HP Network Node Manager i Software Smart Plug-in for MPLS

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

Software Version: 9.00

Deployment Guide

Document Release Date: May 2010
Software Release Date: May 2010

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

Acrobat® is a trademark of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

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

Microsoft and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, refer to the `license-agreements` directory on the NNMi product DVD.

Printed in the U.S.

Documentation Updates

The title page of this document 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://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

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

Visit the HP Software Support web site at:

www.hp.com/go/hpsoftwaresupport

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

HP Software online 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 valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into 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 sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1 Introducing the iSPI for MPLS

HP Network Node Manager i Software Smart Plug-in for MPLS (Multi Protocol Label Switching) (NNMi iSPI for MPLS) helps you to extend the capability of HP Network Node Manager i Software (NNMi) to monitor the overall health of the network.

You can plan the deployment of the iSPI for MPLS based on how NNMi is deployed in the environment. While planning the deployment, consider the following areas to achieve an optimum size and performance of the system:

- Number of MPLS objects
- Deployment of the iSPI for MPLS in a High Availability (HA) environment.
- Deployment of the iSPI for MPLS in an Application Failover environment
- Deployment of the iSPI for MPLS along with other iSPIs (iSPI for IP Multicast, iSPI Performance for QA, RAMS, and iSPI Performance forMetrics/ NPS).
- Deployment of the iSPI for MPLS in a Global Network Manager (GNM) environment.

Preparing for Deployment

Before you start deploying the iSPI for MPLS, you must plan the installation based on your deployment requirements. You must identify the ideal deployment scenarios for the supported configuration and make sure that all the prerequisites are met before you begin the installation process.

Factors that impact the deployment of the iSPI for MPLS include the type of database configured with NNMi and the size of the network that you want to monitor. In addition, make sure to install the latest NNMi patches before installing the iSPI for MPLS.

To install and configure the iSPI for MPLS in an HA and application failover environment, see the HA and Application Failover section of *NNMi Deployment Reference Guide*.

Read the following NNMi documents before you start installing and configuring the iSPI for MPLS:

- *HP Network Node Manager i Software Installation Guide, 9.00*
- *HP Network Node Manager i Software Deployment Reference Guide, 9.00*
- *HP Network Node Manager i Software Release Notes, 9.00*
- *HP Network Node Manager i Software Support Matrix, 9.00*

In addition, read the following iSPI for MPLS documents before you start deploying the iSPI for MPLS:

- *HP Network Node Manager Smart Plug-in for MPLS Installation Guide, 9.00*
- *HP Network Node Manager Smart Plug-in for MPLS Release Notes, 8.10*
- *HP Network Node Manager Smart Plug-in for MPLS Support Matrix, 8.10*

For current versions of all documents listed here, go to: **http://h20230.www2.hp.com/selfsolve/manuals.**

Environment Variables Used in the iSPI for MPLS Documents

The iSPI for MPLS documents use the following NNMi environment variables to refer to file and directory locations. The default values are listed here. Actual values depend upon the selections made during NNMi installation.

- On Windows Server 2008, the NNMi installation process creates the following system environment variables, so they are always available to all users:
  - *%NnmInstallDir%*: `<drive>\Program Files\HP\HP BTO Software`
  - *%NnmDataDir%:* `<drive>\ProgramData\HP\HP BTO Software`

- Windows Server 2003, the NNMi installation process creates the following system environment variables, so they are always available to all users:
  - %NnmInstallDir%: `<drive>\Program Files\HP\HP BTO Software`
  - *%NnmDataDir%:* `<drive>\Documents and Settings\All Users\Application Data\HP\HP BTO Software`
- On UNIX systems, you must manually create the following environment variables
  - *$NnmInstallDir:* `/opt/OV`
  - *$NnmDataDir:* `/var/opt/OV`

2 Deploying the iSPI for MPLS

The iSPI for MPLS and NNMi must be installed on the same management server. To install and configure NNMi on a management server, see the *NNMi Installation Guide and Deployment Reference*.

You can deploy the iSPI for MPLS for the following scenarios:

- Installing NNMi and iSPI for MPLS together on a management server. NNMi and iSPI for MPLS are both configured together.
- Installing the iSPI for MPLS on the management server where NNMi is already installed and configured.
- Installing the iSPI for MPLS in a Global Network Management environment.
- Installing NNMi, iSPI Performance for Metrics/ NPS, and iSPI for MPLS on the same management server.
- Installing NNMi and iSPI for MPLS in a management server and the iSPI Performance for Metrics/ NPS on a dedicated server.
- Installing the iSPI for MPLS with iSPI for IP Multicast, RAMS, and iSPI Performance for Quality Assurance.

Deploy the iSPI for MPLS and NNMi Together

To deploy the iSPI for MPLS on a management server, follow these steps:

1. Start the NNMi installation process.
2. Create a New User with the Web Service Client Role from the NNMi console.

Make sure to use the same database type (Postgres Embedded or Oracle) as NNMi when you are installing the iSPI for MPLS.

3 Install the iSPI for MPLS, 9.00. For more information, see the *iSPI for MPLS Installation Guide*.

4 Start the iSPI for MPLS processes by using the command: **`ovstart -c mplsjboss.`**

5 Log on with the administrative privileges to use the `MPLS Configuration` workspace. If you have the list of Route Targets (RTs) to be excluded in the network, you can add the RTs to be excluded from the `MPLS Configuration` workspace. Similarly, you can group the Pseudowires based on the attributes such as Id or encapsulation type to discover VPWS VPNs. These configurations help in discovering the L3VPNs and L2VPNs.

You can add the list of RTs to be excluded anytime after starting the iSPI for MPLS processes.

