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

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

Software Version: 9.00

Online Help

Document Release Date: March 2010

Software Release Date: March 2010

HP Network Node Manager i Software iSPI for MPLS

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.

For information about third-party license agreements, see the license-agreements directory on the product installation media.

Copyright Notices

Trademark Notices

Acrobat® is a trademark of Adobe Systems Incorporated.

DOM4J® is a registered trademark of MetaStuff, Ltd.

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.

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

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

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, see the license-agreements directory on the NNMi product DVD.

Table of Contents

Introduction

HP Network Node Manager (NNM) i Software Smart Plug-in for MPLS (Multi Protocol Label Switching) (**NNMi iSPI for MPLS**) provides real-time data that enables you to monitor the health of L3 Virtual Private Network (L3 VPN), Layer 2 VPNs (L2 VPNs), Multicast VPNs (MVPNs), PseudoWire VCs, and Traffic Engineering (TE) tunnels.

The iSPI for MPLS uses the properties of NNMi to gather information and monitor the MPLS-enabled nodes. The iSPI for MPLS provides you information of your converged network and the ability to perform fault analysis. The MPLS workspace helps you to monitor the traffic on the network.

The iSPI for MPLS supports the following device types:

- Cisco routers
- Cisco IOS-XR routers
- Juniper(M/T/J) series routers

The iSPI for MPLS, in conjunction with NNMi, performs the following tasks:

- Discovering and monitoring the (Layer 3 Virtual Private Network) L3 VPNs configured in the provider edge devices of the network.
- Discovering and monitoring the Virtual Private LAN Service VPNs (VPLS VPNs) in the network.
- Discovering and monitoring the Virtual Private Wire Service VPNs (VPWS VPNs) in the network.
- Discovering and monitoring the TE tunnels in the network.
- Discovering and monitoring the PseudoWire VCs in the network.
- Discovering and monitoring the Multicast VPNs (MVPNs) in the network.
- Monitoring the health of the MPLS objects in the network.
- Monitoring the PE-CE relationship in the network. Monitoring the Customer Edge nodes and finding the service-related impact analysis.
- Monitoring the MPLS Inventory from the Global Network Manager and Regional Manager.
- Troubleshooting the network by using the MPLS map views.
- Investigating the problems of the network by viewing the incidents and service impact incidents.
- Troubleshooting the network by viewing the MPLS reports. This is only possible after you integrate the iSPI for MPLS with iSPI Performance for Metrics.
- Monitoring and troubleshooting an L3VPN by using Route Analytics Management System (RAMS) capabilities.
- Monitoring and troubleshooting an MVPN by using the iSPI for IP Multicast capabilities.
- Monitoring the network by using the iSPI Performance for Quality Assurance (QA) capabilities.

After you install (and configure) the iSPI for MPLS on the NNMi management server, you can monitor and troubleshoot the problems in your network with the additional table and map views provided by the iSPI for MPLS.

For more information about L3 VPNs, VPLS VPNs, VPWS VPNs, PseudoWire VCs, and TE tunnels, see the following topics:

Overview of the MPLS L3 VPN

Overview of the MPLS L2 VPN

Overview of the MVPN

Overview of the MPLS TE Tunnel

Overview of the MPLS PseudoWire VC

For more information about how to use the help for the iSPI for MPLS, see Using the iSPI for MPLS.

Using the iSPI for MPLS

The iSPI for MPLS helps you to quickly monitor, detect, and troubleshoot abnormal behavior in the network.

To perform a basic monitoring of the MPLS services in the network, you can log on to the NNMi console with the operator (level 1 or 2) or guest credentials. After you log on to the NNMi console, you can view the inventory views introduced by the iSPI for MPLS. The iSPI for MPLS discovers the MPLS-enabled nodes participating in the network. You can access the MPLS views to monitor the status and necessary details for all the MPLS objects.

The following table describes some of the ways that *Help for iSPI for MPLS* assists you in accomplishing your tasks.

Task	Help Topics
Overview	Overview of the MPLS L3 VPN Overview of the VPN, VRFs, and Route Targets Overview of the MPLS TE Tunnel Overview of the MPLS PseudoWire VC Overview of the MPLS L2 VPN Overview of the MPLS CE Management Overview of the Multicast VPN (MVPN)
View the MPLS inventory	Monitoring Your MPLS Inventory
View the details of the devices	Monitoring Your Network with MPLS Forms
View the MPLS incidents	Viewing the MPLS Incidents
View the map views	Viewing the Network Connectivity
Monitor the network health	Monitoring Your Network Health
Monitor your network by using the iSPI for MPLS and RAMS	Integrating the iSPI for MPLS with Router Analytics Management System
Monitor your network by using the iSPI for MPLS and the iSPI for IP Multicast	Integrating the iSPI for MPLS with the iSPI for IP Multicast
Monitor your network by using the iSPI for MPLS and the iSPI Performance for Quality Assurance (QA)	Integrating the iSPI for MPLS with the iSPI Performance for QA

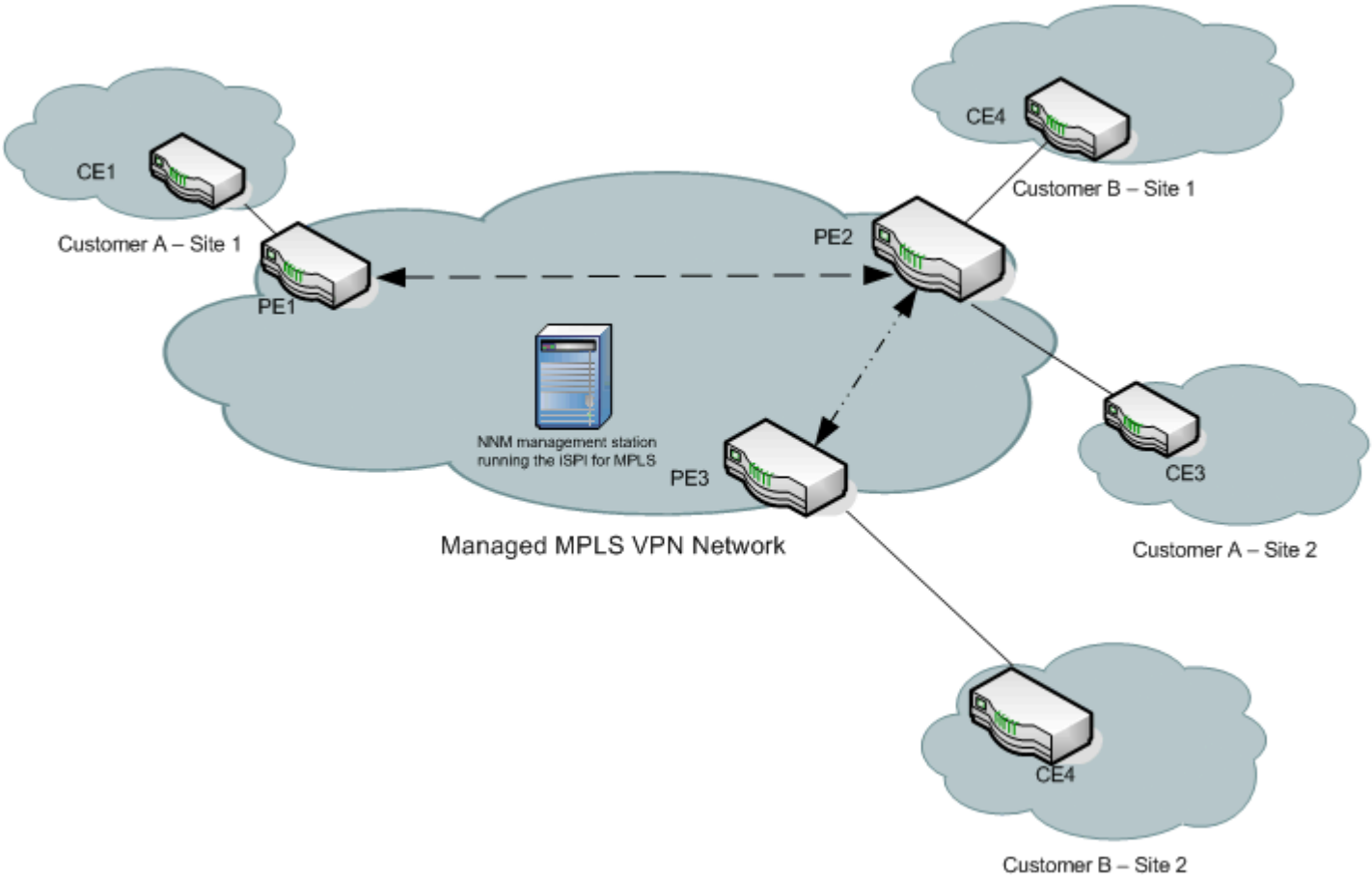
Overview of the MPLS L3 VPN

The iSPI for MPLS helps you to monitor an L3 VPN network topology.

In an MPLS-enabled network, the provider edge (PE) routers reside on the perimeter of the service provider's network. The PE routers communicate with two other kinds of routers-- routers inside the MPLS VPN cloud that belong to the service provider (P routers) and customer edge (CE) routers that are located and managed at customer sites.

Each L3 VPN contains the backbone routers (P routers), the provider edge (PE) routers, and the customer edge (CE) routers.

Example of an MPLS L3 VPN Network



The iSPI for MPLS helps you to perform the following tasks:

Monitor L3 VPNs and VRFs

You can discover the VRFs and Route Targets (RTs) participating to form an L3 VPN in the network. A VPN is formed by the set of Virtual Routing and Forwarding (VRFs) tables on an edge router (PE). You can monitor and view the real-time status of the complex L3 VPNs. You can navigate to L3 VPN forms to view the attributes and incidents-related to the network. In addition, you can navigate to the PE node form to troubleshoot the network connectivity. For more information, see Node Form: L3 VPN PE Interfaces Tab.

