# HP OpenView Reporting and Network Solutions

## MPLS VPN Smart Plug-in
**to**
**Network Node Manager**

## User's Guide

**Software Version: 2.1**

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


**Manufacturing Part Number: None**
**July 2004**

# Legal Notices

**Warranty.**

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

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

**Restricted Rights Legend.**

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

Hewlett-Packard Company
United States of America

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

**Copyright Notices.**



**Trademark Notices.**

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

UNIX® is a registered trademark of The Open Group.

# Contents

# Contents

# Contents

# Support

Please visit the HP OpenView web site at:

`http://openview.hp.com/`

There you will find contact information and details about the products, services, and support that HP OpenView offers.

You can go directly to the HP OpenView support web site at:

`http://support.openview.hp.com/`

The support site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

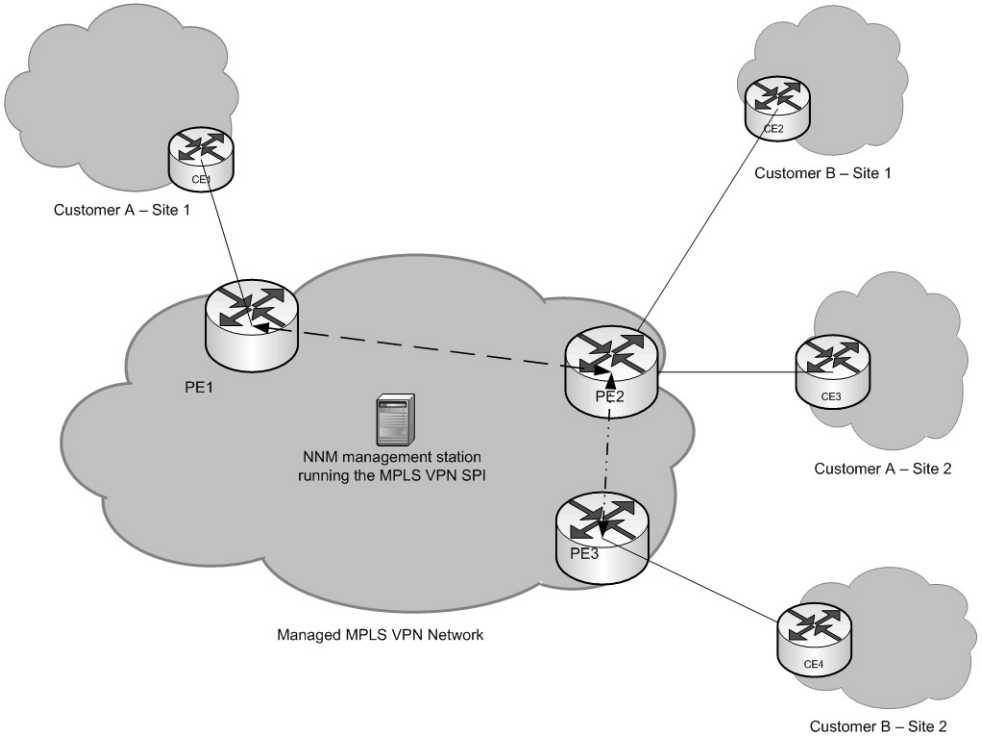
# 1 Introducing the MPLS VPN Smart Plug-in

# 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 matching VRFs from all network devices comprises the actual VPN. Figure 1-1 shows an example MPLS VPN network.

**Figure 1-1 Example MPLS VPN Network**



The HP OpenView Network Node Manager Smart Plug-in (SPI) for MPLS VPN provides additional value to HP OpenView Network Node Manager (NNM) by near real-time monitoring of the MPLS VPN edge routers. The provider edge (PE) routers sit on the perimeter of the service provider's network. They communicate with provider (P) routers in the MPLS VPN cloud and customer edge (CE) routers that are managed by the service provider's customers. The MPLS VPN SPI monitors the connectivity between the PE routers taking part in the VPN within the core MPLS network and discovers VPN network topology. It uses this information to map raw nodes, PE interfaces, and related traps to VPN service-affecting events.

The MPLS VPN SPI uses event enrichment, a process of identifying relationships between events and enriching the data contained in an event, to generate a smaller number of new events with the same or more detailed information content as the individual events. These events allow you to more effectively understand and react to a problem on your network. This faster reaction time reduces the mean time to repair (MTTR) problems within your MPLS VPN network and improves your quality of service.

For a list of the edge router devices that the MPLS VPN SPI supports, see "Router Requirements" on page 25.

In addition to near real-time diagnostics of PE and CE router infrastructure problems, the MPLS VPN SPI allows monitoring of the end-to-end path reachability between two PE routers taking part in a VPN. This monitoring is achieved using the Cisco Service Assurance Agent (SAA) testing based on the Cisco RTTMON MIB. The MPLS VPN SPI configures SAA echo tests between PE routers to test the reachability across edge routers. This testing gives real-time monitoring of the PE-PE connections and generates an SNMP event if a failure occurs. The MPLS VPN SPI also supports user-configured end-to-end reachability testing between two CE routers.

When HP OpenView Performance Insight (OVPI) is integrated with NNM, the MPLS VPN SPI works proactively with NNM and OVPI to provide analysis and reporting of both fault and performance data.

# Features and Benefits of the MPLS VPN SPI

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

- The MPLS VPN SPI monitors the status of the PE routers in MPLS VPN networks and reports device outages.
- For each CE router to which the service provider has access, the MPLS VPN SPI monitors the status of the CE router and the PE-CE connection.
- By enriching network status events, the MPLS VPN SPI generates new, more meaningful events for display in the NNM alarm browser.
- Optionally, the MPLS VPN SPI automatically configures reachability tests for valid PE-PE router pairs within a VPN.
- The MPLS VPN SPI allows users to configure various types of PE- and CE-specific reachability tests and generates events to indicate changes in the tested connections.
- When OVPI is installed, OVPI monitors the carrier access rate, SAA, and MPLS VPN counters and sends a trap to NNM when any counter crosses a configured threshold. The NNM alarm browser displays the trap as an alarm from which you can launch an OVPI report containing additional information about the interface that crossed the threshold.