6 Seed the MPLS nodes from the NNMi console. The NNMi discovery process starts after you seed the nodes and MPLS-enabled nodes are discovered along with NNMi nodes. For more information, see *NNMi Online Help.*

7 Wait for sometime till the iSPI for MPLS nodes are discovered. Log on to the NNMi console and then verify the availability of the MPLS workspace and MPLS views.

Deploy the iSPI for MPLS in an NNMi Environment

To deploy the iSPI for MPLS on a management server where NNMi is already installed and running, follow these steps:

Make sure to use the same database type (Postgres Embedded or Oracle) as NNMi when you are installing the iSPI for MPLS.

1 Install the iSPI for MPLS on a management server where NNMi is already installed, running, and nodes are discovered.

2 Start the MPLS processes. If you have the list of Route Targets (RTs) to be excluded in the network, you can add the RTs to be excluded from the `MPLS Configuration` workspace. Similarly, you can group the

Pseudowires based on the attributes such as Id or encapsulation type to discover VPWS VPNs. These configurations help in discovering the L3VPNs and L2VPNs.

3 You can start the iSPI for MPLS discovery process to discover the MPLS objects from the discovered NNMi nodes in any *one* of the following ways:

- Run the following command to discover the MPLS objects from the discovered NNMi nodes:

  ```
  $InstallDir/bin/nmsmplsdisco.ovpl -u <user> -p
  <password>[ -all | -node <node_name>]
  ```

- Select NNMi nodes from NNMi inventory and start the configuration poll. For more information, see *Help for NNMi, Launch the Actions: Configuration Poll Command*.
- Wait for the next NNMi discovery cycle.

4 After installing the iSPI for MPLS, log on to the NNMi console, and then verify the availability of the MPLS workspace and MPLS views.

Deploy the iSPI for MPLS with the iSPI Performance for Metrics/NPS

You must install NNMi 9.00, iSPI of MPLS, NNM iSPI Performance for Metrics/ Network Performance Server (NPS) to view the MPLS reports. You can deploy these products for the following scenarios:

- Installing NNMi, iSPI for MPLS, and the iSPI Performance for Metrics/ NPS on the same server.
- Installing the iSPI for MPLS and NNMi on one server and the iSPI Performance for Metrics/NPS on a dedicated server.

To deploy all the products on the same management server, follow these steps:

1 Install NNMi, 9.00.

2 Install the iSPI Performance for Metrics/NPS. 9.00. For information about the steps to install, see *HP NNMi iSPI Performance for Metrics/NPS Installation Guide.*

3 Install the iSPI for MPLS, 9.00.

Always install the iSPI Performance for Metrics/NPS and then install the iSPI for MPLS. If you have installed NNMi and iSPI for MPLS before installing NPS and iSPI Performance for Metrics, remove the `<Extension Pack>.processed` copy from the following location:

- On UNIX

  <$NNMDatadir>/ `shared/ perfSpi/ datafiles/ extension/ final` folder.

- On Windows
  <%NNMDatadir%>`\shared\perfSpi\datafiles\extension\final` folder.

Replace the <extension pack> in the `<Extension Pack>.processed` copy with the following:

- MPLS_LSR_Node
- MPLS_LSR_Interface
- L3_VPN_VRF

After removing the file, the extension packs are installed automatically.

To deploy NNMi and iSPI for MPLS on the same management server and the iSPI Performance for Metrics/NPS on a dedicated server, follow these steps:

1 Install NNMi, 9.0 and iSPI for MPLS, 9.0 on the same management server.

2 Install the iSPI Performance for Metrics/ NPS on the dedicated server. For information about the steps to install, see *HP NNMi iSPI Performance for Metrics/NPS Installation Guide*.

3 Complete the necessary configurations for NNMi, iSPI for MPLS, and iSPI Performance for Metrics/NPS.

Always install the iSPI Performance for Metrics/NPS and then install the iSPI for MPLS. If you have installed NNMi and iSPI for MPLS before installing NPS and iSPI Performance for Metrics, remove the `<Extension Pack>.processed` copy from the following location:

- On UNIX - *<$NNMDatadir>*`/ shared/ perfSpi/ datafiles/ extension/ final` folder.
- On Windows -*<%NNMDatadir%>*`\shared\perfSpi\datafiles\extension\final` folder.

Replace the <extension pack> in the *`<Extension Pack>`*`.processed` copy with the following:

- MPLS_LSR_Node
- MPLS_LSR_Interface
- L3_VPN_VRF

After removing the file, the extension packs are installed automatically.

After you complete the installations, the iSPI for MPLS introduces the following extension packs on the NPS/ Metrics console:

Extension Pack Name	**Purpose**
MPLS LSR Node	Shows report based on the available metric definitions for an MPLS-enabled node or nodes on the network.
MPLS LSR Interface	Shows report based on the available metric definitions for an MPLS-enabled interface or interfaces on the network.
L3_VPN_VRF	Shows report based on the available metric definitions for a VRF or an L3VPN on the network.

The extension packs use data collected by the iSPI for MPLS. Make sure that iSPI Performance for Metrics/NPS is up and running. To view the MPLS reports from the NNMi console, click **Actions->Report-Reporting Menu.** The iSPI Performance for Metrics console appears with the MPLS metrics and you can generate the MPLS reports.

After you uninstall the iSPI for MPLS, the extension packs introduced by the iSPI for MPLS are not removed. If the iSPI Performance for Metrics is running, the extension packs introduced by the iSPI for MPLS, still appear. You must remove the extension packs manually before you start installing the iSPI for MPLS again. For more information, see *Troubleshooting the iSPI for MPLS* section from the *iSPI for MPLS Installation Guide*.