Manage Faults

You can detect the changes in the topology such as the status of the VRF changes from up to down by using the iSPI for MPLS views. The iSPI for MPLS provides a quick way to view the enriched incidents that help you quickly understand and react to a problem in your network. For more information, see MPLS Incidents.

For more information about the L3 VPN, VRFs, and Route Targets, see L3 VPN, VRF, and Route Targets.

L3 VPN, VRFs, Route Targets, and L2 VPN

You can view and monitor the health of the MPLS objects from the iSPI for MPLS forms.

L3 VPN, VRFs, and RTs

The provider edge (PE) routers communicate with each other using the label-switched paths if the service provider implements Multi-Protocol Label Switching (MPLS) in the network.

Each PE router maintains a virtual routing and forwarding table, or VRF. The purpose of the VRF is to transfer traffic towards the correct customer edge (CE) router. An L3 VPN is formed by a set of VRFs. A VRF participates only in a single VPN and is grouped on the basis of the Route Targets.

A Route Target (RT) identifies a group of routers having a set of VRFs that helps in routing traffic. Every VPN route is associated with more than one RT that is exported or imported from other VRFs.

VRFs Grouping for an L3 VPN

Each VRF includes a list of import and export route targets that identify other VRFs in the network. The iSPI for MPLS reads the route targets from the import and export lists to identify groups of VRF neighbors. A VRF exports its route targets to other VRFs in the L3 VPN. Similarly, another VRF imports route targets from other VRFs in the L3 VPN. The import/export relationship creates the logical VRF-VRF neighbor adjacency relationship. These relationships determine the routes through the network which should be tested to ensure adequate service for your customers.

The VRFs that can be linked directly or indirectly by their neighbor relationships are in the same VPN. This approach lets the iSPI for MPLS correctly discover simple network topologies that are fully meshed as well as complex network topologies such as hub and spoke VPN.

Ignore the Route Targets by using the **MPLS Configuration** workspace. This results in regrouping of VRFs to form an L3 VPN. The status of the L3 VPN is again recomputed.

L3 VPN Topology

The L3 VPN topology covers different types of VPNs in the network. The iSPI for MPLS shows the following types of L3 VPN topologies:

- **Full-Mesh** - Full Mesh VPN is formed if all the VRFs have the same RT. The same RT is used for importing and exporting all the VRFs in the specific group. Each VRF exports its route targets to all the other VRFs in the L3 VPN and imports all route targets from the other VRFs in the L3 VPN. All the PE routers are communicating with each other.
- **Other** - All the VRFs are not communicating with all the other VRFs participating to form an L3 VPN. For example, hybrid topology.
- **Isolated** - A VRF participating to form a single L3 VPN (no other VRF imports the route targets of this VRF).
- **Hub and Spoke -** A Hub and Spoke VPN is formed when all the VRFs communicate with each other by using the Hub-VRF. The hub and spoke VPN topology is a star-shaped topology where the Hub VRF is in the center VRF. All the spoke-VRFs connect to a Hub-VRF.

L3 VPN Naming

The iSPI for MPLS uses the internal system naming convention to provide the L3 VPN names. You can use the MPLS views to update the system-generated L3 VPN name.

The VRF grouping relationships results in the system-generated L3 VPN names. The iSPI for MPLS assigns a meaningful L3 VPN name to each discovered VRF group according to the specific rules.

To update the L3 VPN name:

(From the L3 VPN Form, update the system-populated name. Click the  **Save and Close** icon. The new name appears in the L3 VPN inventory.)

The rules used by the system-generated L3 VPN name:

- The common VRF name is used to name the L3 VPN. If the name is already used by one of the VPNs, the system-generated name is the common VRF name appended with Id.
- If there is no common VRF name, the iSPI for MPLS creates a new L3 VPN name by the following rules:

  - If at least 65 percent of the VRFs in the group have the same name and that name would be a unique L3 VPN name, assign that text string as the L3 VPN name for the VRF group.

  - If at least 65 percent of the VRFs in the group have the same name and that name is already a L3 VPN name for another VRF list, assign the L3 VPN name as the VRF name appended with an under-score followed by the VPN internal identification number for this VRF group.
- If at least the first three characters of each name in the VRF group matches, set the L3 VPN name to the initial matching characters.
- The name of the isolated L3 VPN is same as the isolated VRF name.

Examples

VRFs in the VPN	Selected L3 VPN Name	Explanation
VRF 1- Blue VRF 2- Blue	Blue	Same VRF name.
VRF 1- Blue VRF 2- Green VRF 3- Green VRF 4- Green	Green	Select the majority name.
Red_East Red_West	Red	The common initial characters.

VPWS VPN and VPLS VPN

The L2 VPN topology includes the VPLS VPNs and VPWS VPNs in the network.

The VPLS VPNs are associated within one L2 VPN if the VPN id is same for all the PseudoWire VCs participating to form a VPLS VPN.

The VPWS VPNs are associated within one VPN if the VC_id is same for all the PseudoWire VCs participating to form a VPWS VPN. To configure the VPWS VPNs, use the **MPLS Configuration** workspace.

L2 VPN Renaming

The iSPI for MPLS assigns a meaningful VPLS VPN name to each discovered VPLS by appending the VPLS name with unique VPN id. For example, VPLS_VPN ID.

To configure the VPWS, type the VPWS name from the MPLS Configuration workspace. In addition, if any PseudoWire VC is not participating to form a VPLS or a VPWS, appears as **Default Group.**

To update the VPLS VPN name:

(In the VPLS VPN Form, type the new name. Click the **Save and Close** button. The new name appears in the VPLS VPN inventory.)

To update the VPWS VPN name:

(From the VPWS VPN Form, type the new name. Click the **Save and Close** button. The new name appears in the VPWS VPN inventory.)

MVPN Naming

All the MVPNs are named by the internal system naming convention. You can change and rename the system-populated MVPN name. The L3 VPN names results in the MVPN names. The iSPI for MPLS assigns a meaningful MVPN name according to the specific rule.

To update the MVPN name:

(In the MVPN Form, type the new name. Click the **Save and Close** icon. The new name appears in the MVPN inventory.)

The rules used by the system-generated MVPN name:

- The MVPN name uses an L3 VPN name. For example, if the L3 VPN name is Red, MVPN name is Red. You can update the MVPN name from the MVPN form.
- If a single L3 VPN contains multiple MVPNs, assign the MVPN name as the L3 VPN name appended with an underscore followed by the internal identification number. For example, if the name of the L3VPN is Red, multiple MVPNs in the selected L3 VPN are Red_(X) and Red_(Y).
- The MVPN name uses the current name of the L3 VPN. For example, if the L3 VPN is renamed from Red to Blue, MVPN name is Blue. You can update the MVPN name from the MVPN form.
- The L3VPN name is renamed and changed after the MVPN is formed. The MVPN name is not updated. For example, if the L3 VPN name is Red, MVPN name is Red_xyz. Now the L3VPN name is renamed to Blue but the MVPN name still remains as Red_xyz.

Overview of the MPLS L2 VPN

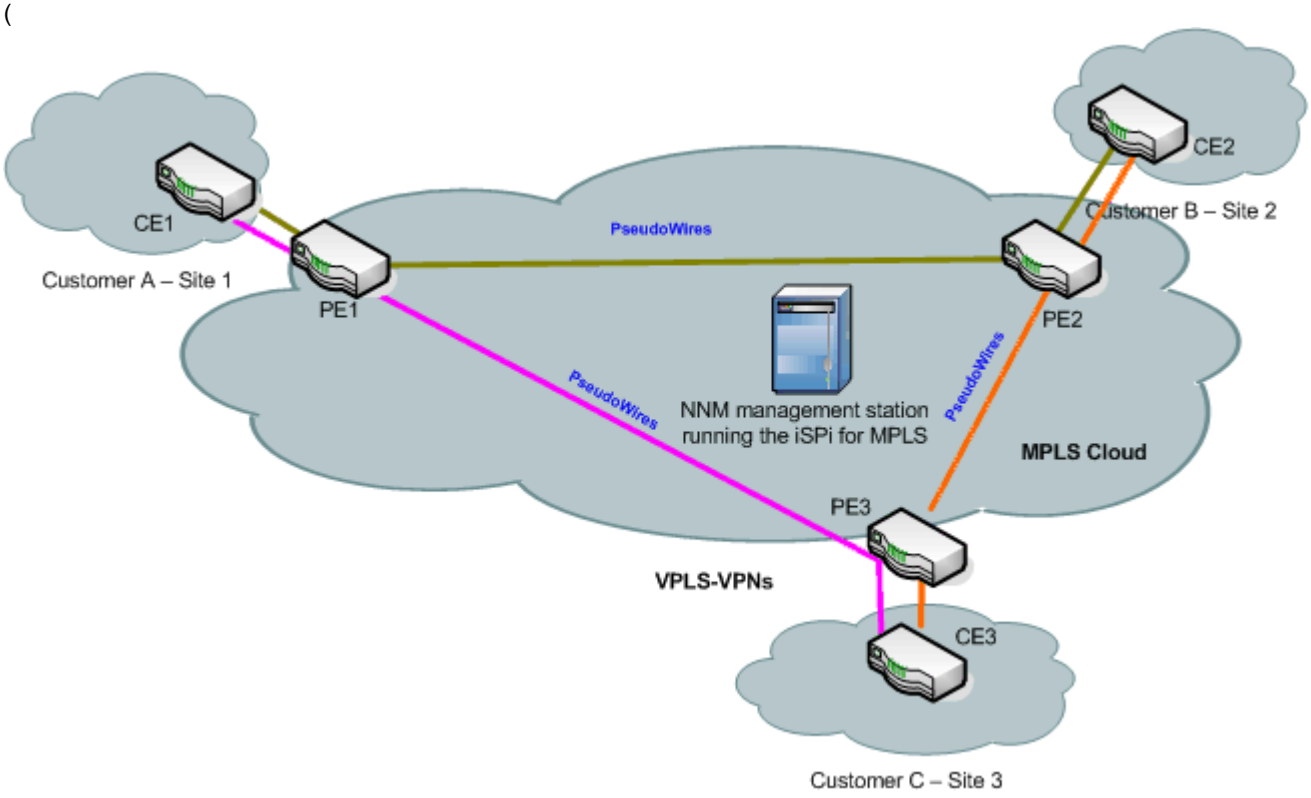
The iSPI for MPLS helps you to monitor the L2 VPNs (VPLS VPN and VPWS VPN) in your network topology.