# 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
- SAA echo test events for PE-PE, PE-CE, and CE-CE reachability tests
- OVPI threshold exceeded traps for MPLS VPN, SAA, and CAR threshold breaches

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

# User Interaction with the MPLS VPN SPI

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

- Observe alarms about situations that affect the status of one or more VPNs by monitoring alarms in the MPLS VPN alarms category. See "MPLS VPN Events" on page 14.
- Examine graphical and tabular representations of the MPLS VPN network through the windows available in the MPLS VPN Views. See "MPLS VPN Views" on page 16.
- 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 16.

## MPLS VPN Events

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

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

- `MPLS/VPN: VPN:VRF [`*`VRF`*`] Down due to [`*`interface`*`] IF down on node [`*`node`*`].`
- `MPLS/VPN: VPN:VRF(s) [`*`VRFlist`*`] Down due to node [`*`node`*`] down.`
- `MPLS/VPN: VPN:VRF(s) [`*`VRFlist`*`] Down due to card [`*`card`*`] down.`
- `MPLS/VPN: VPN:VRF(s) [`*`VRFlist`*`] Unknown status due to node [`*`node`*`] unknown status`
- `MPLS/VPN: SAA test failed between [`*`node1-node2`*`] affected VPN/VRF(s):[`*`VRFlist`*`]. Root cause is `*`cause`*`.`
- `MPLS/VPN: SAA test cleared between [`*`node1-node2`*`] affected VPN/VRF(s):[`*`VRFlist`*`]`
- `MPLS/VPN: VPN:VRF [`*`VRF`*`] Down due to [`*`interface`*`] IF ADDRESS down on node [`*`node`*`]`

- `MPLS/VPN: VPN:VRF [`*`VRF`*`] Down due to connection down between [`*`source_node`*`:`*`interface`*`] and [`*`destination_node`*`:`*`interface`*`]`

Some example messages follow:

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

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

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

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

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

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

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

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

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

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

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

  Or

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

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

## MPLS VPN Views

The MPLS VPN SPI has several views available:

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

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

### Launching MPLS VPN Views

There are several ways to reach the MPLS VPN View:

- To open the MPLS VPN View from the NNM GUI (ovw), click `Tools:Views->MPLS VPN`.
- 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`.

## Reports from OVPI

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

### Cross-Launching OVPI from the NNM Alarm Browser

To start OVPI from the NNM alarm browser, follow these steps:

1. Select an alarm in the MPLS VPN alarm 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 Extended Topology Map

To start OVPI from the Extended Topology map, follow these steps:

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

   A web browser window appears containing the `Report Launchpad`.
4. In the `Report Launchpad`, click the report to view.

### Cross-Launching OVPI from the MPLS VPN View

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

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

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

# Related Documentation

Refer to the following documents for more information:

- *Managing Your Network with HP OpenView Network Node Manager*
- *Using Extended Topology*
- *MPLS VPN Report Pack User Guide*
- *SAA Report Pack User Guide*

# 2 Installing the MPLS VPN Smart Plug-in

# Preparing for Installation

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

## Hardware Requirements

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

**Table 2-1 Recommended Disk Space Settings**

| Location | Size |
|---|---|
| *UNIX*: `$OV_MAIN_PATH`<br>*Windows*: `%OV_MAIN_PATH%` | 2 MB |

## Software Requirements

### Supported Operating Systems

The following operating systems are supported:

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

### Network Node Manager

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

- HP OpenView Network Node Manager Advanced Edition, version 7.5

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

### Verifying Proper Installation of Network Node Manager Advanced Edition

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

*UNIX*:

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

*Windows*:

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

### Determining Which Version of NNM is Installed

To determine which version of NNM is installed:

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

*Windows*: ***`install_dir`*`\bin\ovnnmversion`**

### Setting the NNM Environment Variables

To source the NNM environment variables:

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

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

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

## MIB Dependencies

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

- Cisco SMI MIB—Shipped with NNM and installed to the following location:

  *UNIX*: `$OV_SNMP_MIBS/Vendor/Cisco/CISCO-SMI.my`
  *Windows*: `%OV_SNMP_MIBS%\Vendor\Cisco\CISCO-SMI.my`

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

  *UNIX*: `/opt/OV/newconfig/MPLS/CISCO-RTTMON-MIB.my`
  *Windows*: `%OV_CONF%\MPLS\CISCO-RTTMON-MIB.my`

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

  *UNIX*: `$OV_SNMP_MIBS/Vendor/Juniper/jnx-smi.mib`
  *Windows*: `%OV_SNMP_MIBS%\Vendor\Juniper\jnx-smi.mib`

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

  *UNIX*: `$OV_SNMP_MIBS/Vendor/Juniper/jnx-vpn.mib`
  *Windows*: `%OV_SNMP_MIBS%\Vendor\Juniper\jnx-vpn.mib`

If the Cisco SMI MIB is loaded onto the NNM management station before you install the MPLS VPN SPI, the MPLS VPN SPI installation process loads the other required MIBs. Otherwise, you must manually load all required MIBs. For information, see “Verifying That MIBs Are Loaded” on page 77.

**NOTE** On the Windows operating system, the `Typical` NNM installation option does not load the Cisco SMI MIB. You can choose the `Custom` NNM installation option and specify to load the SNMP MIBs. Alternatively, you can load this MIB as described in “Verifying That MIBs Are Loaded” on page 77.

## Router Requirements

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

- Cisco routers with Internetwork Operating System (IOS) version 12.2(15)T that support MplsVpnMIB.

  The MPLS VPN SPI can perform status management, reachability test configuration, and reachability status reporting for these devices.

- Juniper M and T series routers with Juniper Operating System (JunOS) version 6 that support jnx-smi.mib and jnx-vpn.mib.