Deploy the iSPI for MPLS in a High Availability Cluster Environment

You can install NNMi and iSPI for MPLS in a High Availability (HA) environment to achieve redundancy in your monitoring setup. The prerequisites to configure the iSPI for MPLS in an HA environment are similar to NNMi. For information, see *NNMi Deployment Reference Guide.*

You can deploy the iSPI for MPLS for the following scenarios:

- Configuring NNMi and iSPI for MPLS together in an HA environment.
- Configuring the iSPI for MPLS in an NNMi environment.

Configuring NNMi and iSPI for MPLS Together in an HA Cluster Environment

You can configure NNMi and iSPI for MPLS on the primary and secondary node in an HA environment. Make sure that the primary and secondary servers have different Fully Qualified Domain Names (FQDN) during the installation. See the *NNMi Installation Guide.* For more information about how to install NNMi on an HA environment, see *NNMi Deployment Reference*.

Configure the iSPI for MPLS on the Primary Node

To configure the iSPI for MPLS on the primary node, follow these steps:

1. Install NNMi and then iSPI for MPLS. After you install the iSPI for MPLS, install the iSPI for MPLS non production licenses. For more information, see **https://webware.hp.com/welcome.asp.**
2. Configure NNMi in an HA cluster environment on the primary node. For information, see *NNMi Deployment Reference*.
3. Run the following command from the `$NNM_BIN` directory to find the virtual hostname:

   <*NnmInstallDir*>**/bin/ nnmofficialfqdn.ovpl**
4. Modify the following files from the *$NnmdataDir*/`shared/mpls/conf/`or *%NnmdataDir%*`\shared\mpls\conf` to show the Virtual FQDN instead of hostname:

File Name	Value
`mpls.jvm.properties`	*<hostname>*`.selfsigned`
`nms-mpls.address.properties`	`jboss.nnm.host`
`nms-mpls.jvm.properties`	`Djava.rmi.server.`*<hostname>*
`nnm.extended.properties`	`com.hp.ov.nms.spi.mpls.nnm.`*<hostname>*
`nnm.extended.properties`	`com.hp.ov.nms.spi.mpls.spi.`*<hostname>*

5. Start the NNMi HA resource group by the following command:
   - For Windows:

     %NnmInstallDir%`\misc\nnm\ha\nnmhastartrg.ovpl NNM\ <resource_group>`
   - For UNIX:

     $NnmInstallDir`/misc/nnm/ha/nnmhastartrg.ovpl NNM\ <resource_group>`

   For more information, see *NNMi Deployment Reference Guide*.

The iSPI for MPLS and NNMi must start after this step. If NNMi or the iSPI for MPLS do not start, see *Troubleshooting the HA Configuration from NNMi Deployment Reference*.

6 Configure the iSPI for MPLS by the following commands:

- For Windows:

%NnmInstallDir%`\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon MPLS`

- For UNIX:

$NnmInstallDir/`misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon MPLS`

Configure the iSPI for MPLS on the Secondary Node

To configure the iSPI for MPLS on the secondary node, follow these steps:

1 Configure NNMi on the secondary node. For information, see *Configuring NNMi on the Secondary Cluster Node*. After you install the iSPI for MPLS, install the iSPI for MPLS non production licenses. For more information, see **https://webware.hp.com/welcome.asp.**

2 Modify the following files from the *$NnmdataDir*`/shared/mpls/conf/` or *%NnmdataDir%*`\shared\mpls\conf` to show the Virtual FQDN instead of hostname:

File Name	Value
`mpls.jvm.properties`	`<hostname>.selfsigned`
`nms-mpls.address.properties`	`jboss.nnm.host`
`nms-mpls.jvm.properties`	`Djava.rmi.server.<hostname>`
`nnm.extended.properties`	`com.hp.ov.nms.spi.mpls.nnm.<hostname>`
`nnm.extended.properties`	`com.hp.ov.nms.spi.mpls.spi.<hostname>`

3 Configure the iSPI for MPLS on the secondary node by the following commands:

- For Windows:

%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon MPLS

- For UNIX:

$NnmInstallDir/ misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon MPLS

Configuring the iSPI for MPLS in an NNMi HA Cluster Environment

You can configure the iSPI for MPLS on the primary node and secondary node in an NNMi HA cluster environment. For more information about how to install NNMi in an HA environment, see *NNMi Deployment Reference Guide*.

Configure the iSPI for MPLS on the Primary Node

Before you start configuring the iSPI for MPLS, make sure that NNMi is running on the primary node in an HA cluster environment. In addition, update the NNMi in the maintenance mode to prevent failover. Follow the steps documented in the *NNMi Deployment Reference* to put NNMi into the maintenance mode. Make sure that NNMi (ovjboss) is running by the following command: **`ovstatus -c`**.

To configure the iSPI for MPLS on the primary node, follow these steps:

1. Install the iSPI for MPLS.
2. Remove NNMi from maintenance mode. For information, see *Removing an HA Resource Group from Maintenance Mode* from the *NNMi Deployment Reference*.
3. Start configuring the iSPI for MPLS by the following commands:

   - For Windows:

   %NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon MPLS

   - For UNIX:

   *$NnmInstallDir/*misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon MPLS

4. Stop NNMi and iSPI for MPLS to start the failover by the following command:

ovstop -c

Configure the iSPI for MPLS on the Secondary Node

Before you start configuring the iSPI for MPLS, make sure that NNMi is running on the secondary node in an HA cluster environment. Stop NNMi and iSPI for MPLS by using **ovstop -c** to initiate the failover. In addition, change NNMi into the maintenance mode to prevent failover. Follow the steps documented in the *NNMi Deployment Reference* to put NNMi into the maintenance mode. Make sure that NNMi (ovjboss) is running by the following command: **ovstatus -c**.

