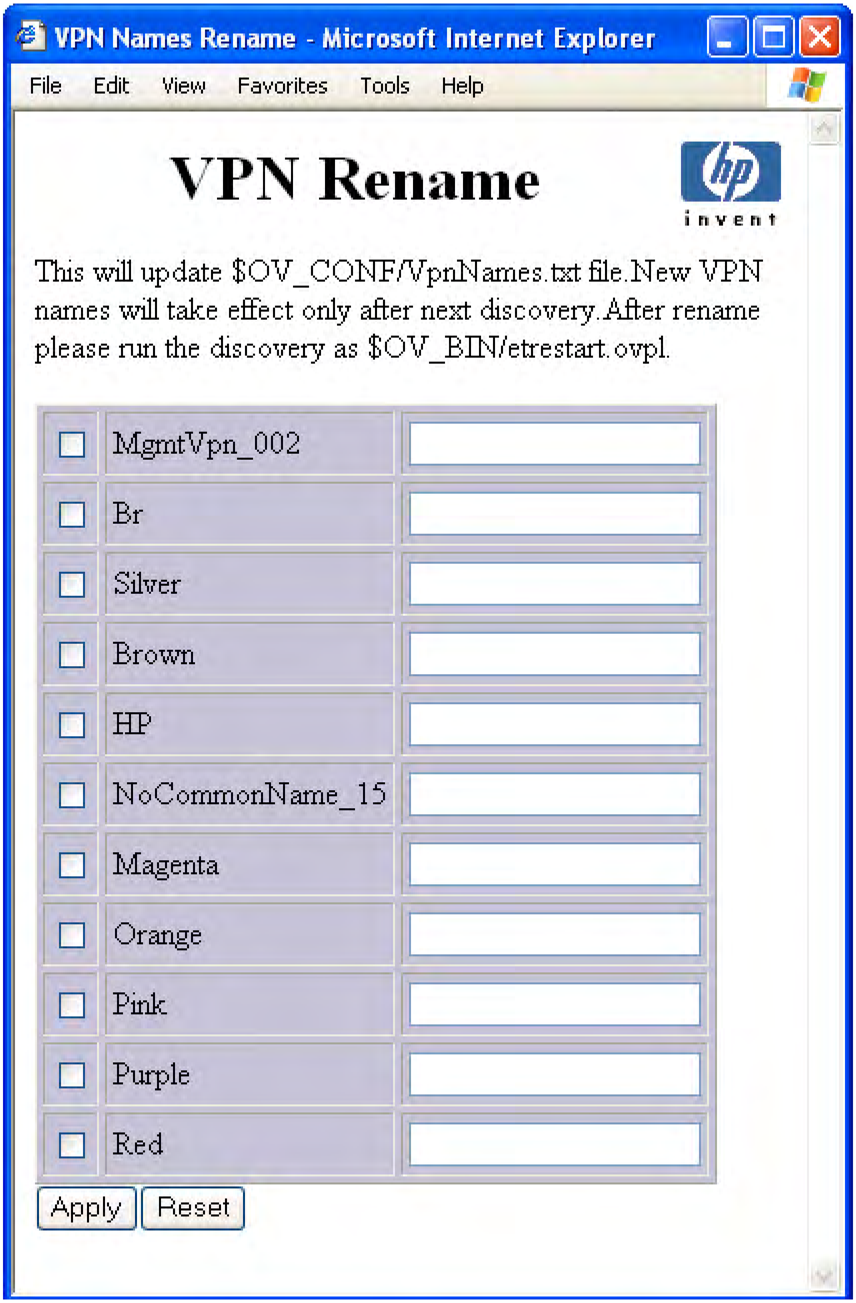


	VPN Name	VPN Status	Last Status Up...	Reachability ...	VPN Type
⊟ VPN Class: Management-VPN (1 item)					
	MgmtVpn_002	Normal	Jul 18, 2006 1...	Normal	non Full-Mesh
⊟ VPN Class: Traffic-VPN (10 items)					
	Red	Normal	Jul 18, 2006 1...	Normal	Full-Mesh
	Br	Normal	Jul 18, 2006 1...	Normal	non Full-Mesh

2. Click **Launch**.
3. Select the VPNs to be renamed, and then enter the new name for the selected VPN. See Figure 4.
4. Click **Apply**.

New VPN names will take effect after the next discovery cycle. To expedite discovery, execute **`etrestart.ovpl`**.