  The MPLS VPN SPI can perform status management only for these devices.

## Performance Insight

Optionally, you can install HP OpenView Performance Insight (OVPI) 5.0 on a separate server and use the NNM / OVPI Integration Module to integrate the trending analysis by OVPI with the fault management capability of NNM. If you integrate OVPI and NNM, threshold breaches detected by OVPI appear in the NNM alarm browser and the Report Launchpad window provides access to numerous OVPI reports.

# Updating SAA Test Definitions from a Previous Version of the MPLS VPN SPI

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

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

   a. Export all existing SAA tests into a file:

      - *UNIX*:

        **$OV_BIN/saa_config.ovpl -e /tmp/saa_test_A**

      - *Windows*:

        **%OV_BIN%\saa_config.ovpl -e C:\temp\saa_test_A**

      For more information, see “Changing SAA Test Definitions” on page 65.

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

      For more information, see “Configuring SAA Using the MPLS VPN SPI” on page 67.

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

      - *UNIX*:

        **$OV_BIN/saa_config.ovpl -i /tmp/saa_test_A**

      - *Windows*:

        **%OV_BIN%\saa_config.ovpl -i C:\temp\saa_test_A**

      For more information, see “Changing SAA Test Definitions” on page 65.

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

2. Back up the `VpnNames.txt` file:
   - *UNIX*:

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

   - *Windows*:

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

3. Remove the MPLS VPN SPI.

   For instructions, see “Removing the MPLS VPN SPI” on page 35.

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

   For instructions, see “Installing the MPLS VPN SPI” on page 30.

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

   For instructions, see “Configuring SNMP Access” on page 37.

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

   For instructions, see “Discovery Process” on page 40.

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

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

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

      - *Windows*:

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

      For more information, see “Changing SAA Test Definitions” on page 65.

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

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

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

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

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

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

For more information, see “Configuring SAA Using the MPLS VPN SPI” on page 67.

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

- *UNIX*:

  **`$OV_BIN/saa_config.ovpl -i /tmp/saa_test_B`**

- *Windows*:

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

For more information, see "Changing SAA Test Definitions" on page 65.

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

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

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

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

   For more information, see "Changing VPN Names in the MPLS VPN SPI Configuration" on page 44.

# Installing the MPLS VPN SPI

If you encounter problems while performing any of these installation steps, see Chapter 6, "Troubleshooting the MPLS VPN Smart Plug-in," on page 71 or the *Release Notes for MPLS VPN Smart Plug-in to Network Node Manager* for possible assistance.

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

**NOTE** If you are installing the MPLS VPN SPI over an existing installation of the MPLS VPN SPI, see "Updating SAA Test Definitions from a Previous Version of the MPLS VPN SPI" on page 26 for specific instructions.

## Installing the MPLS VPN SPI on a UNIX Operating System

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

1. Log on to the NNM management station as user `root`.
2. Verify that the NNM environment variables are sourced properly.

   For instructions, see "Setting the NNM Environment Variables" on page 23.
3. If you are using an Oracle database for the NNM data warehouse, follow these steps to configure Oracle for the MPLS VPN SPI:

   a. **`cd $OV_CONF/nnmet/topology/extensibility`**

   b. **`cp UpdateColumn.xslt UpdateColumn.xslt.orig`**

   c. Using any text editor, delete the word `COLUMN` from line 36 of the `UpdateColumn.xslt` file.

4. Mount the Reporting and Network Solutions CD-ROM.
5. From the Reporting and Network Solutions CD-ROM directory, start `setup`

   The installation script verifies that the target system has the correct version of NNM installed. If NNM is not installed, the installation script exits with an error. See "Handling Other Problems" on page 81 for more information.
6. Follow the instructions on the screen to install the MPLS VPN SPI. Table 2-2 lists the decisions you will be asked to make during the installation process.

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

| Option | Description |
|---|---|
| List of product types to install | Select to install the NNM Smart Plug-ins. |
| List of SPIs to install | Select to install the MPLS VPN SPI. |
| Start MPLS VPN discovery? | Type **yes** to initiate Extended Topology discovery including MPLS VPN discovery at the end of the installation.<br>Type **no** to leave the MPLS VPN network undiscovered. If you enter no, The MPLS VPN network is not discovered until the next time you run Extended Topology discovery. See "Discovery Process" on page 40. |
| Configure SAA tests at the end of each MPLS VPN discovery cycle? | Type **yes** to have the MPLS VPN SPI automatically update the SAA MIB on each managed PE router with the SAA test definitions after MPLS VPN discovery completes. If you enter yes, ensure that the SNMP configuration database contains the set community string for each PE router. See "Initial Configuration" on page 36.<br>Type **no** to prevent automatic updates to the SAA MIBs. If you enter no, the MPLS VPN SPI updates the SAA MIB upon explicit command only. See "SAA Configuration" on page 66.<br>You can change the automatic configuration setting. See "Setting SAA Configuration Parameters" on page 66. |

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

| Option | Description |
|---|---|
| SAA test frequency | Type the number of seconds between SAA test executions. The default value is 600 seconds (10 minutes).<br>You can change the SAA test frequency. See "Setting SAA Configuration Parameters" on page 66. |
| SAA test timeout | Type the number of milliseconds before an SAA test times out. The default value is 100 milliseconds.<br>You can change the SAA test timeout value. See "Setting SAA Configuration Parameters" on page 66. |

## Installing the MPLS VPN SPI on a Windows Operating System

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

1. Log on to the NNM management station as user `administrator`.
2. Verify that the NNM environment variables are sourced properly.

   For instructions, see "Setting the NNM Environment Variables" on page 23.
3. If you are using an Oracle database for the NNM data warehouse, follow these steps to configure Oracle for the MPLS VPN SPI:

   a. **`cd %OV_CONF%\nnmet\topology\extensibility`**

   b. **`copy UpdateColumn.xslt UpdateColumn.xslt.orig`**

   c. Using any text editor, delete the word `COLUMN` from line 36 of the `UpdateColumn.xslt` file.
4. Insert the Reporting and Network Solutions CD-ROM into the CD-ROM drive.