To configure the iSPI for MPLS on the secondary node, follow these steps:

1. Start installing the iSPI for MPLS. While installing the iSPI for MPLS, the following errors appear:
   - Create Database User
   - Create Database

   Ignore the error messages and click **OK**. The database is created on the primary node while installing the iSPI for MPLS and exists on the shared disk.
2. Remove NNMi from maintenance mode. For information, see *Removing an HA Resource Group from Maintenance Mode* from the *NNMi Deployment Reference*.
3. Start configuring the iSPI for MPLS by the following commands:
   - For Windows:

   %NnmInstallDir%`\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon MPLS`
   - For UNIX:

   $NnmInstallDir/`misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon MPLS`
4. Stop NNMi and iSPI for MPLS to start the failover back to the primary node by the following command:

   ovstop -c

Remove the iSPI for MPLS from an HA Cluster Environment

To remove the iSPI for MPLS from an HA cluster environment, first remove the iSPI for MPLS from the secondary node and then from the primary node.

To remove the iSPI for MPLS from an HA cluster environment, follow these steps:

1. Remove the iSPI for MPLS from an HA cluster environment by the following command:

   - Windows:

   %NnmInstallDir%`\misc\nnm\ha\nnmhaunconfigure.ovpl NNM -addon MPLS`

   - UNIX:

   $NnmInstallDir/`misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon MPLS`

2. Remove NNMi from an HA cluster environment. For information, see *NNMi Deployment Reference Guide*.

Deploy the iSPI for MPLS in an Application Failover Environment

You can configure the iSPI for MPLS in an application failover environment from the following scenarios:

Deploy the iSPI for MPLS in an Application Failover Environment with Oracle Database

Scenario 1: In this scenario, consider that you want to install the iSPI for MPLS with NNMi and then configure application failover on NNMi:

1. Install NNMi in the primary server mode server 1 and install NNMi in the secondary server mode on server 2.
2. Start NNMi on server 1.
3. Install the iSPI for MPLS on server 1 with Oracle database by following the steps listed in the *HP Network Node Manager i Software Smart Plug-in for MPLS Installation Guide*.
4. Merge the keystores on one server and copy the keystores to both the primary and the secondary servers. For information, see the *NNMi Deployment Reference Guide* for instructions.
5. Install the iSPI for MPLS non production license on server 1.
6. Stop NNMi on server 1.
7. Start NNMi on server 2.
8. Install the iSPI for MPLS on server 2.
9. Configure iSPI for MPLS on server 2 with the same database instance, user name, and password configured on server 1.
10. After the installation of the iSPI for MPLS, install the iSPI for MPLS non production license on server 2.
11. Configure application failover server 1 and server 2 according to the instructions provided in the *NNMi Deployment Reference Guide*.

Scenario 2: In this scenario, consider that you want to install the iSPI for MPLS after configuring NNMi in an application failover environment:

1. Remove configuration for application failover from the NNMi primary and secondary servers.
2. Restore the old keystore and truststore specific to the primary server and the secondary server.
3. Remove the iSPI for application failover by using the following steps:

a. Disable application failover for the iSPI for MPLS following the steps discussed in the *Disabling NNMi for Application Failover* section in the *NNMi Deployment Reference Guide*.

b. Restore the keystore and the truststore for the systems that you backed up before configuring them for application failover.

4. Install the iSPI for MPLS on both primary and secondary servers following the steps discussed in Scenario 1.
5. Install the non production licenses available for the iSPI for MPLS installed on a server 1 and a server 2.
6. Configure the iSPI for MPLS for an application failover.

Deploy the iSPI for MPLS in an Application Failover Environment with Embedded Database

Scenario 1: In this scenario, consider that you want to install the iSPI for MPLS and NNMi in an application failover mode:

1. Install the iSPI for MPLS and NNMi on the primary server and the secondary server.
2. After the installation of the iSPI for MPLS, install the iSPI for MPLS non production licenses on both the servers.
3. Follow instructions documented in the *NNMi Deployment Reference Guide* to configure NNMi in application failover mode. After this, the iSPI for MPLS automatically gets configured in the application failover mode.

Scenario 2: In this scenario, consider that you want to install the iSPI for MPLS after configuring NNMi in the application failover mode:

1. Remove the NNMi application failover configuration from the primary and secondary nodes.
2. Restore the old keystore and truststore specific to the primary server and the secondary server configured. See the *NNMi Deployment Reference Guide* for instructions.
3. Install the iSPI for MPLS on both the primary and the secondary servers.
4. Install the iSPI for MPLS non production license on both the servers.
5. Configure the iSPI for MPLS in the application failover mode.

6 Configure NNMi in the application failover mode. Follow instructions from the *NNMi Deployment Reference Guide* to configure NNMi in an application failover mode.

Deploy the iSPI for MPLS with the iSPI for IP Multicast

The iSPI for MPLS helps you to monitor the Provider Edge (PE) routers discovered in a Multicast VPN (MVPN) topology. The PE routers are configured with the multicast-enabled VRF (MVRF) capabilities and use the multicast services to transmit data.

The iSPI for IP Multicast helps you to monitor the multicast services in the network. If the multicast services are used over an MPLS cloud, the integration of the iSPI for MPLS and IP Multicast provides the collaborative monitoring of an MVPN topology.

Navigate from the iSPI for MPLS to the iSPI for IP Multicast to view the multicast tree used by multicast traffic in the core network (cloud between the PE routers). The multicast tree shows the default and data Multicast Distribution Tree (MDTs). For more information, *see iSPI for MPLS Online Help, Overview of the Multicast VPN (MVPN) and MPLS view.*

For more information about launching the MPLS views, see IP Multicast View from the *MPLS Online Help*.