Figure 4 VPN Rename Tool



VPN Names Rename - Microsoft Internet Explorer

File Edit View Favorites Tools Help

VPN Rename

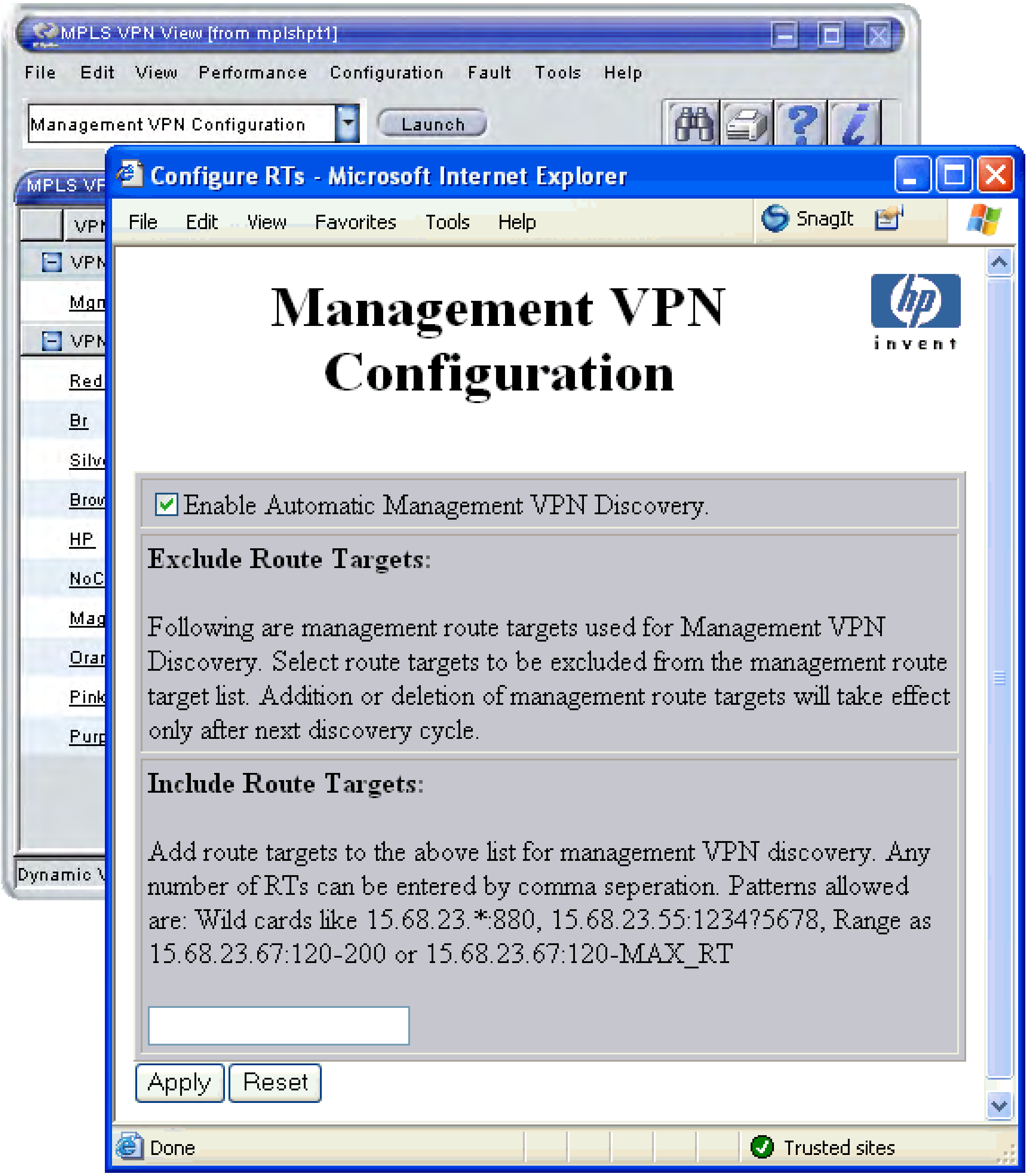
This will update $OV_CONF/VpnNames.txt file.New VPN names will take effect only after next discovery.After rename please run the discovery as $OV_BIN/etrestart.ovpl.

□	MgmtVpn_002	
□	Br	
□	Silver	
□	Brown	
□	HP	
□	NoCommonName_15	
□	Magenta	
□	Orange	
□	Pink	
□	Purple	
□	Red	

Launching Management VPN Configuration Tool

To launch the Management VPN Configuration view, select the `Management VPN Configuration` tool from the list box in the MPLS VPN view. See Figure 5.

Figure 5 Management VPN Configuration Tool


MPLS VPN View [from mplshpt1]
File Edit View Performance Configuration Fault Tools Help
Management VPN Configuration
Launch
MPLS VF
VPN
VPN
Mgn
VPN
Red
Br
Silv
Brov
HP
NoC
Mag
Orar
Pink
Purp
Dynamic V
Configure RTs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
SnagIt
invent

Management VPN Configuration

☑ Enable Automatic Management VPN Discovery.

Exclude Route Targets:

Following are management route targets used for Management VPN Discovery. Select route targets to be excluded from the management route target list. Addition or deletion of management route targets will take effect only after next discovery cycle.

Include Route Targets:

Add route targets to the above list for management VPN discovery. Any number of RTs can be entered by comma seperation. Patterns allowed are: Wild cards like 15.68.23.*:880, 15.68.23.55:12345678, Range as 15.68.23.67:120-200 or 15.68.23.67:120-MAX_RT

Apply Reset

Done Trusted sites

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*
- *Service Assurance Report Pack User Guide*
- *MPLS VPN Smart Plug-in Installation and Configuration 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:

  — 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 *NNM Smart Plug-ins Release Notes*, which can be found in `$OV_WWW/htdocs/` or `%OV_WWW%\htdocs` on your NNM management station.

2 Configuring the MPLS VPN Smart Plug-in

Introduction to MPLS VPN SPI Configuration

Two configuration files that are of importance to you are the `mpls.conf` file and the `MgmtVpn.cfg` file. Both files store configuration data that let you customize your MPLS VPN SPI deployment.

The configuration files are modified during the installation process based on setting information you enter during the initial configuration process, and can be modified after installation.

Modifying the MPLS VPN SPI Configuration File

The mpls.conf file stores configuration parameters for the MPLS VPN SPI. Most of these parameters are set during the installation process. The `mpls.conf` file is located in the following directory:

UNIX: `$OV_CONF`

Windows: `%OV_CONF%`

Figure 6 shows a sample `mpls.conf` file.

Figure 6 Sample `mpls.conf` File

```
IPSLA_TRIG=true
FREQUENCY=600
TIMEOUT=100
PINGMIB_TRIG=true
PINGMIBFREQ=600
PINGMIBTIMEOUT=1
PINGMIBPOLLINTERVAL=60
HANDLE_ADDR_EVENTS=false
MAX_VPN_MSG_SIZE=20
HANDLE_RAMS_EVENTS=true
RAMSVPN_NAMESYNC=false
```

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

- `IPSLA_TRIG`

  Determines whether the IP SLA reachability configuration process runs after MPLS VPN discovery completes. Possible values are `true` and `false`.

- `FREQUENCY`

  Sets the standard frequency (in seconds) for IP SLA 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 standard timeout value (in milliseconds) for IP SLA 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 standard 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 standard 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.

- `PINGMIBPOLLINTERVAL`

  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, set `HANDLE_ADDR_EVENTS=true`. Possible values are `true` and `false`.

- `MAX_VPN_MSG_SIZE`

  Sets the number of affected VPNs that can be included in a single MPLS VPN SPI event. When the number of affected VPNs is very large and/or VPN names are long, the NNM Alarms Browser may truncate the event text. To prevent this truncation, set the `MAX_VPN_MSG_SIZE` parameter to a value appropriate for your network. If the event condition affects more VPNs than the configured number, the MPLS VPN SPI splits the list of affected VPNs among multiple copies of the event. By default, a single MPLS VPN SPI event contains up to 20 affected VPNs.