5. The CD-ROM should start automatically. If it does not, go to the Reporting and Network Solutions CD-ROM directory, and then double-click `setup.bat`.

   The installation script verifies that the target system has the correct version of NNM installed. If NNM is not installed, the installation script exits with an error. See "Handling Other Problems" on page 81 for more information.

6. Follow the instructions on the screen to install the MPLS VPN SPI. Table 2-3 lists the decisions you will be asked to make during the installation process.

**Table 2-3 Windows Installation Options for the MPLS VPN SPI**

| Option | Description |
|---|---|
| List of product types to install | Select to install the NNM Smart Plug-ins. |
| List of SPIs to install | Select to install the MPLS VPN SPI. |
| Start MPLS VPN discovery? | Type **yes** to initiate Extended Topology discovery including MPLS VPN discovery at the end of the installation.<br><br>Type **no** to leave the MPLS VPN network undiscovered. If you enter no, The MPLS VPN network is not discover until the next time you run Extended Topology discovery. See "Discovery Process" on page 40. |
| Configure SAA tests at the end of each MPLS VPN discovery cycle? | Type **yes** to have the MPLS VPN SPI automatically update the SAA MIB on each managed PE router with the SAA test definitions after MPLS VPN discovery completes. If you enter yes, ensure that the SNMP configuration database contains the set community string for each PE router. See "Initial Configuration" on page 36.<br><br>Type **no** to prevent automatic updates to the SAA MIBs. If you enter no, the MPLS VPN SPI updates the SAA MIB upon explicit command only. See "SAA Configuration" on page 66.<br><br>You can change the automatic configuration setting. See "Setting SAA Configuration Parameters" on page 66. |

**Table 2-3 Windows Installation Options for the MPLS VPN SPI**

| Option | Description |
|---|---|
| SAA test frequency | Type the number of seconds between SAA test executions. The default value is 600 seconds (10 minutes).<br>You can change the SAA test frequency. See “Setting SAA Configuration Parameters” on page 66. |
| SAA test timeout | Type the number of milliseconds before an SAA test times out. The default value is 100 milliseconds.<br>You can change the SAA test timeout value. See “Setting SAA Configuration Parameters” on page 66. |

**NOTE** The installation process creates the `C:\tempschlist` file. This file is not used after the installation process completes. You can safely delete it.

# Removing the MPLS VPN SPI

**NOTE** Removing the MPLS VPN SPI does not delete the MPLS VPN alarms from the NNM alarm browser. When you no longer need these alarms, delete them manually using the alarm browser delete functionality.

## Removing the MPLS VPN SPI on a UNIX Operating System

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

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

   ```
   mpls_unconfig.ovpl
   ```

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

   ```
   /usr/sbin/pkgrm HPOvMPLS
   /usr/sbin/pkgrm HPOvCisMPLSAgt
   ```

## Removing MPLS VPN SPI on a Windows Operating System

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

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

   ```
   mpls_unconfig.ovpl
   ```

**NOTE** The removal process creates the `C:\tempschlist` file. This file is not used after the removal process completes. You can safely delete it.

# Initial Configuration

The MPLS VPN SPI uses NNM Advanced Edition functionality to monitor the health of the virtual private networks in a multiprotocol label switching (MPLS VPN) environment.

## Configuring SNMP Polling Access

The MPLS VPN SPI relies on NNM knowing the correct status of the nodes and interfaces of the provider edge (PE) and customer edge (CE) routers in the MPLS VPN network. NNM determines this status information using the netmon process to perform status polling. netmon must be aware of and able to reach each node and interface.

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

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

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

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

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

   - If the interface card does *not* have an IP address, add the IP address of the managed node to the `netmon.snmpStatus` file as described in step 2.

2. As determined in step 1, add IP address information to the `netmon.snmpStatus` file. This file is located in the following directory:

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

   a. If the `netmon.snmpStatus` file does not exist, create it in the specified directory.

b. If possible, add IP address wildcards to cover multiple IP addresses that cannot be reached directly from the NNM management station.

   Use a single line for each IP address wildcard entry.

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

   Use a single line for each specific IP address entry.

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

netmon uses SNMP requests of the ifIndex, ifOperStatus, and ifAdminStatus MIB objects to determine the status of these interface cards.

## Configuring SNMP Access

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

**NOTE** This access is a requirement for automatic configuration of SAA echo tests. If you do not specify the set community string for an edge router, you must directly configure the SAA echo tests for that router. For instructions, see "Configuring SAA Using the Cisco IOS Commands" on page 69.

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

1. Start the SNMP configuration utility:
   - *UNIX*: **`$OV_BIN/xnmsnmpconf`**
   - *Windows*: **`%OV_BIN%\xnmsnmpconf`**
2. In the `SNMP Configuration` window, specify the set community string for each edge router.

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

## Configuring SNMP Trap Forwarding

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

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

# 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 Cisco router devices to determine the provider edge (PE) router configuration and virtual route forwarding (VRF) groupings. Additionally, it uses subnet information in the Extended Topology database to identify the interfaces in each customer network that are connected to the PE routers in the managed network and identifies these as customer edge (CE) routers.

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

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

- Details about the PE routers:
  - VRF details (from the mplsVpnVrfTable)
  - Interface-to-VRF relationships (from the mplsVpnInterfaceConfTable)
  - Route target import/export lists (from the mplsVpnVrfRouteTargetTable)
- Details about the outward-facing interface cards on the PE routers:
  - The interface number (the MplsVpnInterfaceConfIndex from the mplsVpnInterfaceConfTable)
- 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 (from the mplsVpnVrfRouteTargetTable)

MPLS VPN discovery is integrated with the Extended Topology discovery of NNM Advanced Edition. The process ovet_daCiscoMplsVpn is the MPLS VPN discovery agent. It runs whenever the Extended Topology discovery runs.