To deploy the iSPI for MPLS with the iSPI for MPLS, follow the steps:

1 Install NNMi 9.00.

2 Install the iSPI for MPLS, 9.00.

3 Install the iSPI for IP Multicast, 9.00.

There is no order to deploy the iSPIs (iSPI for MPLS or iSPI for IP Multicast) on a management server.

Deploy the iSPI for MPLS with the iSPI Performance for Quality Assurance

The iSPI for MPLS helps you to monitor the VRFs available on the network. The iSPI Performance for Quality Assurance measures the network traffic performance by configuring various tests on the VRFs. After installing the iSPI Performance for Quality Assurance, the iSPI for MPLS uses the QA performance capabilities. You can view the tests configured for the selected VRF by using the VRF form.

The integration of the iSPI for MPLS and NNM iSPI Performance for QA enables you to do the following:

- View the tests configured on VRFs. Troubleshoot the connectivity for the selected VRFs on basis of the configured tests. For example, finding the quality of connectivity for the multiple sites.
- Troubleshoot the PE-PE connectivity.
- Generate the reports based on the QA metrics. For example, find out the delay for data packet to reach the destination or the packet loss.

For more information, see *Help for iSPI Performance for QA*.

You must deploy NNM iSPI Performance for QA and iSPI for MPLS on the same NNMi management server.

Deploying the iSPI for MPLS with Route Analytics Management System

HP Route Analytics Management System (RAMS) integrates with NNMi to provide the routing protocol path for the layer 3 topology. You can use the RAMS features and functionality to monitor the L3 VPNs that uses the mBGP protocol. In addition, you can use the RAMS capabilities to draw the MPLS path within the PE - PE cloud that helps you to monitor the network over the MPLS cloud. After the integration with RAMS, you can monitor and view the SNMP traps from the RAMS appliance in the RAMS tab. The RAMS tab appears in the L3 VPN form. For more information, see *MPLS Online Help and MPLS Reference Pages*.

Deploy the iSPI for MPLS in Global Network Management Environment

You can deploy the iSPI for MPLS in a Global Network Management (GNM) environment. The iSPI for MPLS uses the capabilities of NNMi Global Network Manager (NNMi GNM) and provides a centralized view to monitor the multiple sites. The iSPI for MPLS allows you to configure the Regional Manager connections by using the **MPLS Configuration** workspace. After the connection is established, view and monitor the MPLS nodes from the iSPI for MPLS inventory (GNM). For more information about how to configure the iSPI for MPLS regional managers, see the *iSPI for MPLS Online Help*.

You can deploy NNMi and iSPI for MPLS in a GNM environment for the following scenarios:

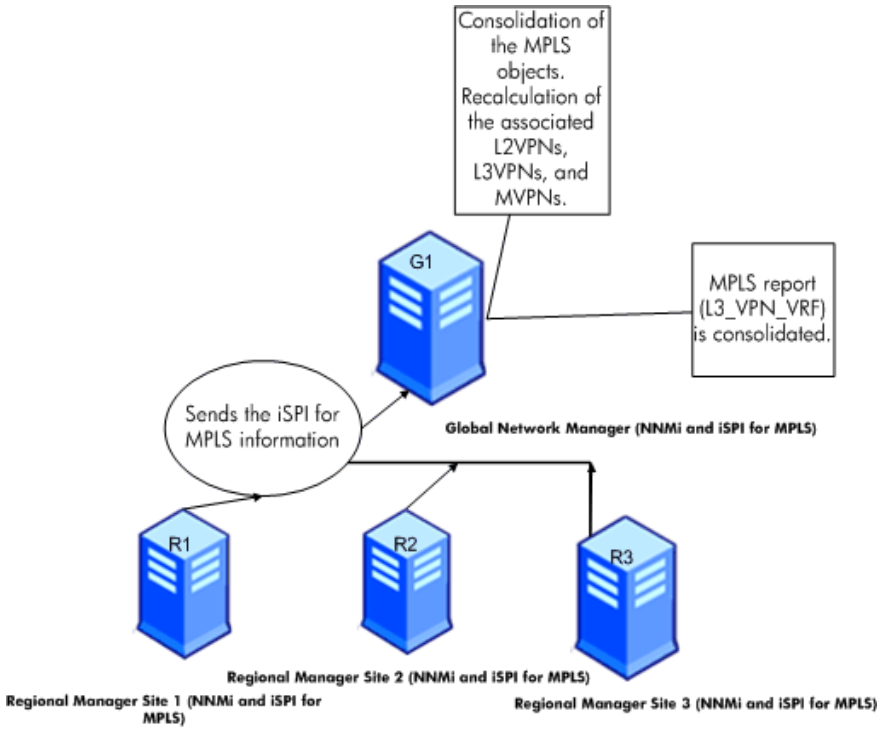
- Both NNMi and iSPI for MPLS are configured on the Global Network Manager server and Regional Manager management servers.
- NNMi is configured on the Global Network Manager server and NNMi and iSPI for MPLS are configured on the Regional Manager management servers.
- Both NNMi and iSPI for MPLS are configured on the Global Network Manager server and NNMi is configured on the Regional Manager management server.

Deploying NNMi and iSPI for MPLS on the Global Network Manager and Regional Manager Management Server

You can install and configure NNMi and the iSPI for MPLS on the Global Network Manager and Regional Managers. For information about the configuration steps, see *NNMi and iSPI for MPLS Online Help*.