- `RAMSVPN_NAMESYNC`

  Determines whether the MPLS VPN SPI synchronizes VPN names with the RAMS appliance. Possible values are `true` and `false`. For more information, see the *NNM Smart Plug-in for MPLS VPN User's Guide*.

- `HANDLE_RAMS_EVENTS`

  Determines whether the MPLS VPN SPI responds to RAMS events regarding the status of label switch paths between PE router pairs in the network core. Possible values are `true` and `false`.

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

1. Using a text editor (such as vi) that works directly with the raw file data and does not insert extra characters, edit the `mpls.conf` file to contain the desired values.
2. The MPLS VPN SPI reads the `mpls.conf` file each time it needs information from the file.
3. Changing the value of the `FREQUENCY`, `TIMEOUT`, `PINGMIBFREQ`, or `PINGMIBTIMEOUT` parameters affects new or modified reachability test definitions only. Existing reachability test definitions do not change.

Modifying Management VPN Configuration

Most of the Management VPN configuration parameters are set during the installation process. To modify any Management VPN configuration after installation, use the Management VPN configuration tool.

Limitations of the Management VPN Discovery

The Management VPN discovery algorithm places all management route targets belonging to a VRF into one Management VPN. Hence, a VRF can belong to only one Management VPN.

For example, assume three Management VPNs are defined: `Mgmt1` with route target `rt1`, `Mgmt2` with route target `rt2`, and `Mgmt3` with route target `rt3`. Assume a VRF exists that contains the three route targets `rt1`,`rt2` and `rt3`. The Management VPN discovery algorithm discovers the three Management VPNs and displays them as a single Management VPN.

Including and Excluding Route Targets

To include or exclude a route target from the next discovery cycle, do the following:

1. From the MPLS VPN view, select `Management VPN Configuration` view from the list box, and then click **Launch**. See Figure 5.

2. From the Exclude Route Target section, select the route targets to remove from the management route targets.
3. From the Include Route Target section, enter the route targets to add to the management route target. You can use any of the supported filtering syntax as described in Filtering Route Targets on page 33.
4. Click **Apply**.

Management route target modifications will take effect after the next discovery cycle. To expedite discovery, execute **`etrestart.ovpl`**.

Modifying the Management VPN Configuration File

The `MgmtVpn.cfg` file stores configuration parameters for management route targets. Most of these parameters are set during the installation process.

Under normal circumstances, you should not edit this file. Configuration of the Management VPNs can be achieved through the MPLS VPN views.

The `MgmtVpn.cfg` file is located in the following directory:

UNIX: `$OV_CONF`

Windows: `%OV_CONF%`

Figure 7 shows an example of the `MgmtVpn.cfg` file.

Figure 7 Sample MgmtVpn.cfg File

```
MGMTDISCOFLAG   1

RT-PATTERN  12356:12345678      ACTIVE

RT-PATTERN  13.0.5.6:123445678  INACTIVE

DISCO-RT    12367:475869        ACTIVE

DISCO-RT    18.4.6.6:12367      INACTIVE
```

The parameters in the `MgmtVpn.cfg` file are as follows:

- `MGMTDISCOFLAG`

  `MGMTDISCOFLAG` turns on or off the automatic discovery of the management route targets.

  - If set to 1, the MPLS VPN SPI turns on automatic management VPN discovery.
  - If set to 0, the MPLS VPN SPI turns off automatic management VPN discovery.

- RT-PATTERN

  When a route target is added to or excluded from the management route target list, the MPLS VPN SPI writes the route target pattern into the MgmtVpn.cfg file. RT-PATTERN sets the management route targets as valid or invalid.

  - An ACTIVE setting indicates the pattern is valid.
  - When the route target is excluded from the management route target list, the management route target becomes INACTIVE.

- DISCO-RT

  DISCO-RT is a list of route targets identified as management route targets by the automatic management VPN discovery algorithm.

  - An ACTIVE setting indicates the list of active management route targets that have been automatically discovered.
  - An INACTIVE setting inactivates a route target as a management route target discovered by the MPLS VPN SPI. After the next discovery, the INACTIVE route targets are treated as belonging to a traffic VPN.

  To reactivate an inactive route target, the inactive entry should be deleted from the MgmtVpn.cfg configuration file. The MPLS VPN views remove the inactive entries when modified through the MPLS VPN views, except when the route target is being reactivated by using a wildcard route target.

  For example, suppose a wildcard route target pattern 12345:1567??? is specified as inactivate in the MgmtVpn.cfg file. If you add the pattern 12345:1567890 by using the MPLS VPN views (or modifying the configuration file), you must delete the inactive wildcard pattern 12345:1567??? from the MgmtVpn.cfg file.

- RTCNT_THRESHOLD

  RTCNT_THRESHOLD is a heuristic approach for classifying route targets with a high number of occurrences. The threshold value is set depending on the count of occurrences of route targets. If a route target count is greater than 3.5 times that of the next lower route target count, the route target is taken as the threshold above which the route targets qualify as management route targets.

- RTCNT_THRESHOLD defaults to 3.5.
- To change RTCNT_THRESHOLD, add the following line in the MgmtVpn.cfg configuration file:

  ```
  RTCNT_THRESHOLD <any number>
  ```

- SPOKE-THRESHOLD

  This is a heuristic approach for classifying a hub-and-spoke topology.

  - The SPOKE-THRESHOLD defaults to 80 percent, which means that at least 80% of the nodes in the respective hub-and-spoke topology should be spokes.

    For example, if the total number of occurrences of a route target equals 500, the SPOKE-THRESHOLD equals 80% of 500, or 400. So, at least 400 of these nodes should be spokes.

  - To change the SPOKE-THRESHOLD, add the following line in the MgmtVpn.cfg configuration file:

    ```
    SPOKE-THRESHOLD <any number>
    ```

Filtering Route Targets

You can configure a list of route targets that the MPLS VPN SPI ignores when computing VPN relationships and when synchronizing VPN names with a RAMS appliance.