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

## VPN Naming Algorithm

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

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

The MPLS VPN SPI stores the VRF grouping relationships and the VPN names in the VpnNames.txt file. This file is described in "Changing VPN Names in the MPLS VPN SPI Configuration" on page 44.

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 each VRF in the group has the same name and that name would be a unique VPN name, then assign that text string as the VPN name for that VRF group.
   - If each VRF in the group has 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 `Unknown_` followed by the VPN internal identification number.

   To change a VPN name, manually edit the `VpnNames.txt` file to change the VPN name to something meaningful for your network as described in "Changing VPN Names in the MPLS VPN SPI Configuration" on page 44.

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

**Table 3-1 Example VPN Naming**

| VRFs in the VPN | Selected VPN Name | Explanation |
|---|---|---|
| Blue<br>Blue | Blue | All VRF names are the same; choose that name |
| Red_East<br>Red_West | Red_ | The common initial characters |
| Red_North<br>Red_South | Red__5 | The common initial characters with underscore and the VPN internal identifier appended for uniqueness |
| Blue<br>Green<br>Yellow | Unknown_1 | VRF names cannot be matched or formed into a meaningful name |

# Changing VPN Names in the MPLS VPN SPI Configuration

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

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

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

```
VpnName  VPN_Internal_Id  VrfList
```

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

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

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

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

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

Figure 3-1 shows an example `VpnNames.txt` file.

**Figure 3-1 Example VpnNames.txt file**

```
Blue    1    Device1<<>>Blue    Device2<<>>Blue    Device3<<>>Blue
Unknown_2    2    Device3<<>>Red    Device4<<>>Green    Device5<<>>Purple
Cust    3    Device6<<>>CustEast    Device7<<>>CustWest
    Device8<<>>CustNorth    Device9<<>>CustSouth
```

To change an assigned VPN name:

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

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

# 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 alarm browser when appropriate.

The MPLS VPN SPI status manager process (`MPLS_sm`) is an NNM service managed by `ovspmd`. It logs 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 49
- "Reachability Status Change Events" on page 52
- "OVPI Report Pack Threshold Events" on page 55

## 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 alarm browser displays these enriched events in the `MPLS VPN` category.

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

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

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

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

| Enriched Event Name/ HP OpenView Event OID | Meaning | Input Event Name/ HP OpenView Event OID | Input Event Source |
|---|---|---|---|
| OV_MPLS_VPN_ADDRDOWN/ 70001009 | An interface card on a device in the affected VPN is not responding to a ping request of its IP address | OV_APA_ADDR_DOWN/ 58983011 | APA |
| None; clears the OV_MPLS_VPN_ADDRDOWN event from the alarm browser | An interface card is now responding to a ping request of its IP address | OV_APA_ADDR_UP/ 58983001 | APA |
| OV_MPLS_VPN_IFDOWN/ 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 |
| None; clears the OV_MPLS_VPN_IFDOWN event from the alarm browser | A CE-facing interface configured for the MPLS VPN on a PE router is back up | OV_APA_IF_UP/ 5893002 | APA |
| | | OV_IF_Up/ 58916866 | netmon |
| OV_MPLS_VPN_NODEDOWN/ 70001002 | A PE router is down | OV_APA_NODE_DOWN/ 58983013 | APA |
| | | OV_Node_Down/ 58916865 | netmon |
| None; clears the OV_MPLS_VPN_NODEDOWN event from the alarm browser | A PE router is back up | OV_APA_NODE_UP/ 58983003 | APA |
| | | OV_Node_Up/ 58916864 | netmon |

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

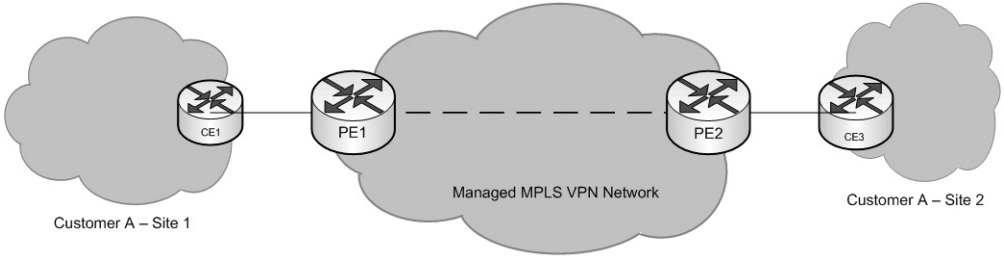
| Enriched Event Name/ HP OpenView Event OID | Meaning | Input Event Name/ HP OpenView Event OID | Input Event Source |
|---|---|---|---|
| OV_MPLS_VPN_Card_Down/ 70001013 | A card with a VRF-enabled interface is down | OV_APA_CARD_DOWN/ 58983035 | APA |
| None; clears the OV_MPLS_VPN_Card_Down event from the alarm browser | A card with a VRF-enabled interface is back up | OV_APA_CARD_UP/ 58983034 | APA |
| OV_MPLS_VPN_CONNDOWN/ 70001011 | The connection between two interface cards on devices in the affected VPN is not functioning correctly | OV_APA_CONNECTION_DOWN/ 58983014 | APA |
| None; clears the OV_MPLS_VPN_CONNDOWN event from the alarm browser | The connection between two interface cards is now functioning correctly | OV_APA_CONNECTION_UP/ 58983004 | APA |
| OV_MPLS_VPN_NODEUNKNOWN/ 70001004 | The status of an intermediate device in the VRF path cannot be determined | OV_TOPOLOGY_Status_ Change_Notification/ 60001101 | netmon |

# 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 alarm browser displays these enriched events in the `MPLS VPN` category.

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

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




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

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

The CE-CE end-to-end reachability test looks at the connectivity of the source CE router to the near PE router to the far PE router to the far CE router. If the source CE router is not a Cisco device, the MPLS VPN SPI breaks this test into separate SAA tests that cover the entire path.