Virtual Private LAN Service (VPLS VPN)

A VPLS VPN is formed by Layer 2 VPNs where multiple sites communicate using Ethernet-based multipoint to multipoint communication over a Packet Switched Network (PSN). The PE routers use Border Gateway Protocol (BGP) and Label Distribution Protocol (LDP) protocols to communicate within the VPLS VPNs.

Example of a VPLS VPN

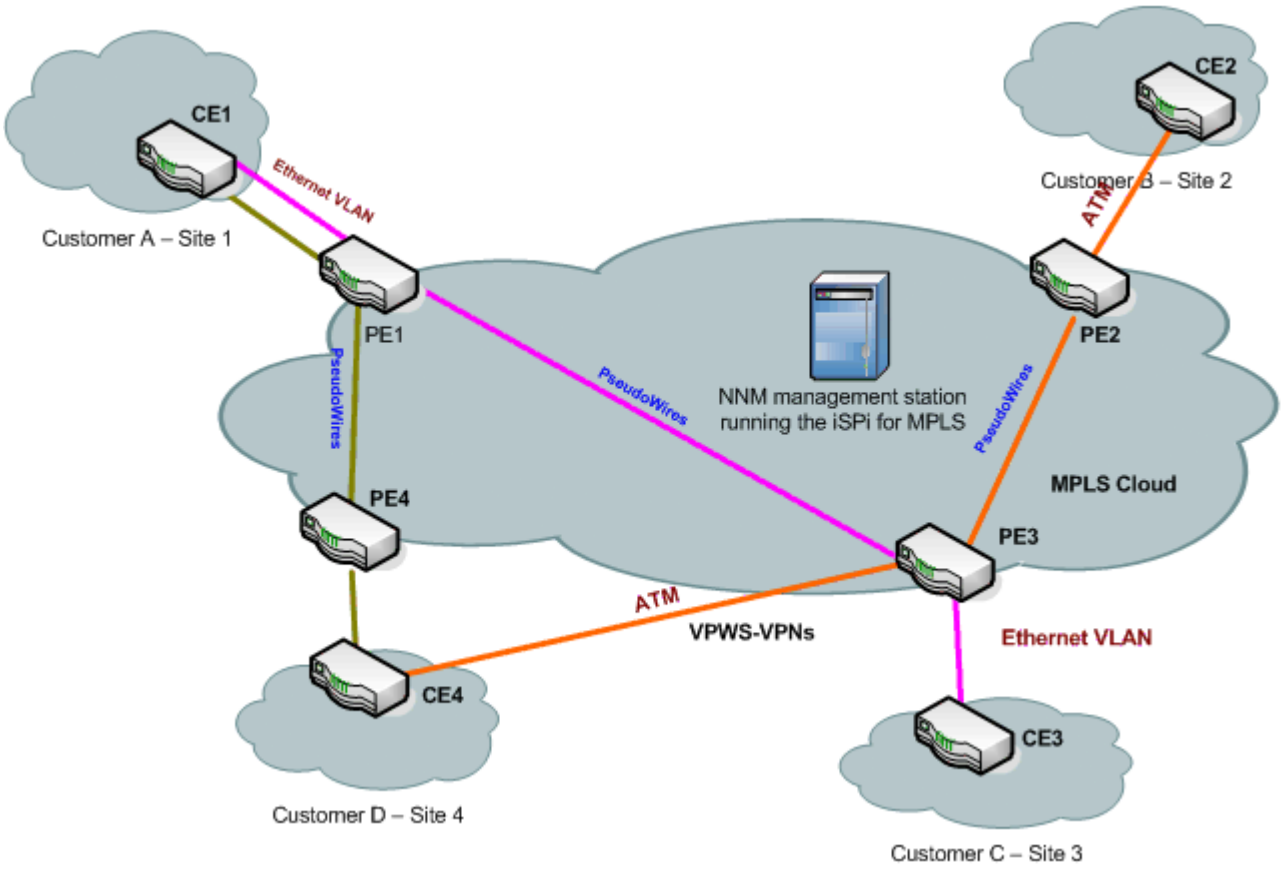
(



Virtual Private Wire Service VPN (VPWS VPN)

A VPWS VPN is formed by Layer 2 VPNs where point-to-point link connects the CE devices through a Packet Switched Network (PSN) using PseudoWires VCs. Configure the VPWS VPNs from the MPLS Configuration workspace.

Example of a VPWS VPN



The iSPI for MPLS helps you perform the following tasks:

Monitor PseudoWires VCs

You can discover the PseudoWires VCs participating to form an L2 VPN. You can monitor and view the real-time status of the L2VPNs. You can navigate to L2 VPN forms to view the attributes and incidents-related to the network.

Manage Faults

You can detect the changes in the topology such as PseudoWire VC is down and up by using the iSPI for MPLS views. The iSPI for MPLS provides a quick way to view the enriched incidents that help you quickly understand and react to a problem in your network. For more information, see MPLS Incidents.

Overview of the Multicast-VPN (MVPN)

The iSPI for MPLS helps you to monitor the Multicast VPN (MVPN) network topology.

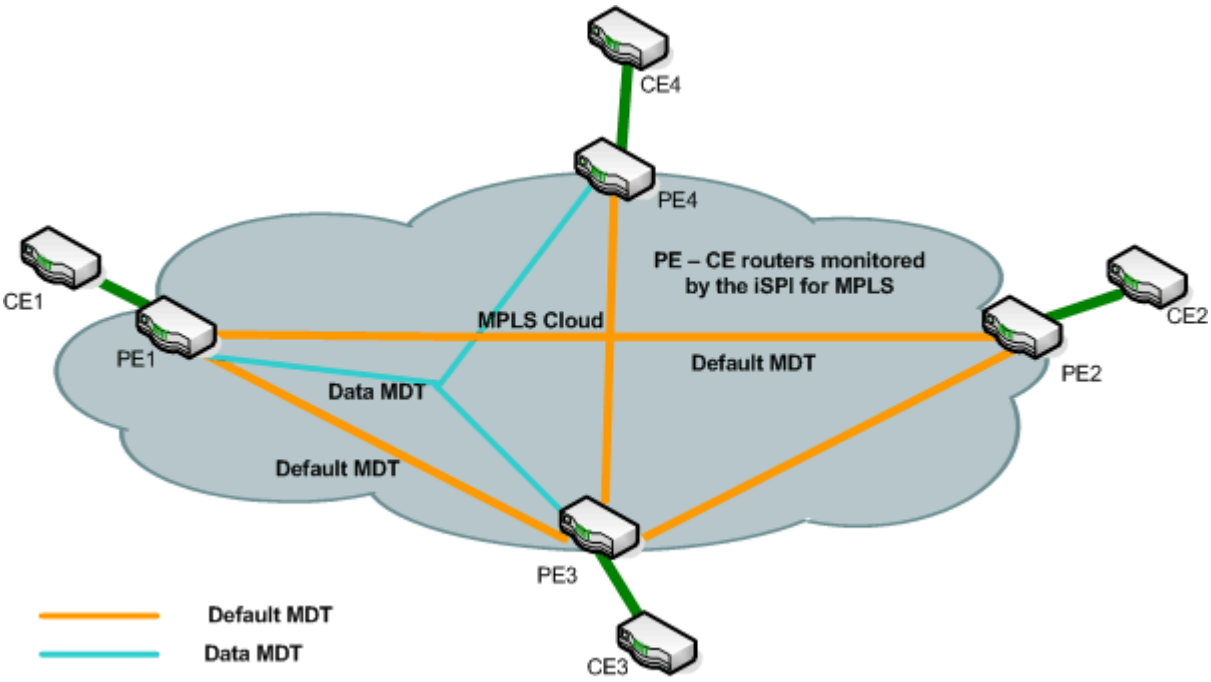
MVPN

In the Layer 3 VPNs, the PE routers use the unicast services to transmit packets. With the emergence of MVPN technology, the service providers use the multicast services to transmit data packets in the core network (between the two PE routers) over an MPLS cloud. In an MVPN topology, the provider edge (PE) routers sit on the perimeter of the service provider's network and communicate with Provider routers inside the MPLS VPN cloud and customer edge (CE) routers that are located and managed at the customer sites.

In the core network, the multicast services are enabled to transmit data packets. The PE routers are configured with multicast-enabled VRF (MVRF) and use the multicast services to transmit the customer multicast traffic.

You can monitor the PE routers that are configured with MVRFs. These PE nodes participate to form an L3 VPN. The set of MVRFs connected to the source and receivers in the CE network form a Multicast Domain (MD). Every MD has a default Multicast Distribution Tree (MDT). The iSPI for MPLS monitors the upstream and downstream MDTs passing through the MVRFs. To view the multicast flow details, start the iSPI for IP Multicast. For more information, see Integrating the iSPI for MPLS with the iSPI for IP Multicast.

Example of an MVPN Network



The PE routers (PE1 and PE2) are monitored by the iSPI for MPLS. The core network consists of the provider routers (PE1, PE2, P1, P2, P3, and P4). The traffic flowing from or into these core routers are monitored by the iSPI for IP Multicast. You can view the downstream path and upstream path to find the multicast flow in the network. For more information, see IP Multicast map view. The iSPI for MPLS helps you perform the following tasks:

Monitor MVPNs and MVRFs:

You can monitor and view the status of the MVRFs and MVPNs in the network. Navigate to MVPN forms to view the MVPN attributes and incidents-related to the network. In addition, view the incidents for the status change such as an MVRF is down that affects an MVPN status.