The following figure represents a deployment scenario, where NNMi and iSPI for MPLS are configured on the Global Network Manager (G1) and Regional Managers (R1, R2, and R3):

In this deployment scenario, all the Regional Managers (R1, R2, and R3) send the MPLS information to the Global Network Manager (G1). You can view the following information from G1:

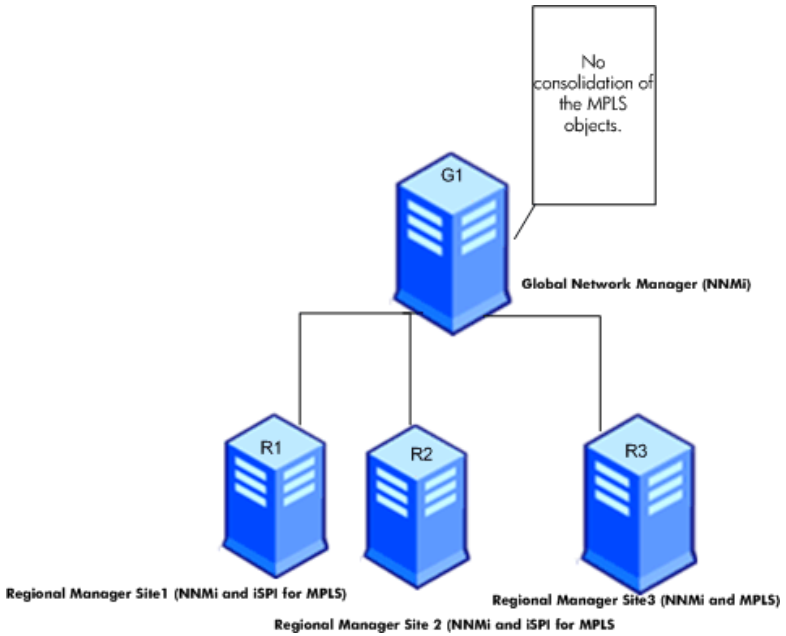


- Consolidated MPLS topology is available. The regional managers send the information about the MPLS objects such as VRFs, TE Tunnels, VC LSPs, and MVRFs to the Global Network Manager (G1). The GNM uses the MPLS object related information from the regional managers to regroup and form the L3 VPNs, L2VPNs, MVPNs, and PseudoWire VCs in the network. In the G1 inventory, the status is recalculated for the MPLS objects. In addition, the incidents are also generated for the MPLS topology in the GNM (G1). The incidents are not forwarded from the regional managers to GNM (G1) as the MPLS topology is derived again in the G1. The incidents are only generated for the MPLS objects available in the G1 inventory.
- Consolidated L3_VPN_VRF report is available. Other MPLS reports are available only for the local MPLS nodes in the G1.

Deploying NNMi on the Global Network Manager and NNMi and iSPI for MPLS on the Regional Manager Management Server

You can install and configure NNMi on the Global Network Manager and both NNMi and iSPI for MPLS on the Regional Managers. For information about the configuration steps, see the *NNMi and iSPI for MPLS Online Help.*

The following figure represents a deployment scenario, where NNMi is configured on the Global Network Manager (G1). NNMi and the iSPI for MPLS are configured on the Regional Managers (R1, R2, and R3):

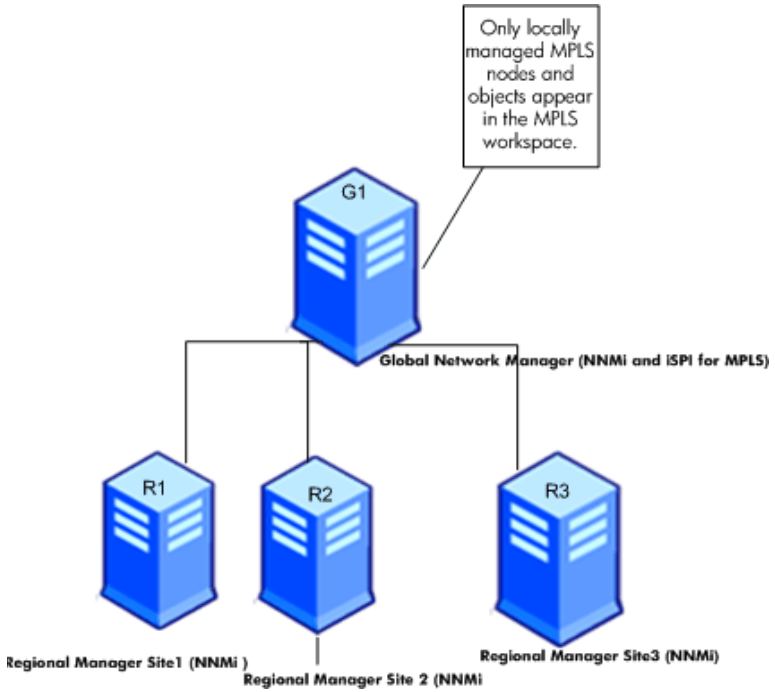


In this deployment scenario, all the Regional Managers (R1, R2, and R3) discover the MPLS nodes and objects such as VRFs, TE Tunnels, VC LSPs, and MVRFs. The iSPI for MPLS is not available on G1 so there is no communication established between G1 and regional managers for the iSPI for MPLS. Thus, the MPLS nodes and objects from the Regional Managers are not available in the G1 inventory. In addition, no aggregated MPLS reports are available in the MPLS (GNM) inventory.

Deploying NNMi on the Global Network Manager and NNMi and iSPI for MPLS on the Regional Manager Management Server

You can install and configure NNMi and the iSPI for MPLS on the Global Network Manager and only NNMi on the Regional Managers. For information about the configuration steps, see in the *NNMi and iSPI for MPLS Online Help*.