## Cisco Router Reachability Tests

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

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

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

Table 4-2 lists the enriched events that the MPLS VPN SPI generates for SAA test conditions. The format of these events is described in “MPLS VPN Events” on page 14. For information about the variable bindings associated with an event, see the `trapd.conf` file in the following directory:

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

**Table 4-2 Enriched Reachability Status Events Generated by the** MPLS VPN SPI

| Enriched Event Name/ HP OpenView Event OID | Meaning | SAA MIB Object/ OID = Value |
|---|---|---|
| OV_MPLS_VPN_SAA_FAIL/ 70001006 | The connection between two devices is down | rttMonCtrlOperTimeoutOccurred/ .1.3.6.1.4.1.9.9.42.1.2.9.1.6 = TRUE |
| OV_MPLS_VPN_SAA_PASS/ 70001007<br>Clears the OV_MPLS_VPN_SAA_FAIL event from the alarm browser | The connection between two devices is back up | rttMonCtrlOperTimeoutOccurred/ .1.3.6.1.4.1.9.9.42.1.2.9.1.6 = FALSE |

## 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 alarm browser. It does not add any information to these events.

Table 4-3 lists and describes the threshold events that the MPLS VPN SPI receives from OVPI.

**Table 4-3 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 below the acceptable threshold. |
| VPN_ERROR_PCT | The average packet error percentage of all interfaces in the VPN is below the acceptable threshold. |
| VPN_SNMPRESPONSE | The average SNMP response from OVPI to the device/interface of all interfaces in the VPN is below the acceptable threshold. |
| VRF_OPERSTATUS | A VRF is in a non-operational status. |

# 5 Using Service Assurance Agent

# Service Assurance Agent

Cisco Internetwork Operating System (IOS) Service Assurance Agent (SAA) is an embedded software agent in Cisco IOS devices. It performs active monitoring of network health and can verify that service level agreements are being met. The values of the Cisco RTTMON MIB (SAA MIB) variables on a router determine the SAA configuration for that device. You can configure SAA to perform differently on each router in the network.

The MPLS VPN Smart Plug-in (SPI) configures the SAAs 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 using the ICMP echo request. If a reachability test times out, the SAA 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 alarm browser.

"Reachability Status Change Events" on page 52 describes how the MPLS VPN SPI processes these traps.

## SAA Tests

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 SAA on PE1 to send an ICMP echo request from PE1 to PE2. The MPLS VPN SPI also configures the SAA on PE2 to send an ICMP echo request 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.

# SAA Test Definitions

SAA test definitions are stored in an MPLS VPN SPI internal file. The MPLS VPN SPI processes this file and configures each SAA in the MPLS VPN network. Use the saa_config.ovpl command to access the current SAA test definitions. For information on this command, see "Changing SAA Test Definitions" on page 65.

To configure an SAA test, create a new test definitions file and import that file into the MPLS VPN SPI SAA test definitions file. You can export the current SAA 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 SAA test definitions to the MPLS VPN SPI. Whenever the SAA test definitions file changes, the MPLS VPN SPI updates the SAA test configurations on each managed PE router and each Cisco CE router.

If a non-Cisco CE router is specified as the source router in an SAA test configuration, the MPLS VPN SPI breaks the test into multiple segments that can be configured on a PE router. For example, consider the following network path:

CE1-PE1-PE2-CE2

If CE1 is not a Cisco device, then the MPLS VPN SPI splits the test into a PE1-CE1 reachability test and a PE1-CE2 reachability test. It configures these tests on the PE1 device.

## SAA Test Definitions File Format

The SAA test definitions file is a flat text file that defines the ICMP echo requests for each SAA to perform. The file contains one or more `BEGIN`/`END` pairs, each of which defines a specific test. Figure 5-1 on page 63 through Figure 5-4 on page 64 show example SAA test definitions.

The elements within an SAA test definition are as follows:

- `BEGIN`—The element that starts the definition of an SAA test.

- TEST_TYPE—The type of SAA test to be defined. Possible values are PE-PE, PE-CE, and CE-CE:
  - Use PE-PE for a PE-PE VRF-unaware test or for a PE-PE VRF-aware test.
  - Use PE-CE for a PE-local CE VRF-aware test.
  - Use CE-CE for an end-to-end CE-CE test.
- SOURCE—The selection name of the source router for the SAA test. This value must match the selection name in the NNM topology database. The source router is the initiator of the SAA test.
- DEST—The selection name of the destination router for the SAA test. This value must match the selection name in the NNM topology database. The destination router is the device that is verified by the SAA test.
- VRF—Optional. This value applies to PE-PE VRF-aware and PE-CE VRF-aware tests only. 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`
- OP—The operation to be performed when this file is imported into the SAA test configuration tool. Possible values are ADD, DELETE, and MODIFY.
- CONFIG_TYPE—The configuration method to be used. Possible values are SAA_TEST_CONFIG and SAA_TEST_SYNC:
  - Use SAA_TEST_CONFIG to cause the MPLS VPN SPI SAA configuration process to configure this SAA test in the SAA MIB on the source router when you import this file.
  - Use SAA_TEST_SYNC to prevent the SAA configuration process from changing the configuration of this SAA test in the SAA on the source router. If you use this value, you must explicitly configure this SAA test in the SAA MIB on the source router using the Cisco IOS commands.

- SAA_SRC_ADDR—Optional. The IP address of the source interface card on the router for the SAA 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_DEST_ADDR—Optional. The IP address of the destination interface card on a router for the SAA test. The address must be within the VPN address range that is reachable through the specified destination router for this SAA 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.
- 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 SAA test definition. This value applies only when the value of the CONFIG_TYPE parameter is SAA_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 SAA test definition, the value of the FREQUENCY parameter in the mpls.conf file when this SAA test is configured will be used for this test. For information on the mpls.conf file, see "Setting SAA Configuration Parameters" on page 66.
- TIMEOUT—Optional. The length of time allowed for an ICMP echo response before considering that the test failed. Specify the number of milliseconds for the timeout value.