Manage Faults:

You can view the changes in the topology such as the status of the MVRF changes from up to down and generates a new incident. The iSPI for MPLS provides a quick way to view the enriched incidents that help you quickly understand and react to a problem in your network. For more information, see MPLS Incidents.

Related Topics:

Integrating with the iSPI for IP Multicast

IP Multicast map view

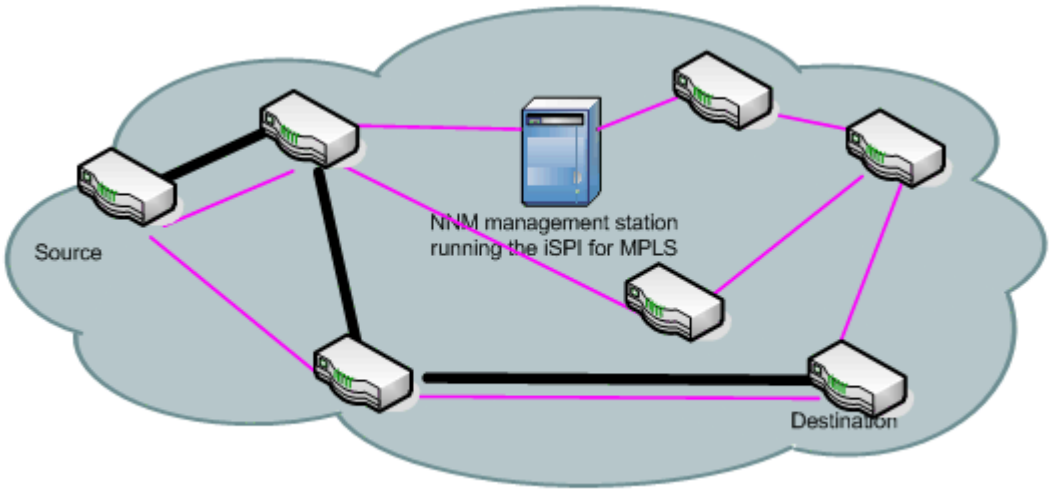
Overview of the MPLS TE Tunnels

In an MPLS Traffic Engineering[1] network, communication between the routers is through the TE tunnels. The TE Tunnels help you manage the data transmission from a source to a destination.

Traffic engineering is defined by the presence of single or multiple paths (tunnels) in the network for the transmission of the packets. The network administrator configures the TE Tunnels to ensure the optimal bandwidth usage and to provide better service. Usually the shortest path is chosen for data transfer but TE tunnels allow traffic to be routed through a specific path (tunnel) helping in the required throughput and bandwidth.

You can monitor the TE tunnels in the network by using the TE Tunnel inventory. In addition, you can find the faults in MPLS traffic engineering tunnels. Check incidents and status tabs.

Example of the TE Tunnels in the network



Managed MPLS Network

The iSPI for MPLS helps you to perform the following tasks:

Monitor TE Tunnels

You can monitor the TE Tunnels participating in the network. You can navigate to L3 VPN forms to view the attributes and incidents-related to the network. This helps in fault management and reduces the Mean Time to Repair (MTTR).

Manage Faults

[1]MPLS Traffic Engineering (MPLS TE) is the process of selecting and reserving the path between the nodes to optimize network resources for better bandwidth utilization and ensure better Quality of Service (QoS). Traffic Engineering (TE) is essential for service provider backbones.

You can detect the changes in the topology such as the status of the TE Tunnel is down. The iSPI for MPLS provides a quick way to view the enriched incidents that help you quickly understand and react to a problem in your network. For more information, see MPLS Incidents.

Overview of the MPLS PseudoWire VC

In an MPLS network, communication between the routers can be through PseudoWire Virtual Channels (VCs).

A PseudoWire VC is a point-to-point link for data transmission between the two nodes using any L2 technology. There are two types of L2 VPNs - Virtual Private Wire Service (VPWS)[1] and Virtual Private LAN Service (VPLS)[2]. In PseudoWire VC, the transmission of data is bi-directional. For example, if there are two endpoints A and B, data transmission is from A to B and B to A. A bidirectional PseudoWire VC consists of a pair of unidirectional LSPs, one in each direction. The unique VC ID in between two endpoints identifies the LSPs. To discover the complete Pseudowire VCs, make sure to discover both the endpoints (VC LSPs).

You can discover and monitor the PseudoWires VCs in the network. The iSPI for MPLS helps you perform the following tasks:

Monitor PseudoWIre VC

You can monitor the PseudoWires VC participating in the network from the Pseudo Wire VC inventory. You can navigate to PseudoWires VC forms to view the attributes and incidents-related to the network.

Manage Faults

The iSPI for MPLS identifies the changes in the topology such as the status of the PseudoWire VC is down by using the iSPI for MPLS views. The iSPI for MPLS provides a quick way to view the enriched incidents that help you quickly understand and react to a problem in your network. For more information, see MPLS Incidents.

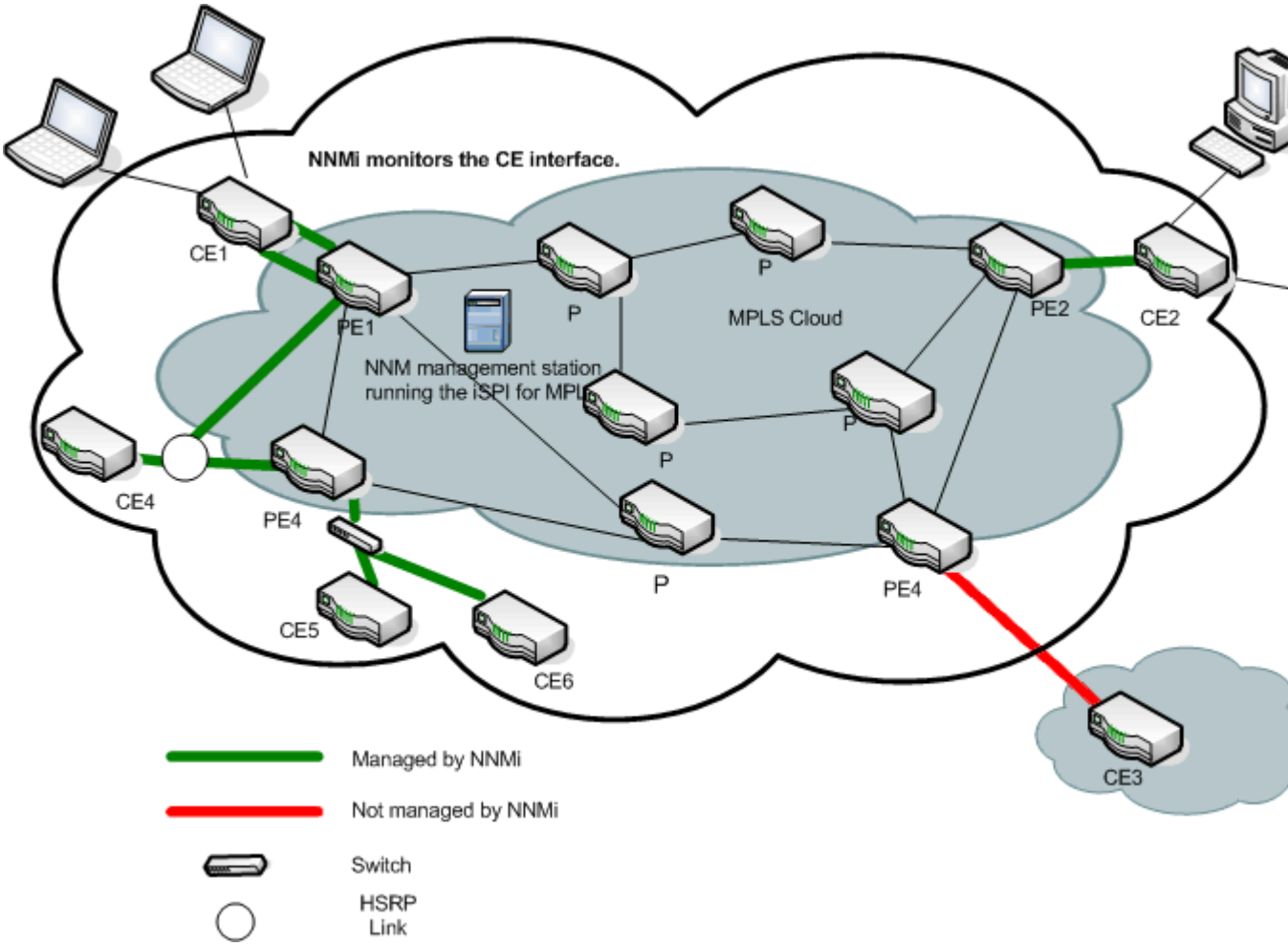
Overview of the MPLS Customer Edge (CE) Management

You can monitor the logical link connectivity between the PE node and CE node in an L3VPN topology. The iSPI for MPLS helps you monitor the following:

- One PE interface connected to one CE interface in the topology.
- One PE interface connected to multiple CE interfaces in the topology. This PE-CE links are connected through a switch in the network.
- Multiple PE interfaces connected to one CE interface on node in the topology. This PE-CE link connectivity is using the Hot Standby Routing Protocol (HSRP).
- Multiple PE interfaces connected to multiple CE interfaces in the topology.

Example of the PE - CE connectivity in the network

[1]A Virtual Private Wire Service VPWS is a point-to-point link through a packet switched network connecting two Customer Edge devices.
[2]A VPLS connects several LAN segments over a packet switched network (PSN).



For example, NNMi monitors the CE1 and CE2 nodes and interfaces on the nodes. The iSPI for MPLS helps you monitor the PE-CE communication links. In addition, the iSPI for MPLS helps you monitor two CE interfaces on the CE node communicating with one PE interface and two PE interfaces communicating with one CE interface. The iSPI for MPLS does not monitor the PE3- CE3 link connectivity as the CE3 node is not available in NNMi topology.