The following configuration file specifies a list of route targets that the MPLS VPN SPI should ignore during discovery:

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

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

1 Using a text editor (such as vi) that works directly with the raw file data and does not insert extra characters, 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. The route target identifier must be contained within single quotations marks.

   For supported filter syntax, see Supported Route Target Filtering Syntax on page 34.

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 8.

Figure 8 Sample 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'
);
```

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

Supported Route Target Filtering Syntax

The values clause contains two values separated by a colon (:). The first value identifies the AS number or the IP address of the BGP extended community attribute. Wildcarding is permitted.

The second value identifies the assigned number of the route target, and can take one of three forms:

- A specific route target identifier.
- A range of route target identifiers. To create a range of route targets, use a hyphen (-) between two values to identify which route targets are to be ignored.

  The second integer must be larger than the first integer, and must be a 32 bit or 16 bit number, depending on whether the administrator subfield contains an AS number or an IP address, respectively.

  A `MAX_RT` parameter can be used in the place of the second value of the range to exclude all route targets larger than the first integer listed. This parameter is context-sensitive.
- A route target identifier where one of the digits in the assigned number subfield are wildcarded.

  The hook character (`?`) can be used to represent a single digit within an assigned number value. Any combination of digits and hooks are supported as long as the value represents a 32 bit or 16 bit number, depending on whether the administrator subfield contains an AS number or an IP address, respectively.

Examples

- To exclude route targets 12345:11, 12345:12, and 12345:13, enter the following:

  `‘12345:11-13’`
- To exclude all route targets for AS 12345, enter the following:

  `‘12345:0-MAX_RT’`
- To exclude all route targets for AS 12345 that differ by one digit (12345:1**1**3, 12345:1**2**3, 12345:1**3**3, and so on), enter the following:

  `‘12345:1?3’`
- To exclude all IP addresses that start with 17.68.23 (17.68.23.11, 17.68.23.12 and so on), enter the following:

  `‘17.68.23.*:880’`

Renaming VPNs

To change the name of VPNs, see Launching the VPN Rename Tool on page 22.

3 Understanding MPLS VPN Discovery

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.

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

Management VPN Discovery

Your network management environment can include management route targets that belong to several or all of the VPNs in the network. The management route targets let you manage traffic flow within the MPLS VPN network.

The MPLS VPN SPI can automatically discover management route targets as well as differentiate between traffic and management VPNs. VPNs that are created by the service provider to manage Customer Edge devices are called Management VPNs. VPNs that are provided by the service provider for carrying the customer data and traffic are called Traffic VPNs.

Management VPNs can also be configured prior to discovery. While automatically discovering management route targets, the MPLS VPN SPI checks if those route targets form a hub-and-spoke topology as per recommendations of RFC2547bis. Use the MPLS VPN views to set up and modify the Management VPNs. For more details, see Available MPLS VPN Views on page 17.

Discovery Details Found in MPLS VPN Views

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, ovet_daJunMplsVpn, and ovet_daJunEMplsVpn. 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 lets the MPLS VPN SPI correctly discover simple network topologies that are fully meshed as well as complex network topologies that are formed from a hub and spoke design.

The MPLS VPN SPI stores the VRF grouping relationships and the VPN names in the VpnNames.txt file.

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, use the VPN Rename view available from the MPLS VPN view. See Launching the VPN Rename Tool on page 22.

Table 1 shows several applications of the VPN naming algorithm.

Table 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
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

The Management VPNs are automatically named as MgmtVpn_001, MgmtVpn_002, and so on. The suffixed numbers are for differentiating the VPNs only and have no special meaning. Management VPN names, however, can be renamed using the VPN Rename option available from the MPLS VPN view. See Launching the VPN Rename Tool on page 22. Changes to the Management VPN names display in the MPLS VPN views after the next discovery cycle.

Synchronizing VPN Names with RAMS

When the HP OpenView Route Analytics Management System (RAMS) for mBGP is integrated with NNM, the MPLS VPN SPI can configure the RAMS appliance with the route targets and VPN names that the MPLS VPN SPI has discovered. The MPLS VPN SPI then synchronizes these VPN names at the end of each MPLS VPN discovery cycle. This behavior is on by default and is controlled with the RAMSVPN_NAMESYNC parameter in the mpls.conf file. For information, see "RAMSVPN_NAMESYNC" in the *MPLS VPN Smart Plug-in Installation and Configuration Guide*.

When the MPLS VPN SPI has control of VPN name synchronization (RAMSVPN_NAMESYNC=true), the MPLS VPN SPI disables the `Import Customer Configuration` pane in the RAMS `VPN Explorer` to prevent users from changing the shared configuration. The pane is still visible but will not accept any data. The `VPN Customer Configuration Table` that displays the current VPN names is still functional.

➤ To view the `Import Customer Configuration` pane and the `VPN Customer Configuration Table`, expand the `VPN` folder in the `VPN Explorer`, then expand the `Configuration` folder, and then click `Customers`.

If you turn off VPN name synchronization by setting RAMSVPN_NAMESYNC=false, you may need to stop and restart the MPLS VPN SPI status manager to re-enable the `Import Customer Configuration` pane in the `VPN Explorer`:

- *UNIX*:

```
$OV_BIN/ovstop MPLS_sm
$OV_BIN/ovstart MPLS_sm
```

- *Windows*:

```
%OV_BIN%\ovstop MPLS_sm
%OV_BIN%\ovstart MPLS_sm
```

4 Understanding Events from the MPLS VPN Smart Plug-in

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 the clearing event is received within 10 minutes of the fault event.

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 44
- Network Core Status Events on page 49
- Reachability Status Change Events on page 50
- OVPI Report Pack Threshold Events on page 54

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 2 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 15. 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 2 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_Standby_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/ VRRP backup device.	`OV_APA_IF_DOWN`/ 5893012	APA
		`OV_IF_Down`/ 58916867	netmon
`OV_MPLS_VPN_IF_Up`/ 70001001 Clears the `OV_MPLS_VPN_IF_Down`, `OV_MPLS_VPN_IFAdmin_Down`, or `OV_MPLS_VPN_Standby_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

Table 2 Enriched Router Status Events Generated by the MPLS VPN SPI (cont'd)

Enriched Event Name/ HP OpenView Event OID	Meaning	Input Event Name/ HP OpenView Event OID	Input Event Source
OV_MPLS_VPN_Node_Down/ 70001002	A PE router is down.	OV_APA_NODE_DOWN/ 58983013	APA
		OV_Node_Down/ 58916865	netmon
OV_MPLS_VPN_Node_Up/ 70001003 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_BOARD_DOWN/ 58983035	APA
OV_MPLS_VPN_Board_Up/ 70001012 Clears the OV_MPLS_VPN_Board_Down event from the Alarms Browser	A card with a VRF-enabled interface is back up.	OV_APA_BOARD_UP/ 58983034	APA

Table 2 Enriched Router Status Events Generated by the MPLS VPN SPI (cont'd)

Enriched Event Name/ HP OpenView Event OID	Meaning	Input Event Name/ HP OpenView Event OID	Input Event Source
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
OV_MPLS_VPN_Conn_Up/ 70001010 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
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

Table 2 Enriched Router Status Events Generated by the MPLS VPN SPI (cont'd)

Enriched Event Name/ HP OpenView Event OID	Meaning	Input Event Name/ HP OpenView Event OID	Input Event Source
OV_MPLS_VPN_Node_Normal/ 70001005 Clears the OV_MPLS_VPN_Node_Unknown event from the Alarms Browser	The status of an intermediate device in the VRF path is now normal.	OV_TOPOLOGY_Status_Change_Notification/ 60001101	netmon
OV_MPLS_VPN_Addr_Down/ 70001009 **NOTE**: This alarm is *off* by default. See "HANDLE_ADDR_EVENTS" in Modifying the MPLS VPN SPI Configuration File on page 27 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
OV_MPLS_VPN_Addr_Up/ 70001008 Clears the OV_MPLS_VPN_Addr_Down event from the Alarms Browser **NOTE**: This alarm is *off* by default. See "HANDLE_ADDR_EVENTS" in Modifying the MPLS VPN SPI Configuration File on page 27 for more information.	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 OSPF or IS-IS option to 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 3.

Table 3 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 web-based online help for NNM (URL: `http://nnm_mgmt_station:3443/OvCgi/OvWebHelp.exe`).

Table 4 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 15. 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 **Enriched Network Core Status Events Generated by the MPLS VPN SPI**

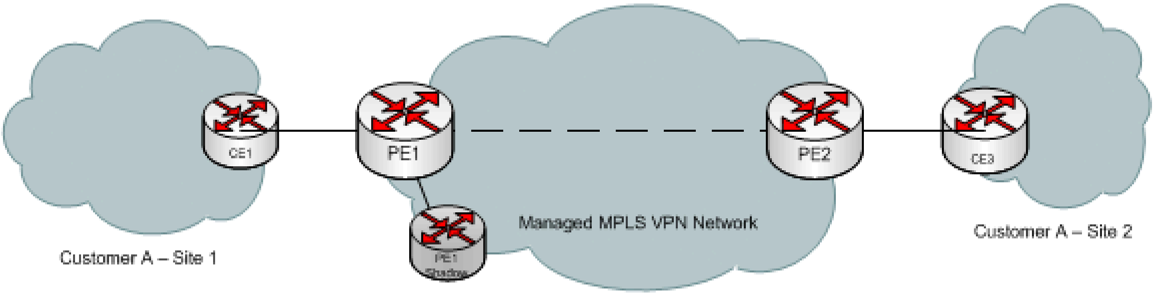
Enriched Event Name/ HP OpenView Event OID	Meaning
OV_MPLS_VPN_RAMS_Path_Down/ 70001018	The path between two PE routers is down.
OV_MPLS_VPN_RAMS_Path_Up/ 70001019 Clears the OV_MPLS_VPN_RAMS_Path_Down event from the Alarms Browser	The path between two PE routers is back up.
OV_MPLS_VPN_RAMS_Path_Worse/ 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 9 shows an example of a path through an MPLS VPN network.

Figure 9 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)
- Shadow router to Any router (for example, PE1 Shadow to CE3)

Table 5 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 15.

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 5 Enriched Reachability Status Events Generated by the MPLS VPN SPI

Enriched Event Name/ HP OpenView Event OID	Meaning	Notes
OV_MPLS_VPN_IPSLA_FAIL/ 70001006	There is no connectivity over the label switch path between two devices.	Received the rttMonTimeout Notification trap with rttMonCtrlOperTimeoutOccurred/ .1.3.6.1.4.1.9.9.42.1.2.9.1.6 = TRUE
OV_MPLS_VPN_IPSLA_PASS/ 70001007 Clears the OV_MPLS_VPN_ IPSLA_FAIL event from the Alarms Browser	The connectivity over the label switch path between two devices is restored.	Received the rttMonTimeout Notification trap with rttMonCtrlOperTimeoutOccurred/ .1.3.6.1.4.1.9.9.42.1.2.9.1.6 = FALSE
OV_MPLS_VPN_PingMib_ Fail/ 70001015	There is no connectivity over the label switch path between two devices.	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 connectivity over the label switch path between two devices is restored.	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) IP Service Level Agreement (IP SLA) monitoring agent for reachability tests. (IP SLA replaces the Service Assurance Agent, or SAA.) Each test is an ICMP echo request from one PE or CE router to another PE or CE router in the VPN. The IP SLA monitoring agent calculates the round trip time of its echo request. If the round trip time exceeds the timeout value for that test, the IP SLA monitoring agent 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 IP SLA test failure to NNM.

If the failed IP SLA 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 IP SLA test succeeds, the IP SLA monitoring agent 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 IP SLA failure trap, sends a new, enriched trap describing the reachability change in status to NNM. This new event clears the IP SLA 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.

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.

Shadow Router Reachability Tests

Juniper and Cisco router reachability tests can be performed on a shadow router, which is a low end router connected to the provider edge router. Shadow routers relieve the PE router from performing the reachability tests and let the PE router focus on typical VPN traffic. All shadow routers perform reachability tests that are VPN (VRF) aware.

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 6 lists and describes the threshold events that the MPLS VPN SPI receives from OVPI.

Table 6 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 50 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 IP Service Level Agreement (IP SLA) monitoring agent that uses the values of the Cisco RTTMON 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 52.

- 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 53.

➤ Juniper router reachability tests are not supported on Juniper E Series routers.

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.