  If this element is not included in the SAA test definition, the value of the TIMEOUT parameter in the mpls.conf file when this SAA test is configured will be used for this test. For information on the mpls.conf file, see "Setting SAA Configuration Parameters" on page 66.

- TAG—The identifier for this SAA 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 an SAA test.

**Figure 5-1 Example Test Definition for a PE-PE VRF-Unaware SAA Test**

```
BEGIN
TEST_TYPE=PE-PE
SOURCE=mplspe01
DEST=mplspe04
VRF=
OP=ADD
CONFIG_TYPE=SAA_TEST_CONFIG
SAA_SRC_ADDR=
SAA_DEST_ADDR=
SET_COMM=ntcprivate
FREQUENCY=600
TIMEOUT=100
TAG=
END
```

**Figure 5-2 Example Test Definition for a PE-PE VRF-Aware SAA Test**

```
BEGIN
TEST_TYPE=PE-PE
SOURCE=mplspe01
DEST=mplspe04
VRF=Red_East
OP=ADD
CONFIG_TYPE=SAA_TEST_CONFIG
SAA_SRC_ADDR=
SAA_DEST_ADDR=10.97.255.27
SET_COMM=ntcprivate
FREQUENCY=600
TIMEOUT=100
TAG=
END
```

**Figure 5-3 Example Test Definition for a PE-CE Local VRF-Aware SAA Test**

```
BEGIN
TEST_TYPE=PE-CE
SOURCE=mplspe01
DEST=mplsce01
VRF=Red_East
OP=ADD
CONFIG_TYPE=SAA_TEST_CONFIG
SAA_SRC_ADDR=
SAA_DEST_ADDR=10.10.20.1
SET_COMM=ntcprivate
FREQUENCY=600
TIMEOUT=100
TAG=
END
```

**Figure 5-4 Example Test Definition for a CE-CE End-to-End SAA Test**

```
BEGIN
TEST_TYPE=CE-CE
SOURCE=mplsce02
DEST=mplsce04
VRF=
OP=ADD
CONFIG_TYPE=SAA_TEST_CONFIG
SAA_SRC_ADDR=
SAA_DEST_ADDR=
SET_COMM=ntcprivate
FREQUENCY=600
TIMEOUT=100
TAG=
END
```

## Changing SAA Test Definitions

You can view and change the current SAA test definitions:

- To view the current SAA test definitions:

  **`saa_config.ovpl -e filename`**

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

- To create new or modified SAA test definitions:

  **`saa_config.ovpl -i filename`**

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

See “Configuring SAA Using the MPLS VPN SPI” on page 67 for step-by-step instructions on how to change SAA test definitions.

# SAA Configuration

By default, the MPLS VPN SPI updates its SAA test definitions at the completion of MPLS VPN discovery. It then configures the SAA MIB on each managed router with any changes to the existing SAA test definitions. See “Setting SAA Configuration Parameters” on page 66.

Because the MPLS VPN SPI communicates with an SAA using SNMP, unassisted configuration of SAA tests requires access to the SNMP set community string for each router. See “Configuring SAA Using the MPLS VPN SPI” on page 67.

If you do not want to supply the SNMP set community string for a router, you can configure the SAA MIB on the router using the Cisco IOS commands. See “Configuring SAA Using the Cisco IOS Commands” on page 69.

## Setting SAA Configuration Parameters

The MPLS VPN SPI installation process sets the values of several parameters that control unassisted SAA configuration. These parameters are stored in the file:

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

Figure 5-5 shows an example `mpls.conf` file.

**Figure 5-5 Example mpls.conf File**

```
SAA_TRIG=true
FREQUENCY=600
TIMEOUT=100
```

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

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

To change the parameters for SAA configuration via the MPLS VPN SPI:

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

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

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

## Configuring SAA Using the MPLS VPN SPI

Unassisted SAA 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 router access to NNM for all of its management functions.
- Supply the community string in the imported SAA test definitions file. This method gives router access to the MPLS VPN SPI for SAA test configuration only.

By default, the MPLS VPN SPI creates VRF-unaware SAA tests for each PE-PE router pair in each VPN in the network.

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

1. Create an SAA test definitions file:

   **`saa_config.ovpl -e filename`**

   *`filename`* contains the current SAA test definitions.

2. Using any text editor, in *`filename`*, define the SAA tests to be performed in the SAA test definitions file:

   a. As needed, modify the existing definitions:

   - To change an existing test definition, make the appropriate edits to the test definition, and then set the `OP` parameter to `MODIFY`.
   - To delete an existing test definition, set the `OP` parameter to `DELETE`.

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

   b. As needed, add new test definitions:

   - Follow the format of the test definitions file.
   - Set the `OP` parameter to `ADD`.

   c. As needed, supply the SNMP set community string for each SAA 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 SAA 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 SAA test definition.

3. Import the updated SAA test definitions:

   **`saa_config.ovpl -i`** ***`filename`***

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

## Configuring SAA Using the Cisco IOS Commands

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

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

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

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

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

   For information about the file format, see “SAA Test Definitions File Format” on page 60.

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

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

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

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

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

   Figure 5-6 shows an example Cisco IOS command sequence for configuring an SAA test. For instructions on configuring your router, see the related Cisco documentation.

**Figure 5-6 Example Cisco IOS Commands for SAA Configuration**

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

# 6 Troubleshooting the MPLS VPN Smart Plug-in

# Troubleshooting Checklist

**NOTE**

If you are trying to install the MPLS VPN Smart Plug-in (SPI) over an existing version, remove the MPLS VPN SPI as described in "Removing the MPLS VPN SPI" on page 35 before performing the MPLS VPN SPI installation steps.