Check the status of the PE interface, CE interface, and the PE-CE connectivity from the MPLS views. View the PE-CE information in the CE Interface tab, PE Interface tab, and L3 VPN tab of the node form. For more information, see Node Form: L3 VPN PE interfaces.

You can monitor your network by using the MPLS L3 VPN Topology map view. For more information, see L3 VPN Topology map view.

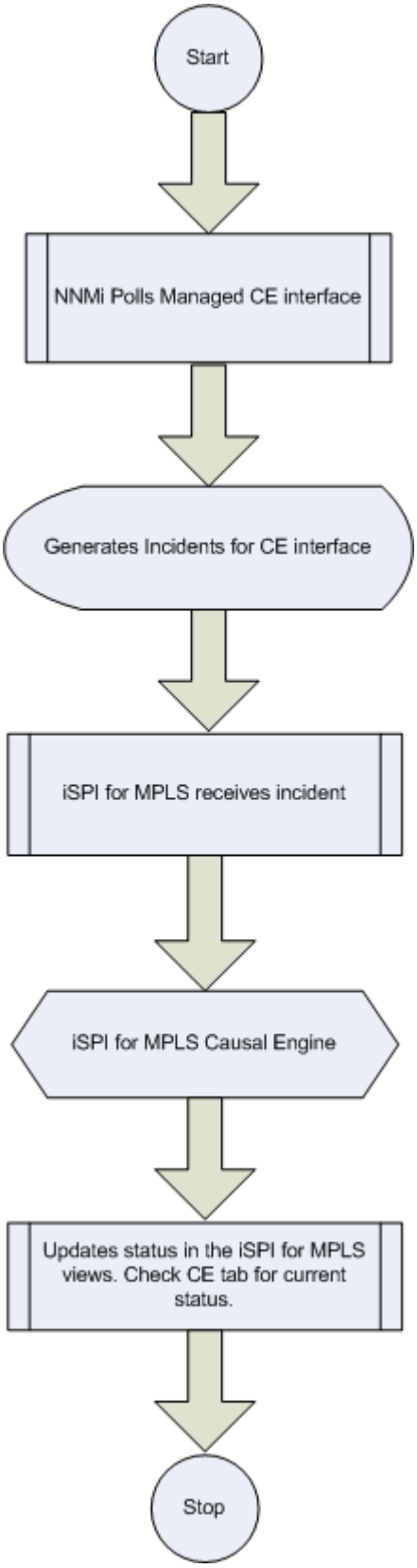
The discovery of CE nodes participating in an L3VPN may require multiple rounds of discovery, even if both the CE node and the corresponding PE node are seeded at the same time. The actual number of discovery cycles (one or two) depends on manageability of CE node and also, the sequence in which the PE and CE nodes are discovered by NNMi and the iSPI for MPLS.

The iSPI for MPLS supports the duplicate IP address for the PE-CE link connectivity. For more information, see Duplicate IP address Support with the iSPI for MPLS.

The iSPi for MPLS uses NNMi capabilities to monitor and manage the CE interface. NNMi polls the CE interface on the CE node and generates incidents whenever the status of the CE interface is down. The

iSPI for MPLS listens to the incident and updates the status of the CE interface in the MPLS views. To show how the iSPI for MPLS updates the status of the CE interface, see the following:

The iSPI for MPLS updates the status of the PE-CE link connectivity


Start
NNMi Polls Managed CE interface
Generates Incidents for CE interface
iSPI for MPLS receives incident
iSPI for MPLS Causal Engine
Updates status in the iSPI for MPLS views. Check CE tab for current status.
Stop

To use the feature of CE management, use **NNMi Configuration** workspace to configure the CE interfaces in the interface group. You should add the interface groups with MPLS capabilities that help in monitoring the PE- CE logical link connectivity.

To add an interface group to include the MPLS CE capabilities from NNMi Configuration workspace, follow these steps:

1. From the workspace navigation panel, select the **Configuration** workspace.
2. Select **Interfaces Groups** ->**Interface Settings** tab.
3. Do one of the following:
   - To create an Interface Settings definition, click the **New** icon.
   - To edit an Interface Settings definition, select a row, click the **Open** icon.
   - To delete an Interface Settings definition, select a row and click the **Delete** button.
4. In the Interface Group form, select the **Additional Filters** tab.
5. Add the following MPLS capability to monitor the CE interfaces `capability = com.hp.nnm-.capability.mpls.iface.l3vpnceiface`.
6. Click **Save and Close.**

To enable polling for the CE interfaces, check the **Global Control** group box from the **Monitoring Configuration** workspace. For more information, see *NNMi Help for Administrator, Using the Monitoring Configuration form*.

Related Topics:

Node Form: L3 VPN PE interfaces

PE Interface Form: L3 VPN Tab

CE Interface Form: L3 VPN Tab

Using the iSPI for MPLS

The iSPI for MPLS helps you to quickly monitor, detect, and troubleshoot abnormal behavior in the network.

To perform a basic monitoring of the MPLS services in the network, you can log on to the NNMi console with the operator (level 1 or 2) or guest credentials. After you log on to the NNMi console, you can view the inventory views introduced by the iSPI for MPLS. The iSPI for MPLS discovers the MPLS-enabled nodes participating in the network. You can access the MPLS views to monitor the status and necessary details for all the MPLS objects.

The following table describes some of the ways that *Help for iSPI for MPLS* assists you in accomplishing your tasks.

Task	Help Topics
Overview	Overview of the MPLS L3 VPN Overview of the VPN, VRFs, and Route Targets Overview of the MPLS TE Tunnel Overview of the MPLS PseudoWire VC Overview of the MPLS L2 VPN Overview of the MPLS CE Management Overview of the Multicast VPN (MVPN)
View the MPLS inventory	Monitoring Your MPLS Inventory
View the details of the devices	Monitoring Your Network with MPLS Forms
View the MPLS incidents	Viewing the MPLS Incidents
View the map views	Viewing the Network Connectivity
Monitor the network health	Monitoring Your Network Health
Monitor your network by using the iSPI for MPLS and RAMS	Integrating the iSPI for MPLS with Router Analytics Management System
Monitor your network by using the iSPI for MPLS and the iSPI for IP Multicast	Integrating the iSPI for MPLS with the iSPI for IP Multicast
Monitor your network by using the iSPI for MPLS and the iSPI Performance for Quality Assurance (QA)	Integrating the iSPI for MPLS with the iSPI Performance for QA

Monitoring Your Network with MPLS Inventory

After the regular discovery of the MPLS nodes in NNMi topology, you can access the MPLS views to monitor the status and check the attributes of the MPLS devices.

The iSPI for MPLS adds a new workspace to the NNMi console—the **MPLS** workspace. You can access all the MPLS views from the iSPI for MPLS workspace. The MPLS views provide the comprehensive list of the discovered MPLS objects. In addition, you can present device details in tables and you can navigate and open the MPLS forms and map views from the MPLS views to access the device details.

View Type	Purpose
LSR(Label-Switched Routers) Inventory	Lists all the MPLS-enabled routers managed by the iSPI for MPLS. The MPLS-enabled routers participates to form the L3 VPNs, L2 VPNs, TE Tunnels, and PseudoWire VCs.
L3 VPN Inventory	Provides a list of available L3VPNs in the network.

View Type	Purpose
MVPN Inventory	Provides a list of available MVPNs in the network.
VPLS VPN Inventory	Provides a list of available VPLS VPNs in the network.
VPWS VPN Inventory	Provides a list of available VPWS VPNs in the network.
PseudoWire VC Inventory	Provides a list of available PseudoWire VCs in the network.
TE Tunnel Inventory	Provides a list of available Traffic Engineering (TE) tunnels in the network.

To launch the MPLS specific views, follow the steps:

1. From the workspace navigation panel, select the **MPLS** workspace.
2. Click < *MPLS views*> to open the selected views. For example, MPLS TE Tunnel Inventory.

Related Topics:

LSR Inventory

L3 VPN Inventory

MVPN Inventory

VPLS VPN Inventory

VPWS VPN Inventory

PseudoWire VC Inventory

TE Tunnels Inventory

LSR (Label-Switched Routers) Inventory

The LSR Inventory is an active table that lists all the nodes participating in L3 VPNs, L2 VPNs, MVPNs, PseudoWire VCs, and TE tunnels. The LSR view is useful to identify all the MPLS-enabled nodes in the network.

Use the LSR inventory for the following tasks:

- Monitor the LSR routers in the network.
- View the problem LSR nodes in the network. Check the status of the LSR routers.
- Access the MPLS Path view.
- Navigate to the node form to check the other attributes of the node.

Basic Attributes

Attribute	Description
Status	The status of the selected node. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical
Name	The name of the router as set by the network administrator.
Device Profile	The device and vendor information of the node.
L3VPN-PE	If the selected MPLS-enabled router participates to form a L3 VPN, the value is true. The possible values are true or false. True is represented by ☑.
L2VPN-PE	If the PseudoWire VCs are configured on the router, the value is true. The possible values are true or false. True is represented by ☑.
TETunnel-Head	If the TE tunnel is configured on the router, the value is true. The possible values are true or false. True is represented by ☑.

Sort Column Data

The sort option is available on the following attributes in the MPLS LSR view:

- Status
- Device Profile
- L3VPN-PE
- L2VPN- PE

For more information, see *Help for NNMi, Use Table View*.

L3 VPN Inventory

The L3 VPN Inventory provides a list of available Layer 3 Virtual Private Network (L3 VPNs) in the network.

Use the L3 VPN Inventory for the following tasks:

- Monitor the nodes participating to form an L3 VPN.
- View and check the status of the available L3VPNs in the network.

- Navigate to the L3 VPN form to check the list and status of VRFs participating in the selected L3 VPN.
- Access an L3 VPN topology map view of the network.