The following figure represents a deployment scenario, where NNMi and iSPI for MPLS is configured on the Global Network Manager (G1) and NNMi on the Regional Managers (R1, R2, and R3):



In this deployment scenario, only the locally managed MPLS nodes and objects such as L3 VPNs, L2VPNs, MVPNs, and PseudoWire VCs are available in the MPLS inventory (G1).

Deploying the Regional Manager in the Application Failover Environment

When the iSPI for MPLS Regional Manager is in the Application failover environment, use the **ORDER** parameter to decide the priority to establish the connection.

To use the regional manager in an application failover environment, follow these steps:

1. Configure the Regional Manager connection using MPLS configuration workspace.
2. Add the two regional manager connections and provide the two hostnames.
3. Use the **ORDER** parameter to give different values to the two regional managers.

Whenever there is an application fail-over available on the regional manager, the GNM will always use the lowest order value to establish the next connection.

You can configure the regional manager in the application failover environment by using the steps documented in the Deploy the iSPI for MPLS in an Application Failover Environment with Oracle Database on page 24 and Deploy the iSPI for MPLS in an Application Failover Environment with Embedded Database on page 25.

3 Upgrading to the iSPI for MPLS, 9.00

Before you start upgrading the MPLS VPN SPI from 7.5x to newer version, make sure that you upgrade NNMi 7.5x version to 9.x version. For upgrading NNMi from the earlier versions, see the *NNMi Deployment Reference Guide*.

License for Upgrading from the Earlier Versions

If you are upgrading from the earlier versions of the MPLS SPI, then you can obtain the iSPI for MPLS, 9.00 upgrade licenses. You can contact HP sales to know about your upgrade license entitlement based on your order number for the earlier versions of the MPLS VPN SPI.

License for Upgrading from the MPLS, Version 7.53 to Version 9.00

To upgrade to the iSPI for MPLS, the Contract Migration is required. The Special Migration SKUs are available from **http://support.openview.hp.com/software_updates.jsp.** The iSPI for MPLS, 9.0 is password protected product so you have to acquire your technical password migration. You can obtain your password from the following URL **http://support.openview.hp.com/software_updates.jsp.**

License for Upgrading from the iSPI for MPLS, Version 8.10 to Version 9.00

To upgrade to the iSPI for MPLS, the Contract Migration is *not* required as both the versions use the same LTU's SKU. You only need the media product number. The iSPI for MPLS, 9.0 is password protected product so you have to

acquire your technical password migration. You can obtain your password from the following URL **http://support.openview.hp.com/software_updates.jsp.**

Upgrading from Version 7.53 to Version 9.00

The MPLS VPN SPI, 7.53 is supported on UNIX 32 bit platform in contrast to the iSPI for MPLS which is supported on 64 bit Windows and UNIX platforms. For more information on supported database, hardware and software requirements, see the *iSPI for MPLS, Support Matrix, 9.00*.

There are no direct steps available for upgrading the MPLS VPN SPI, 7.53 to the iSPI for MPLS, 9.00.

After you migrate the community string configuration from NNM 7.53 installation to NNMi 8.10, make sure that community strings for MPLS nodes are also present in the NNMi communication configuration.

While migrating from MPLS VPN SPI, 7.53 to the iSPI for MPLS, 8.x version, you can use the data specified in following configuration files:

- Migrate the data specified in the `MplsVpn.cfg` file of MPLS VPN SPI, 7.53.

  Install the iSPI for MPLS, 9.00. Make a note of the Route Targets (RTs) specified in `Ignore RT` section of MPLS VPN SPI, 7.53. Add these RTs in `Exclude RT` section of the `MPLS Configuration` workspace of the iSPI for MPLS, 9.00

  Start the VPN computation only after you add and save all the RTs to be excluded from the `MPLS Configuration` workspace

  You can add the RTs in the following ways:

  — Add one RT value to be excluded and then, click **Save**. This automatically starts the L3 VPN computation.

  — Add all the RT values to be excluded sequentially and then, click **Save**. This automatically starts the L3 VPN computation. This is a preferred option as you have to perform this task only once for the proper computation and grouping of all the VRFs that are already discovered in the network.

- Migrate the data specified in the `MgmtVpn.cfg` file of MPLS VPN SPI, 7.53 to the iSPI for MPLS, 9.00

  The iSPI for MPLS, 9.00 does not support Management VPNs feature.

  To migrate the data specified in the `MgmtVpn.cfg` file, follow the steps:

  a. From the `MgmtVpn.cfg` file, select the RT values with `Active` settings across the `RT-PATTERN`.

  b. Add the selected RT values in the `MPLS Configuration` workspace.

     This automatically starts the L3 VPN computation after you add all the RTs and helps to get the consolidated group of the L3VPNs.

- Use the data specified in the `VpnNames.txt` file of MPLS VPN SPI, 7.53 to the iSPI for MPLS, 9.00.

  The MPLS VPN SPI, 7.53 stores the VRF grouping relationships and VPN names in the `VpnNames.txt` file. You can rename the VPNs in the iSPI for MPLS, 9.00 according to the list in the `VpnNames.txt` file from MPLS views. For more information, see *Help for MPLS, 9.00*.

Upgrading from Version 8.10 to Version 9.00

To upgrade the iSPI for MPLS from version 8.10 to version 9.00, follow these steps:

1. Uninstall the 8.10 version of the iSPI for MPLS.
2. Install NNMi 9.00.
3. Install the iSPI for MPLS, 9.00.

Product Comparison

You can compare the features of the iSPI for MPLS, 9.00 with the earlier versions of the MPLS VPN SPI. This section helps you to understand the product when you are upgrading from the earlier versions.