If this installation is an update from a previous version of the MPLS VPN SPI, see "Updating SAA Test Definitions from a Previous Version of the MPLS VPN SPI" on page 26.

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 23.
  - ❑ Verify that the NNM environment variables have been sourced properly as described in "Setting the NNM Environment Variables" on page 23.
  - ❑ 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 78.

- No events appear in the MPLS VPN alarm 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 77.
  - ❑ 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" on page 36.
  - ❑ Verify that MPLS VPN discovery has occurred as described in "Verifying That MPLS VPN Discovery Has Occurred" on page 78.
  - ❑ Verify that the MPLS VPN SPI is operating as described in "Verifying That the MPLS VPN SPI Is Operating" on page 76.

- No SAA test events appear in the MPLS VPN alarm browser.

  The MPLS VPN SPI is not receiving SAA 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 SAA test definitions exist. See "Verifying SAA Test Definitions" on page 79.
  - ❏ Verify that the MPLS VPN SPI is operating. See "Verifying That the MPLS VPN SPI Is Operating" on page 76.

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

# Verifying 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 23.
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`**
   - *Windows*: **`%OV_BIN%\ovstatus -v`**

   The `MPLS_sm` process should be running.

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

   - *UNIX*:

     ```
     $OV_BIN/ovstop -c
     $OV_BIN/ovstart -c
     ```

   - *Windows*:

     ```
     %OV_BIN%\ovstop -c
     %OV_BIN%\ovstart -c
     ```

## Verifying That MIBs Are Loaded

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

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

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

2. Verify that the MIBs named in "MIB Dependencies" on page 24 are loaded.

3. If one or more of the required MIBs is not loaded, add it using this window.

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

# Verifying That MPLS VPN Discovery Has Occurred

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

- *UNIX*:

  ```
  $OV_BIN/ovstatus -v ovet_daCiscoMplsVpn
  $OV_BIN/ovstatus -v ovet_daJunMplsVpn
  ```

- *Windows*:

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

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

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

# Verifying SAA Test Definitions

The `saa_tag.xml` and `saa.conf` files store the SAA test definitions that the MPLS VPN SPI configures on the PE routers. The `saa_tag.xml` file stores these test definitions in XML format.

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

- *UNIX*: `$OV_DB/saa_tag.xml saa.conf`
- *Windows*: `%OV_DB%\saa_tag.xml saa.conf`

## Recreating the saa_tag.xml File

If the `saa_tag.xml` file does not exist or has size 0 and the `saa.conf` file does exist, follow these steps to recreate the `saa_tag.xml` file:

1. Export the current SAA test definitions to a file:
   - *UNIX*:

     **`$OV_BIN/saa_config.ovpl -e /tmp/current_saa.txt`**
   - *Windows*:

     **`%OV_BIN%\saa_config.ovpl -e C:\temp\current_saa.txt`**
2. Edit the `temp_current_saa.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/saa_config.ovpl -i /tmp/current_saa.txt`**
   - *Windows*:

     **`%OV_BIN%\saa_config.ovpl -i C:\temp\current_saa.txt`**

   The `saa_tag.xml` file should now exist.

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

## Recreating the saa.conf File

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

1. Log on to an edge router that is the source for one or more SAA tests.
2. Edit the Cisco RTTMON MIB to remove all SAA test configurations.
3. Repeat steps 1 and 2 for each edge router that is the source for one or more SAA tests in the MPLS VPN network.
4. Ensure that the `SAA_TRIG` parameter in the `mpls.conf` file is set to `true`. See "Setting SAA Configuration Parameters" on page 66.
5. Initiate Extended Topology discovery to rediscover the MPLS VPN topology. After MPLS VPN discovery completes, the NNM generates the `saa.conf` file.

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

# 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 72 matches your need.

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

**NOTE** This situation applies Cisco routers only.

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

To work around this situation:

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

  **`write mem`**

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

## PE Router Symbols Show Red in NNM

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

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

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

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

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

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

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

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

- Upon success, `snmpwalk` displays the values of the system variables.

  If there are multiple LAN cards, the PE router symbol should now be a diamond shape.

- Upon failure, `snmpwalk` displays the message “No response arrived before timeout.”

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

## VPN Names Are Confusing

You can configure VPN names that make sense for your environment. See “Changing VPN Names in the MPLS VPN SPI Configuration” on page 44.

## A Change to the MPLS VPN Configuration Does Not Appear

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

# Collecting Information for HP Support

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

1. Take note of the error.
2. Verify that NNM is operating. For instructions, see "Verifying That the NNM Services Are Operating on the Management Station" on page 75.
3. Gather the following information for your HP support representative:
   - Data and configuration files:

     *UNIX*:

     — `$OV_DB/Vpn_Info.xml`

     — `$OV_CONF/VpnNames.txt`

     — `$OV_CONF/mpls.conf`

     *Windows*:

     — `%OV_DB%\Vpn_Info.xml`

     — `%OV_CONF%\VpnNames.txt`

     — `%OV_CONF%\mpls.conf`
   - SAA export file (`current_saa.txt`):

     Create the export file:

     — *UNIX*:

     ```
     $OV_BIN/saa_config.ovpl -e /tmp/current_saa.txt
     ```

     — *Windows*:

     ```
     %OV_BIN%\saa_config.ovpl -e
     C:\temp\current_saa.txt
     ```

- The file `ovobjprint.output`:

  Create the output file:

  — *UNIX*:

  ```
  $OV_BIN/ovobjprint > /tmp/ovobjprint.output
  ```

  — *Windows*:

  ```
  %OV_BIN%\ovobjprint > C:\temp\ovobjprint.output
  ```

- Topology of your MPLS VPN network including:
  — Connectivity information
  — Names, IP addresses
- VPN information:
  — PE router – VRF – Interface relationships
  — VPN details (which VRF on which PE router corresponds to which VPN)
- Screenshots as appropriate:
  — Alarm browser showing events

  (Modify the column widths of the browser to display as much of the event message text as possible.)

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

# Index