Basic Attributes

Attribute	Description
Name	The system-generated name of the L3 VPN. You can update the system-generated L3 VPN name from the L3 VPN form. Type the new name in the box. Click **Save and Close** button to update the L3 VPN Name. For more information about L3 VPN naming rules, see L3 VPN, VRF, and Route Targets.
Status	The overall status of the L3 VPN. The status of a VPN is derived and calculated based on the status of all the VRFs participating in the VPN. Possible values are: **No Status** - L3 VPN is newly formed and not polled; status of the L3 VPN is No Status. When all the VRFs participating to form an L3 VPN are in an unmanaged mode, the derived status of the VPN is No Status. **Normal** - The status of all the VRFs participating in the L3 VPN is Normal. **Unknown** - The status of all the VRFs participating in the L3 VPN is Unknown. **Warning** - The status of one or all the VRFs participating in the L3 VPN is Unknown, however none of them is Critical. **Minor** - The status of one or all the VRFs participating in the L3 VPN is Critical. **Critical** - The status of all the VRFs participating in the L3 VPN is Critical.
VPN Type	The type of connectivity within a VPN. Possible values are: **Full Mesh** - Full Mesh VPN is formed if all the VRFs have the same RT. The same RT is used for importing and exporting all the VRFs in the specific group. Each VRF exports its route targets to all the other VRFs in the L3 VPN and imports all route targets from the other VRFs in the L3 VPN. **Other** - All the VRFs are not communicating with other VRFs belonging to a VPN. For example, hybrid topology. **Isolated** - A single VRF forms a single L3 VPN. This VRF does not import or export the route targets from any other VRF. **Hub and Spoke** - All the VRFs are communicating with each other by using one VRF which is a Hub VRF and all the other VRFs are Spoke VRFs.
Number of VRFs	A VPN is formed by one or more VRFs. Each VRF is configured on a PE router. This value depicts the number of the VRFs participating to form a VPN.
Multicast-Enabled	When the MPLS - enabled router participates to form an L3 VPN and is capable to transmit multicast packets, the value is true. The possible values are true or false. True is represented by ☑.
Status Last Modified	The status of an L3 VPN is calculated whenever there is a change in topology. The Status Last Modified is the time when the status was last updated.

Filter by Attribute Value

The filter option is available on the following attributes:

- Status
- Name

You can create, change or remove a filter at any time. The iSPI for MPLS saves filters per user so that the filters you specify are maintained during subsequent user sessions.

To create, modify or remove filter in the MPLS L3 VPN view, follow these steps:

1. Right-click the column from the view.
2. Select any one of the following filters:
   - Is not empty
   - Is empty
   - Create filter

   The filtered list appears in the view.

   To create a new filter, select **Create Filter**. Select an option from the following list:

   - Starts with
   - Contains
   - Matches
   - less than or equal
   - greater than or equal

   Type the value in the box. Click **Apply.** The filtered list appears in the view.

To update and change the filter, right-click the attribute and click **Modify filter**.

To remove the filter, right-click the attribute and click **Remove filter**.

For more information, see *NNMi Help, Filter a Table View*.

Sort Column Data

The sort option is available on the following attributes in the MPLS L3 VPN view:

- Status
- Name
- VPN Type
- Status Last Modified

For more information about filter and sort, see *Help for NNMi, Use Table View*.

MVPN Inventory

The MVPN inventory view provides a list of layer 3 Virtual Private Network (VPNs) with multicast services in the network. A Layer 3 VPN can contain more than one Multicast Domain (MD) participating to form multiple MVPNs. Each MVPN consists of one default Multicast Distribution Tree (MDT).

Use the MVPN Inventory for the following tasks:

- Monitor the nodes participating to form an MVPN in the network.
- View the problem MVPNs in the network. Check the status of the available MVPNs in the network.
- Navigate to the MVPN form to check the status of MVRFs.
- Navigate to the iSPI for IP Multicast to view the multicast traffic in the network.
- Access a map view of the network.

Basic Attributes

Attribute	Description
Status	The status of the selected MVPN. The status of the MVPN is derived and calculated based on the status of all the MVRFs participating to form an MVPN. Possible values are: **Normal** - The status of the MVPN is Normal if the status of all the MVRFs participating in the MVPN is Normal. **Unknown** - The status of the MVPN is Unknown if the status of all the MVRFs participating in the MVPN is Unknown. **Warning** - The status of the MVPN is Warning if the status of one or more MVRFs participating in the MVPN are Unknown but none of them is Critical. **Minor** - The status of the MVPN is Minor if one or more MVRFs participating in the MVPN is Critical.
Name	The system-generated name of the selected MVPN. Update the system-assigned MVPN name from the MVPN form. Type the new name in the **Name** box. Click **Save and Close** icon to update the MVPN Name. For more information about the MVPN naming rules, see MVPN Naming Rules.
L3 VPN Name	The selected MVPN is a part of the named L3 VPN.
Default MDT	The Default MDT (Multicast Distribution Tree) is the MDT group address used for forwarding multicast packets in an MVPN network.
Number of MVRFs	The total count of MVRFs participating to form an MVPN. The MVRF is the multicast-enabled VRF which participates to form an MVPN.
Status Last Modified	The Status Last Modified is the time when the status was last set.

Filter by Attribute Value

The filter option is available on the following attributes:

- Status
- Name
- L3 VPN Name
- Default MDT

You can create, change or remove a filter at any time. The iSPI for MPLS saves filters per user so that the filters you specify are maintained during subsequent user sessions.

To create, modify or remove filter in the MPLS MVPN view, follow the steps:

1. Right-click the column from the view.
2. Select any one of the following filters:
   - Is not empty
   - Is empty
   - Create filter

   The filtered list appears in the view.

   To create a new filter, select **Create Filter**. Select an option from the following list:
   - Starts with
   - Contains
   - Matches
   - less than or equal
   - greater than or equal

   Type the value in the box. Click **Apply.** The filtered list appears in the view.

To update and change the filter, right-click the attribute and click **Modify filter**.

To remove the filter, right-click the attribute and click **Remove filter**.

For more information, see *NNMi Help, Filter a Table View.*

Sort Column Data

The sort option is available on the following attributes in the MPLS MVPN view:

- Status
- Name
- L3 VPN Type
- Default MDT
- Status Last Modified

For more information about filter and sort, see *Help for NNMi, Use Table View*.

VPLS VPN Inventory

The MPLS VPLS VPN Inventory provides a list of available VPLS Virtual Private Network (VPNs) in the network.

Use the MPLS VPLS VPN Inventory for the following tasks:

- Monitor the VPLS VPNs in the network.
- View the problem VPLS VPNs. Check the status of the L2VPN.

Basic Attributes

Attribute	Description
Status	The status of the VPLS VPN is derived and calculated based on the status of all the PseudoWires VCs participating in the VPLS VPN. Possible values are: **No Status** - A VPLS VPN is newly formed and not polled, status of the L2 VPN is No Status. When all the PseudoWires VCs participating to form an L2VPN are in an unmanaged mode, the derived status of the VPN is No Status. **Normal** - The status of all the PseudoWires VCs participating to form a VPLS VPN is Normal. **Unknown** - The status of all the PseudoWires VCs participating to form a VPLS VPN is Unknown. **Warning** - The status of one or more PseudoWires VCs participating to form a VPLS VPN is Unknown. In addition, the status of none of the PseudoWire VC is Critical. **Minor** - The status of one or more PseudoWires VCs participating to form a VPLS VPN is Critical. **Critical** - The status of all the PseudoWires VCs participating in a VPLS VPN is Critical.
L2VPN Name	The system-assigned name of the selected VPLS VPN. For example, VPLS_200 is the name of the VPLS VPN whose VPN Id is 200. You can change the system-assigned VPN Name from the VPLS VPN form. Type the new name in the **Name** box. Click the **Save and Close** button to update the L2VPN Name.
VPN ID	The unique identifier of the selected VPLS VPN.
Number of PseudoWiresVCs	The count of the PseudoWires VCs participating to form a VPLS VPN.
Status Last Modified	The time when the status was last updated. The status of the VPLS VPN is calculated whenever there is a change in topology.

Filter by Attribute Value

The filter option is available on the following attributes:

- Status
- L2VPN Name
- VPN ID

You can create, change or remove a filter at any time. The iSPI for MPLS saves filters per user so that the filters you specify are maintained during subsequent user sessions.

To create, modify or remove filter in the MPLS VPLS VPN view, follow these steps:

1. Right-click the column from the view.
2. Select any one of the following filters:
   - Is not empty
   - Is empty
   - Create filter

The filtered list appears in the view.

To create a new filter, select **Create Filter**. Select an option from the following list:

- Starts with
- Contains
- Matches
- less than or equal
- greater than or equal

Type the value in the box. Click **Apply.** The filtered list appears in the view.

To update and change the filter, right-click the attribute and click **Modify filter**.

To remove the filter, right-click the attribute and click **Remove filter**.

For more information, see *NNMi Help, Filter a Table View*.

Sort Column Data

The sort option is available on the following attributes in the MPLS VPLS VPN view:

- Status
- L2VPN Name
- VPN ID

For more information about filter and sort, see *Help for NNMi, Use Table View*.

VPWS VPN Inventory

The MPLS VPWS VPN Inventory provides a list of available VPWS VPNs in the network.

Use the MPLS VPWS VPN Inventory for the following tasks:

- Monitor the VPWS VPNs in the network.
- View the problem VPWS VPNs in the network. Check the status of the L2 VPN.
- Check the Last Status Modified to find out when the L2VPN was updated.