- A *SHADOW-ANY VRF aware reachability test* checks the connectivity from a shadow router to any other router over a predefined VRF 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 65.

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 IP SLA) or Juniper (for ping MIB) CE router.

➤ 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 9 on page 51 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* supported in this environment.

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 7 on page 62 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`, `CE-CE`, and `SHADOW-ANY`:

  - 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.
  - Use `SHADOW-ANY` for any shadow router reachability 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 IP SLA 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, and SHADOW-ANY 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.

  Possible values are TEST_CONFIG and IPSLA_TEST_SYNC:

  - Use TEST_CONFIG to cause the MPLS VPN SPI reachability test configuration process to configure this test in the RTTMON MIB or ping MIB (as appropriate) on the source router when you import this file.
  - Use IPSLA_TEST_SYNC to prevent the reachability test configuration process from changing the configuration of this test in the RTTMON MIB on the source router. If you use this value, you must explicitly configure this reachability test in the RTTMON MIB on the source router using the Cisco IOS commands.

There is no counterpart to IPSLA_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-*un*aware tests only.

  - For a PE-PE VRF-*un*aware 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-*un*aware 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.

- SITE_INFO —Required for shadow router reachability tests. The name of the VRF or customer. This is an information only field used to enrich events with VRF information.

  The format for SITE_INFO parameter is *VRF name@ConnectedPERouter*, where VRF corresponds to the VRF configured on the provider edge router connected to the shadow router.

- 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 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 IP SLA 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 Modifying the MPLS VPN SPI Configuration File on page 27.

- 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 IP SLA 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 IP SLA 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 Modifying the MPLS VPN SPI Configuration File on page 27.

- 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 7 shows example reachability test definitions. The values of the SOURCE and CONFIG_TYPE parameters determine whether each test is an IP SLA or ping MIB reachability test.

Table 7 Sample Reachability Test Definitions

IP SLA Test Definitions	Ping MIB Test Definitions
PE-PE VRF-Unaware Reachability Test Samples	

BEGIN
TEST_TYPE=PE-PE
SOURCE=mplspe01
DEST=mplspe04
VRF=
OP=ADD
CONFIG_TYPE=TEST_CONFIG
SRC_ADDR=
DEST_ADDR=
SET_COMM=ntcprivate
FREQUENCY=600
TIMEOUT=100
TAG=
END
	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

PE-PE VRF-Aware Reachability Test Samples	

BEGIN
TEST_TYPE=PE-PE
SOURCE=mplspe01
DEST=mplspe04
VRF=Red_East
OP=ADD
CONFIG_TYPE=TEST_CONFIG
SRC_ADDR=
DEST_ADDR=10.97.255.27
SET_COMM=ntcprivate
FREQUENCY=600
TIMEOUT=100
TAG=
END
	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

Table 7 Sample Reachability Test Definitions (cont'd)

IP SLA Test Definitions	Ping MIB Test Definitions
PE-CE Local VRF-Aware Reachability Test Samples	

BEGIN
TEST_TYPE=PE-CE
SOURCE=mplspe01
DEST=mplsce01
VRF=Red_East
OP=ADD
CONFIG_TYPE=TEST_CONFIG
SRC_ADDR=
DEST_ADDR=10.10.20.1
SET_COMM=ntcprivate
FREQUENCY=600
TIMEOUT=100
TAG=
END
	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

CE-CE End-to-End Reachability Test Samples	

Table 7 Sample Reachability Test Definitions (cont'd)

IP SLA Test Definitions	Ping MIB Test Definitions

BEGIN
TEST_TYPE=CE-CE
SOURCE=mplsce02
DEST=mplsce04
VRF=
OP=ADD
CONFIG_TYPE=TEST_CONFIG
SRC_ADDR=
DEST_ADDR=
SET_COMM=ntcprivate
FREQUENCY=600
TIMEOUT=100
TAG=
END
	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

Shadow Router Reachability Test Sample	

BEGIN
TEST_TYPE=SHADOW-ANY
SOURCE=mplsshadow.hp.com
DEST=mplsce06.hp.com
VRF= Blue
OP=ADD
CONFIG_TYPE=TEST_CONFIG
SRC_ADDR=
DEST_ADDR=
SITE_INFO=Blue@mplspe01.hp.com
SET_COMM=remote-community
FREQUENCY=600
TIMEOUT=100
TAG=
END	

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 66 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.

The MPLS VPN SPI installation process sets the values of several parameters that control unassisted reachability test configuration in the mpls.conf file. The MPLS VPN SPI reads the mpls.conf file each time it performs reachability test configuration.

- The IPSLA_TRIG, FREQUENCY, and TIMEOUT attributes in the mpls.conf file control unassisted reachability test configuration on Cisco routers.
- The PINGMIB_TRIG, PINGMIBFREQ, PINGMIBTIMEOUT, and PINGMIBPOLLINTERVAL attributes in the mpls.conf file control unassisted reachability test configuration on Juniper routers.

See Modifying the MPLS VPN SPI Configuration File on page 27.

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

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 66.

If you do not want to supply the SNMP set community string for a Cisco router, you can configure the RTTMON MIB on the router using the Cisco IOS commands. See Configuring IP SLA Using the Cisco IOS Commands on page 68.

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 66.

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 `xnmsnmpconf` 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.

➤ Shadow router reachability tests cannot be configured as unassisted reachability tests.

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.

   ➤ 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 57.

      — 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.

Configuring IP SLA Using the Cisco IOS Commands

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

Each IP SLA test includes a unique tag name. The MPLS VPN SPI uses this tag name to identify the IP SLA 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 IP SLA tests via the Cisco IOS commands, follow these steps:

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

   - `BEGIN`
   - `TEST_TYPE`
   - `SOURCE`
   - `DEST`
   - `VRF` (if applicable)
   - `OP`
   - `CONFIG_TYPE = IPSLA_TEST_SYNC`
   - `SRC_ADDR` (if applicable)
   - `DEST_ADDR` (if applicable)
   - `END`

   For information about the file format, see Reachability Test Definitions File Format on page 58.

2. Generate a unique tag value for each IP SLA test:

   ```
   reachability_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 IP SLA test definitions file that includes a tag name for each IP SLA test definition.