Comparing the MPLS L3 VPN Features

MPLS L3 VPN Features	Version 7.x	Version 8.x	Version 9.x
Layer 3 VPN MPLS/BGP (RFC 2547 bis) discovery and management.	*Yes*	*Yes*	*Yes*
All the Provider Edge (PE) routers available in the MPLS inventory.	*Yes*	*Yes*	*Yes*
Discovery and management of VRF's from all PE's discovered.	*Yes*	*Yes*	*Yes*
Automatic grouping of the VRFs to form a single VPN.	*Yes*	*Yes*	*Yes*
Tabular view of PEs and related VRFs.	*Yes*	*Yes*	*Yes*
Customization of the system-generated L3VPN names	*Yes*	*Yes*	*Yes*
Customization of RT inclusion and RT exclusion to form an L3 VPN.	*Yes*	*Yes*	*Yes*
Fault management of VRFs through incidents and traps.	*Yes*	*Yes*	*Yes*
CE nodes inventory in the network.	*Yes*	No	No

MPLS L3 VPN Features	Version 7.x	Version 8.x	Version 9.x
CE Management: Tabs and incidents.	*Yes*	No	*Yes*
HSRP/VRRP support on the PE/CE interfaces.	*Yes*	No	No
Duplicate IP Address support between the PE-CE link connectivity	*Yes*	No	*Yes*
Graphical views of the service-oriented L3VPNs.	No	No	*Yes*
Graphical views of PE-CE relationship in an L3VPN.	*Yes*	No	*Yes*
Cisco Support	*Yes*	*Yes*	*Yes*
Cisco IOS-XR Support	No	*Yes*	*Yes*
Juniper J/M/T series routers	*Yes*	No	*Yes*
Juniper E series supported	*Yes*	No	No
Reachability tests between the PE routers through IP SLA between the PE router and corresponding CE router.	*Yes*	No	*Yes*
Reachability tests through PingMib between the PE router and corresponding CE router.	*Yes*	No	*Yes*
VRF-Lite discovery	*Yes*	No	No

MPLS L3 VPN Features	Version 7.x	Version 8.x	Version 9.x
Shadow Router discovery	*Yes*	No	No
Discovery of Management VPNs	*Yes*	No	No
RMTool to support discovery of accurate L3VPNs with RTs configured in Route Maps.	*Yes*	No	No

Comparing the MPLS TE Tunnel Features

MPLS TE Tunnel Features	Version 7.x	Version 8.x	Version 9.x
Discovery & Management of TE Tunnels	*Yes*	*Yes*	*Yes*
Monitoring the TE Tunnels (status / incidents)	*Yes*	*Yes*	*Yes*
Inventory of TE Tunnels	*Yes*	*Yes*	*Yes*
Discovery of TE Tunnel attributes	*Yes*	*Yes*	*Yes*
Map view of the TE Tunnel path.	*Yes*	No	*Yes*
Tabular view of TE Tunnel path.	*Yes*	No	*Yes*
Monitoring the TE Path and RCA.	*Yes*	No	No
Cisco support	*Yes*	*Yes*	*Yes*

MPLS TE Tunnel Features	Version 7.x	Version 8.x	Version 9.x
Cisco IOS-XR support	No	*Yes*	*Yes*
Juniper J/M/T series support	*Yes*	No	*Yes*
Juniper E-series support	No	No	No

Comparing the PseudoWire VC Features

MPLS PseudoWire VC Features	Version 7.x	Version 8.x	Version 9.x
Discovery and Management of point-to-point Pseudowires with encapsulation types (VPWS).	No	*Yes*	*Yes*
Discovery and Management of point-to-multipoint Pseudowires (VPLS).	No	*Yes*	*Yes*
Fault management of PWs through management incidents and traps.	No	*Yes*	*Yes*
Discovery and monitoring of the available VPWS VPNs.	No	No	*Yes*
Discovery and monitoring of the available VPLS VPNs.	No	No	*Yes*
Mapping point-to-point Pseudowires to customers.	No	No	*Yes*

Comparing the LSR Features

MPLS LSR Features	Version 7.x	Version 8.x	Version 9.x
Discovery of all MPLS-enabled routers	*Yes*	*Yes*	*Yes*
Cross launch to TE Tunnels and VRFs configured on a particular device	*Yes*	*Yes*	*Yes*
Quick identification of MPLS features supported by LSR	No	*Yes*	*Yes*

Comparing the RAMS Features

RAMS Integration Features	Version 7.x	Version 8.x	Version 9.x
Integration with the RAMS appliance to configure VPN names in the RAMS device based on RTs discovered	*Yes*	No	*Yes*
Path Monitoring by using RAMS and L3VPN impact analysis	*Yes*	No	No
Capability to launch LSP paths between the PE routers based on the information stored in the RAMS database	*Yes*	No	*Yes*
RAMS Trap resolution to MPLS-VPN objects	No	No	*Yes*

Comparing the iSPI Performance for Metrics Features

iSPI Performance for Metrics Features	Version 7.x	Version 8.x	Version 9.x
L3VPN and VRF availability reports for Layer 3 VPN	*Yes*	No	*Yes*
MTTR and MTBF reports for the VRFs participating to form an L3VPN	No	No	*Yes*
MPLS traffic metrics (packets, octets, and so on) for LSR node & interfaces	No	No	*Yes*

Comparing the MVPN Features

MVPN Features	Version 7.x	Version 8.x	Version 9.x
MVPN capability on an L3VPN	No	No	*Yes*
Identification of default MDTs	No	No	*Yes*
Identification of Data MDT (source and group)	No	No	*Yes*
MVPN flow indicated by upstream & downstream tabs	No	No	*Yes*
MVPN Tree maps indicating the flow of the multicast traffic	No	No	*Yes*

Index

L

P

R

U