Basic Attributes

Attribute	Description
Status	The status of the L2VPN is derived and calculated based on the status of all the PseudoWire VCs that participates to form the VPWS VPN. Possible values are:  **No Status** - A VPWS VPN is newly formed and not polled, status of the L2VPN is No Status. In addition, when all the PseudoWires VCs participating to form an L2VPN are in an unmanaged mode, the derived status of the VPWS VPN is No Status.  **Normal** - The status of all the PseudoWires VCs participating to form a VPWS VPN is Normal.  **Unknown** - The status of all the PseudoWires VCs participating to form a VPWS VPN is Unknown.  **Warning** - The status of one or more PseudoWires VCs participating to form a

Attribute	Description
	VPLS VPN is Unknown. In addition, the status of none of the PseudoWire VC is Critical. **Minor** - The status of one or more PseudoWires VCs participating to form a VPWS VPN is Critical. **Critical** - The status of all the PseudoWires VCs participating to form a VPWS VPN is Critical.
L2VPN Name	The system-generated name of the selected VPWS VPN. You can update the system-generated L2VPN Name from the VPWS VPN form. Type the new name in the **Name** box. Click **Save and Close** to update the L2VPN Name.
Number of PseudoWires VCs	Lists the count of the PseudoWires VCs participating to form a VPWS VPN. For example, 4, 6, and so on.
Status Last Modified	The time when the status was last updated. The status of the VPWS VPN is calculated whenever there is a change in topology.

Filter by Attribute Value

The filter option is available on the following attributes:

- Status
- L2VPN Name

You can create, change or remove a filter at any time. The iSPI for MPLS saves filters per user so that the filters you specify are maintained during subsequent user sessions.

To create, modify or remove filter in the MPLS VPWS VPN view, follow these steps:

1. Right-click the column from the view.
2. Select any one of the following filters:
   - Is not empty
   - Is empty
   - Create filter

   The filtered list appears in the view.

   To create a new filter, select **Create Filter**. Select an option from the following list:
   - Starts with
   - Contains
   - Matches
   - less than or equal
   - greater than or equal

   Type the value in the box. Click **Apply.** The filtered list appears in the view.

To update and change the filter, right-click the attribute and click **Modify filter**.

To remove the filter, right-click the attribute and click **Remove filter**.

For more information, see *NNMi Help, Filter a Table View*.

Sort Column Data

The sort option is available on the following attributes in the MPLS VPWS VPN view:

- Status
- L2VPN Name

For more information about filter and sort, see *Help for NNMi, Use Table View*.

PseudoWire VC Inventory

The MPLS PseudoWire VC Inventory view provides a list of available PseudoWire VCs in the network.

Use the PseudoWire VC Inventory for the following tasks:

- Monitor the PseudoWire VCs in the network.
- View the problem PseudoWire VC in the network. Check the status of the PseudoWire VC.

Basic Attributes

Attribute	Description
Status	Overall status of the PseudoWire VCs. Possible values are :  **Normal** - The status of both the LSPs (Label Switched Path) is Normal.  **Critical** - The status of any one or both the LSPs is Critical.  **Unknown** - The status of any one or both the LSPs is Unknown.
Id	The unique index ID for each virtual circuit.
Encapsulation Type	The kind of service carried in the specific PseudoWire VC. For example, the services are ATM, Frame Relay, Ethernet VLAN, or Ethernet. If both the endpoints (PE1 and PE2) are discovered but the status of LSPs is not Normal, the value of Encapsulation Type is **Other**.
PE 1	The name of the PE router. The selected router is one of the endpoints of the PseudoWire VC. If the status of PE1 is unknown, unmanaged, or not discovered, the value is blank. If PE2 is managed and discovered, an IP address of PE1 is known and appears in the view.
PE 1 Address	The IP address of the PE1 node on which the specific PseudoWire VC is configured.
PE 2	The name of the PE router. This router is one of the endpoints of the PseudoWire VC. If the status of PE 2 is unknown, unmanaged, or not discovered, the value is blank. If PE1 is managed and discovered, an IP address of PE2 address is known and appears in the view.
PE 2 Address	The IP address of the PE2 on which the specific PseudoWire VC is configured.
L2VPN Type	The selected PseudoWire VC participates to form an L2VPN. Possible values are: • **VPLS-VPN** - The selected PseudoWire VC participates to form a VPLS VPN. • **VPWS-VPN** - The selected PseudoWire VC participates to form a VPWS VPN. • **Blank** - The selected PseudoWire VC does not participate in any L2VPN type (VPLS VPN or VPWS VPN). In addition, if the state of the selected PseudoWire VC is partially discovered, VPN type is blank.

Attribute	Description
	• **Unknown** - The PseudoWire VC is discovered but Encapsulation Type is not known, value is unknown. After the Encapsulation Type is known and the selected PseudoWire VC participates to form an L2VPN, the value is VPWS VPN or VPLS VPN.
L2VPN Name	The name of the L2 VPN associated with the selected PseudoWire VC. Possible values are: • **VPLS Name** - The name of a VPLS VPN. • **VPWS Name** - The name of a VPWS VPN. After you configure the VPWS group from **MPLS Configuration** workspace, the same name appears in this field. • **Default Group** - The L2VPN is known as Default Group when the selected PseudoWire VC is partially discovered and does not participate to form a VPLS VPN or VPWS VPN.
Status Last Modified	The status of the PseudoWire VCs is calculated whenever there is a change in the topology. The Status Last Modified is the time when the status was last set.

Filter by Attribute Value

The filter option is available on the following attributes in the PseudoWire VC Inventory:

- Status
- Id

You can create, change or remove a filter at any time. The iSPI for MPLS saves filters per user so that the filters you specify are maintained during subsequent user sessions.

To create, modify or remove filter in the PseudoWire VC view, follow the steps:

1. Right-click the column from the view.
2. Select any one of the following filters:
   - Is not empty
   - Is empty
   - Create filter

   The filtered list appears in the view.

   To create a new filter, select **Create Filter**. Select an option from the following list:
   - Starts with
   - Contains
   - Matches
   - less than or equal
   - greater than or equal

   Type the value in the box. Click **Apply.** The filtered list appears in the view.

To update and change the filter, right-click the attribute and click **Modify filter**.

To remove the filter, right-click the attribute and click **Remove filter**.

For more information, see *NNMi Help, Filter a Table View.*

Sort Column Data

The sort option is available on the following attributes in the PseudoWire VC Inventory:

- Status
- Name
- VPN Type
- Status Last Modified

For more information about filter and sort, see *Help for NNMi, Use Table View*.

TE Tunnel Inventory

The TE Tunnel Inventory provides a list of available Traffic Engineering (TE) tunnels in the network.

Use the TE Tunnel Inventory for the following tasks:

- Monitor the TE Tunnels in the network.
- Check the status and bandwidth of the TE Tunnel.
- Access the TE Tunnel Path view (map view).

Basic Attributes

Attribute	Description
Status	Overall status of the TE Tunnel. Possible values are :  **Normal** - If the status of the TE Tunnel is Up, the status of the TE Tunnel is Normal.  **Critical** - If the status of the TE Tunnel is Down, the status of the TE Tunnel is Critical.  **Unknown** - If there is no SNMP response for the selected node and the selected TE Tunnel is configured on this node, the status of the TE Tunnel is Unknown.
Name	The name of the selected TE tunnel.
Head	The selected TE Tunnel starts from a node. This node is known as the head node. The head and name together makes a unique identification for the selected tunnel. Multiple tunnels originate from the same head router. If a head router is an unmanaged node or does not respond to SNMP query at the time of discovery, no tunnels that start from the head router are discovered. To view the head node details, click the  LookUp icon.
Tail	The selected TE Tunnel terminates at a node. This node is known as the tail node. Sometimes, the tail node is not discovered or managed by NNMi, field is blank. To view the tail node details, click the  LookUp icon.
Tail IP Address	The IP address of the tail node. The Tail IP address is useful when the tail node is not discovered by NNMi.
Bandwidth	The bandwidth configured for the selected TE Tunnel. The value is the maximum data rate for the particular tunnel. For Juniper routers, the value is calculated for the following versions: • 9.6 and above • 9.3R4, 9.4R3, 9.5R2 maintenance releases. For other Juniper nodes, the value is Unknown. For Cisco routers, the value is zero when the status of the TE tunnel is down at the time of

Attribute	Description
	first discovery. Wait till the next discovery to view the actual bandwidth. The value changes only if the status of the TE Tunnel changes from Down to Up.
Description	Information given for the TE Tunnel at the time of configuration.

Filter by Attribute Value

The filter option is available on the following attributes:

- Status
- Name

You can create, change, or remove a filter at any time. The iSPI for MPLS saves filters per user so that the filters you specify are maintained during subsequent user sessions.

To create, modify, or remove filter in the MPLS TE Tunnel view, follow the steps:

1. Right-click the column from the view.
2. Select any one of the following filters:
   - Is not empty
   - Is empty
   - Create filter

   The filtered list appears in the view.

   To create a new filter, select **Create Filter**. Select an option from the following list:
   - Starts with
   - Contains
   - Matches
   - less than or equal
   - greater than or equal

   Type the value in the box. Click **Apply.** The filtered list appears in the view.

To update and change the filter, right-click the attribute and click **Modify filter.**

To remove the filter, right-click the attribute and click **Remove filter**.

For more information, see *NNMi Help, Filter a Table View*.

Sort Column Data

The sort option is available on the following columns in the MPLS TE Tunnel view:

- Status
- Name
- Tail IP Address
- Bandwidth
- Description

For more information about filter and sort, see *Help for NNMi, Use Table View*.

Monitoring Your Network with MPLS Forms

You can use the MPLS forms to view the details associated with the iSPI for MPLS object.

Use the MPLS forms to complete the following tasks:

- View the additional attributes of the MPLS objects.
- Determine the health of the MPLS objects. Check the Status tab.
- Investigate the reason of status change of the MPLS object. Check the Incidents and Conclusions tab.
- Access a map view of the network.
- Navigate to the tabs associated with the MPLS objects.

The following MPLS forms are available from the MPLS workspace:

Form Name	Description
L3VPN Form	Provides details about the selected L3 VPN. For more information, see L3 VPN Form.
VRF Form	Provides details about the selected VRF that participates in a L3 VPN. For more information, see VRF Form.
TE Tunnel Form	Provides details about the selected TE tunnel. For more information, see TE Tunnel Form.
PseudoWire VC Form	Provides details about the selected PseudoWire VCs. For more information, see PseudoWire VC Form.
VC LSP Form	Provides details about the selected VC LSP. For more information, see VC LSP Form.
VPLS-VPN Form	Provides details about the selected VPLS VPN. For more information, see VPLS VPN Form.
VPWS-VPN Form	Provides details about the selected VPWS VPN. For more information, see VPWS VPN Form.
MVPN Form	Provides details about the selected MVPN. For more information, see MVPN Form.
MDT Form	Provides details about the selected MDT. For more information, see MDT Form.