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

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 Step 2.

Figure 10 shows an example of a Cisco IOS command sequence for configuring an IP SLA test. For instructions on configuring your router, see the related Cisco documentation.

Figure 10 Example of Cisco IOS Commands for IP SLA 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

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” in the *MPLS VPN Smart Plug-in Installation and Configuration Guide* 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 74.
- Verify that the NNM environment variables have been sourced properly as described in Setting the NNM Environment Variables on page 75.
- Verify that the NNM services are operating properly as described in Verifying That the NNM Services Are Operating on the Management Station on page 75.

□ 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 77.

□ A VRF is missing from the PE Details View. (A VRF missing from the PE Details View can cause that PE router to be missing from the other MPLS VPN Views.)

There is an error or omission in the VRF configuration.

- Verify that this VRF is included in the VRF table on the PE router.
- Verify that there is at least one interface associated with the VRF.

□ 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 76.
- 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" in the *MPLS VPN Smart Plug-in Installation and Configuration Guide*.
- Verify that MPLS VPN discovery has occurred as described in Verifying That MPLS VPN Discovery Has Occurred on page 77.
- Verify that the MPLS VPN SPI is operating as described in Verifying That the MPLS VPN SPI Is Operating on page 76.
- Verify that the MPLS VPN SPI trap definitions are included in `trapd.conf`.

□ 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 49.

□ 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 78.

- Verify that the MPLS VPN SPI is operating. See Verifying That the MPLS VPN SPI Is Operating on page 76.

□ 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 *NNM Smart Plug-ins Release Notes* available on the Web at http://ovweb.external.hp.com/lpe/doc_serv under the **NNM Smart Plug-in for MPLS VPN** 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: Execute **`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 74.
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 are loaded. These MIBs are named in “MIB Dependencies” in the *MPLS VPN Smart Plug-in Installation and Configuration Guide*.

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
$OV_BIN/ovstatus -v ovet_daJunEMplsVpn
```

- Windows:

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

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 `ipsla.conf` and `ping_mib.conf` files store the IP SLA and ping MIB test definitions, respectively, in plain text. The `reachability_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:
  - `$OV_DB/reachability_tag.xml`
  - `$OV_DB/ipsla.conf` (optional, for reachability tests on Cisco routers)
  - `$OV_DB/ping_mib.conf` (optional, for reachability tests on Juniper routers)
- Windows:
  - `%OV_DB%\reachability_tag.xml`
  - `%OV_DB%\ipsla.conf` (optional, for reachability tests on Cisco routers)
  - `%OV_DB%\ping_mib.conf` (optional, for reachability tests on Juniper routers)

Recreating the reachability_tag.xml File

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

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

Recreating the ipsla.conf File

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

1 Log on to an edge router that is the source for one or more IP SLA tests.

2 Edit the Cisco RTTMON MIB to remove all IP SLA test configurations.

3 Repeat steps Step 1 and Step 2 for each edge router that is the source for one or more IP SLA tests in the MPLS VPN network.

4 On the MPLS VPN management station, delete the following file:

- UNIX: `$OV_DB/pe_pair.disc`
- Windows: `%OV_DB%\pe_pair.disc`

5 Ensure that the `IPSLA_TRIG` parameter in the `mpls.conf` file is set to `true`. See “IPSLA_TRIG” in Modifying the MPLS VPN SPI Configuration File on page 27.

6. Initiate Extended Topology discovery to rediscover the MPLS VPN topology. After MPLS VPN discovery completes, the NNM generates the `ipsla.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 Step 1 and Step 2 for each edge router that is the source for one or more ping MIB tests in the MPLS VPN network.
4. On the MPLS VPN management station, delete the following file:
   - UNIX: `$OV_DB/pe_pair.disc`
   - Windows: `%OV_DB%\pe_pair.disc`
5. Ensure that the `PINGMIB_TRIG` parameter in the `mpls.conf` file is set to `true`. See “PINGMIB_TRIG” in Modifying the MPLS VPN SPI Configuration File on page 27.
6. 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 71 matches your need.

The MPLS VPN View Is Not Available from Home Base

If the MPLS VPN view is not available from the list box on Home Base, try the following command:

UNIX: **`$OV_NEW_CONF/OVNNM-RUN/www/registration/dynamicViews/oneXmlFileCreator/oneXmlFileCreator.ovpl`**

Windows: **`%OV_WWW_REG%\dynamicViews\oneXmlFileCreator\oneXmlFileCreator.ovpl`**

Rebooting an Edge Router Removes the IP SLA Test Definitions from the RTTMON MIB

➤ This situation applies to Cisco routers only.

There is no way to protect the IP SLA 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 IP SLA 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.

Connectivity Issues with Juniper E Series

When a Juniper E Series router acts as a PE and has CE routers connected to the Juniper E Series router, the MPLS VPN SPI does not discover the connectivity.

➤ Juniper E Series routers and Juniper routers share the same icon representation in the MPLS VPN views.

To add connectivity, use the PE-to-CE Connection Editor utility as follows:

1 Create a file to define the connections that need to be made or deleted. The file must be named `peceEdits` and placed in the following location:

   `$OV_DB/nnmet/peceEdits`

2 For each connection to be created or deleted, add the following line to the `peceEdits` file.

   (‘<*PE IF Name*>’, ‘<*CE IF Name*>’, ‘VrfName’, <*cmd*>);

   where `cmd` is either `1`, `2`, or `3`. Enter `1` to add a PE to CE connection entry. Enter `2` to delete a PE to CE connection entry. Enter `3` to delete a VRF to PE interface relationship.

   `PE IF Name` and `CE IF Name` need to match the format as defined in the NNM topology. The interface names for the PE and CE are included in single quotes.

   To find the name of the interface as defined in NNM, check the `entityname` field in the `nwinterface` table. To list the names of the interfaces on the node, execute a query by using the `ovdwquery` utility, such as in the following query:

   select entityname from nwinterface where nodename = ‘*mynode.hp.com*’;

   `VrfName` is the name of the VRF as defined on this PE interface.

   The following is an example of a modified `peceEdits` file:

```
(‘rdnode01.hp.com[ 0 [ 11 ] ]’, ‘yournode.hp.com[ 0 [ 5 ] ]’, ‘Blue_East, 1);
(‘mplsPE04.hp.com[ 0 [ 22 ] ]’, ‘csnode.hp.com[ 0 [ 3 ] ]’, ‘Red_West’, 2);
(‘mplsPE04.hp.com[ 0 [ 22 ] ]’, ‘Red_West’, 3);
```

3 Execute the PE to CE Connection Editor utility:

   $OV_MAIN_PATH/support/MPLS/peceConnEdit.ovpl [-d]

where `-d` turns on debugging.

4 Restart the OV application server to see the GUI changes:

UNIX:

```
$OV_BIN/ovstop ovas
$OV_BIN/ovstart ovas
```

Windows:

```
%OV_BIN%\ovstop ovas
%OV_BIN%\ovstart ovas
```

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 Launching the VPN Rename Tool on page 22.

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.

All VRFs Appear in One VPN - Not As You Expected

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

If you are aware of the route targets configured for the Management VPN, enter them through the management VPN configuration GUI. Else, enable automatic management VPN discovery in the GUI so that the MPLS VPN SPI will discover this route target and exclude it from traffic VPNs.

MPLS Events Are Not Being Correlated

If MPLS events are not being correlated as expected, try one of the following tips:

- Check if the MPLS VPN correlation rules are present in `$OV_CONF/ecs/circuits/PairWidse.ds`. The file should include entries specific to traps `700010*`.
- Check if the time window of the PairWise circuits is as required. By default, the time window is set to 10 minutes.

Discovery Has Discovered Non-management Route Targets As Management Route Targets

You can view the management route targets by using the Management VPN view. From the MPLS VPN views, you can delete any of the route targets that are not management route targets. Also, if you are aware of the management route targets that have not been discovered by the MPLS VPN SPI automatic discovery algorithm, the route target can be added using the MPLS VPN views. Addition or deletion of route targets take effect after the next discovery cycle.

Collecting Information for HP Support

If errors occur that are not documented in this guide, collect information about your system and configuration, and report the problem to your HP support representative. To automate the data collection process, HP offers two alternatives: HP OpenView Self Healing Client and the MPLS VPN SPI Data Collector.

HP OpenView Self Healing Client

The MPLS VPN SPI supports HP OpenView Self Healing, which is software that collects important system parameters, configuration details and files, and log and trace files from your systems and sends them to HP Support.

To install the HP OpenView Self Healing client, go to **http://support.openview.hp.com/self_healing_downloads.jsp**.

MPLS VPN SPI Data Collector

The MPLS VPN SPI data collector, `mplsspi_DataCollector`, gathers application configuration information specific to the MPLS VPN SPI.

To start the MPLS VPN SPI data collector, execute the following command:

UNIX:

```
$OV_MAIN_PATH/support/mpls/dc/mplsspi_DataCollector.ovpl
```

Windows:

```
%OV_MAIN_PATH%\support\mpls\dc\mplsspi_DataCollector.bat
```

When activated, the MPLS VPN SPI data collector extracts the configuration of the MPLS VPN SPI, including the version, operating system, and patch details. The data collector also collects configuration data from the following data and configuration files:

- UNIX:

  ```
  $OV_CONF/VpnNames.txt
  $OV_CONF/mpls.conf
  $OV_CONF/nnmet/agents/MplsVpn.cfg
  ```

$OV_CONF/VrfLite.cfg

$OV_DB/ipsla.conf

$OV_DB/pingmib.conf

$OV_DB/pe_pair.disc

$OV_DB/reachability_tag.xml

$OV_DB/tag_idx.xml

$OV_LOG/MPLS_RAMS25470.0.*

$OV_LOG/System.txt

$OV_PRIV_LOG/mpls_install.log

$OV_PRIV_LOG/MPLSStatusManager.log

$OV_PRIV_LOG/MPLSPingmibPoller.log

$OV_PRIV_LOG/ovet_disco.log

$OV_PRIV_LOG/ovet_disco.old.log

$OV_PRIV_LOG/ovet_daCiscoMplsVpn.log

$OV_PRIV_LOG/ovet_daJunMplsVpn.log

$OV_PRIV_LOG/ovas.log

$OV_PRIV_LOG/ovas.old.log

$OV_PRIV_LOG/ovas_err.log

$OV_TMP/mpls_pre_install.log

- Windows:

  %OV_CONF%\VpnNames.txt

  %OV_CONF%\mpls.conf

  %OV_CONF%\nnmet\agents\MplsVpn.cfg

  %OV_CONF%\VrfLite.cfg

  %OV_DB%\ipsla.conf

  %OV_DB%\pingmib.conf

  %OV_DB%\pe_pair.disc

  %OV_DB%\reachability_tag.xml

```
%OV_DB%\tag_idx.xml

%OV_LOG%\MPLS_RAMS25470.0.*

%OV_LOG%\System.txt

%OV_PRIV_LOG%\MPLSStatusManager.log

%OV_PRIV_LOG%\MPLSPingmibPoller.log

%OV_PRIV_LOG%/mpls_install.log

%OV_PRIV_LOG%\ovet_disco.log

%OV_PRIV_LOG%\ovet_disco.old.log

%OV_PRIV_LOG%\ovet_daCiscoMplsVpn.log

%OV_PRIV_LOG%\ovet_daJunMplsVpn.log

%OV_PRIV_LOG%\ovas.log

%OV_PRIV_LOG%\ovas.old.log

%OV_PRIV_LOG%\ovas_err.log

%OV_TMP%\mpls_pre_install.log
```

The results are posted to the following location:

UNIX: `%OV_MAIN_PATH/support/mpls/dc/results/`
Windows: `%OV_MAIN_PATH%\support\mpls\dc\results\`

The MPLS VPN SPI Data Collector may be used as an integrated component of the HP OpenView Self Healing Client, or as a standalone tool.

Index