To view the MPLS forms, follow these steps:

(1. From the Left navigation panel, select the MPLS workspace and click <MPLS> view (for example, **MPLS- > MPLS L3 VPN view**).

2. Click the  **Open** icon to view the detailed information about a specific object. The form shows the information specific to the MPLS object.)

L3 VPN Form

The L3 VPN form provides details of the VRFs and MVRFs participating to form an L3 VPN or a MVPN. In addition, the L3 VPN form shows the PE routers configured with VRFs and MVRFs participating to form an L3 VPN. All PE routers containing VRFs and MVRFs relevant to the named L3 VPN are grouped in one VPN and displayed in the inventory.

Use the L3 VPN Form for the following tasks:

- Monitor the VRFs participating in the selected L3 VPN.
- Check the VRFs tab to view the status of the VRFs participating in the selected L3 VPN.
- Navigate to the VRF form to check more details of the selected VRF.
- Check the MVPN tab to view the status of the available MVRFs participating in the selected MVPN. The MVPN tab appears only when the multicast services are enabled in the selected L3 VPN.
- Check the Incidents tab to view the cause of the change in the status.
- Access the L3 VPN topology map view of the network.

Basic Attributes

Attribute	Description
Name, VPN Type, Status, VPN Name, Number of VRFs, Multicast Enabled	The attributes listed in the L3 VPN form are same as available in the L3 VPN Inventory view. For more information, see L3 VPN Inventory.
Create Time	The time when the selected L3 VPN was formed.
Status Last Modified	The status of the L3 VPN is calculated whenever there is a change in topology. The Status Last Modified is the time when the status was last set.
Hub VRF	The name of the VRF participating to form a Hub - Spoke VPN. To open the hub VRF, click the LookUp icon.

For more information about the tabs, see VRFs Tab, MVPN Tab, Status Tab, Conclusions Tab, Incidents Tab, RAMS Traps Tab, and Registration Tab.

L3 VPN Form: VRFs Tab

The L3 VPN form provides details about the selected L3 VPN. The VRF tab provides details of all the VRFs participating to form an L3 VPN. Each row represents one VRF. If there are five VRFs participating in an L3 VPN, there are five rows available in the form. To navigate to the VRF form, click the **Open** icon.

Basic Attributes

Attribute	Description
VRF Attributes	The attributes listed in the VRF tab are same as available in VRF form. For more information, see VRF Form.

L3 VPN Form: MVPNs Tab

The Multicast VPN (MVPN) tab provides details about the available MVPNs in the selected L3 VPN.

Basic Attributes

Attribute	Description
Status, Name, Default MDT	The attributes listed in the MVPN tab are same as available in MVPN Inventory. For more information, see MVPN Inventory.

L3 VPN Form: Status Tab

The L3 VPN Form provides details about the all the VRFs participating in an L3 VPN. The status tab is useful for obtaining a quick summary of an MPLS object status to monitor any significant patterns in behavior and activity.

Overall Status

Attribute	Description
Status	The overall status of the L3 VPN. The status of the L3 VPN is derived and calculated based on the status of all the VRFs participating in the L3 VPN. Possible values are: **No Status** - An L3 VPN is newly formed and not polled, status of the L3 VPN is No Status. When all the VRFs participating to form an L3 VPN are in unmanaged mode, the derived status of the L3 VPN is No Status. **Normal** - The status of the L3 VPN is Normal if the status of all the VRFs participating in the L3 VPN is Normal. **Unknown** - The status of the L3 VPN is Unknown if the status of all the VRFs participating in the L3 VPN is Unknown. **Warning** - The status of the L3 VPN is Warning if the status of one or all the VRFs participating in the L3 VPN is Unknown, however none of them is Critical. **Minor**- The status of the L3 VPN is Minor if the status of one or all the VRFs participating in the L3 VPN is Critical. **Critical** - The status of the L3 VPN is Critical if the status of all the VRFs participating in the L3 VPN is Critical.
Last Modified	Date and time when status was last set.

Status History

Attribute	Description
Status History	List of the last thirty status updates for the selected L3 VPN.

L3 VPN Form: Conclusions Tab

The VPN Form contains details about the all the VRFs participating in the VPN. The Conclusions tab shows the results of the overall derived status. You can view a quick summary of the status and problem description for the selected L3 VPN.

Conclusions Table

Attribute	Description
Status	The derived status of the selected L3 VPN. For more information, see VPN Form: Status tab.
Time Stamp	Current status is calculated and set by Causal Engine. The Time Stamp data is the time when the status of the VPN is calculated and last updated in the view.
Conclusions	The conclusions are set by the Causal Engine after the status calculation. Possible conclusions are: • **VPNCritical** • **VPNNormal** • **VPNUnknown** • **VPNMinor** • **VPNWarning** • **VPNHubVRFUp**

L3 VPN Form: Incidents Tab

The VPN Form provides details about the selected VPN.

The Incidents tab provides details of all the Service Impact incidents associated with the selected L3 VPN. The service impact incident is useful to identify and troubleshoot the service that is affected.

NNMi generates incidents for a CE node or interfaces that are participating to form an L3 VPN. The iSPI for MPLS receives the notification and generates an incident that provides details of the affected L3 VPNs in the network. The iSPI for MPLS generates multiple service impact incidents such as Interface Down or Node Down for an L3 VPN. The status of the L3 VPNs does not change with the service impact incidents.

Incidents Table

Attribute	Description
Incidents Attributes	The attributes listed in the incidents tab are same as available in NNMi Incidents form. For more information about the attributes, see the Help for *NNMi Incidents Form.* You can cross launch the VPN or the source node from the service impact incident such as MplsL3VPNImpacted.

L3 VPN Form: RAMS Traps Tab

The VPN form provides details about the selected VPN. The RAMS[1] Traps tab provides details of all the traps generated by a RAMS appliance for the selected L3 VPN.

[1]Route Analytics Management System

After the integration with RAMS, the iSPI for MPLS receives the status traps. These traps are sent by a RAMS appliance for the L3 VPNs within the managed network. The iSPI for MPLS monitors the L3 VPNs by listing the RAMS traps in the L3VPN view. The trap list shows the current 100 traps. The RAMS tab appears even when the iSPI for MPLS is not integrated with a RAMS appliance.

Basic Attributes

Attribute	Description
Attributes	The attributes listed in the incidents tab are same as available in NNMi Incidents form.

L3 VPN Form: Registration Tab

The L3 VPN Form provides details about the selected VPN.

Registration Table

Attribute	Description
Create Time	Date and time the selected L3 VPN was created.
Status Last Modified	Date the selected L3 VPN was last modified.

VRF Form

The VRF form provides details about the selected VRF or MVRF participating to form an L3VPN or MVPN.

Use the VRF form for the following tasks:

- Monitor the VRFs or MVRFs participating in the selected L3 VPN or MVPN. The MVRF and MVRF Status tab appear in the VRF form only when multicast services are enabled in the selected VRF.
- Check the PE Interfaces and CE interfaces tab to view the status and other attributes of the selected VRF.
- Check the Incidents tab to view the cause of the change in the status.
- Access an L3 VPN topology map view of the network.

Basic Attributes

Attribute	Description
Name	The name of a VRF as configured on the PE router.
PE Node	The name of the router. The name can be hostname or IP address. The PE node is the Provider Edge router on the edge of the service provider's network that communicates with other provider devices and with customer devices. The selected VRF or MVRF is configured on the PE Node. Click the LookUp icon to access the node details. For more information for the node, see *NNMi Help*.
Status	Overall status for the current VRF. Possible values are: **No Status**- The VRF is newly created and not polled, status is No Status. **Normal** - The operstatus of the VRF is Up, status is Normal.

Attribute	Description
	Unknown - The VRF is not reachable or not responding, status is Unknown. **Critical** - The operstatus of the VRF is Down when the status of all the interfaces on the VRF is Down, status is Critical.
Management Mode	The iSPI for MPLS uses the NNMi properties to find whether the current node is being managed by NNMi. This field also lets you specify whether a node is temporarily out of service. Possible values are: **Managed** – The node, interface, or address is managed by NNMi. **Not Managed** – The node is intentionally not managed. For example, the node might not be accessible because it is in a private network. NNMi does not update discovery information or monitor these nodes. **Out of Service** – A node is unavailable because it is out of service. NNMi does not update discovery information or monitor these nodes. This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed. For more information, see the *Help for NNMi*,*View the Management Mode for an Object in Your Network*.
Description	The description value is obtained from the PE router during the discovery process.
RD	The numerical route distinguisher of the VRF. This value is stored on the PE router and is unique across the service provider's network. The unique value provides the accurate resolution of the overlapping IP address domains.
Multicast-VRF(MVRF)	The selected VRF has permissions to transmit multicast data packets. The status of the flag is either true or false. This flag is only available for Cisco nodes. True is represented by ☑.
Hub VRF	The selected VRF is a Hub VRF. True is represented by ☑
QA Probes	The selected VRF is configured to run tests from the iSPI Performance for Quality Assurance (QA). True is represented by ☑
Configured Interfaces	The total number of interfaces configured on the selected VRF.
Discovered Interfaces	The number of interfaces on the selected VRF that are discovered by the iSPI for MPLS. The rows on the PE Interfaces tab are same as the number of the discovered interfaces.
Create Time	The time when the VRFs was discovered.
Status Last Modified	The selected VRF is polled in the regular intervals and status change is recorded. The Status Last Modified is the time when the status of the VRF was last set.
Mean Time Between Failures	Total time for which the selected VRF was last available divided by the total number of occurrences when the status of the VRF was down. When the iSPI Performance for Metrics is not installed, value is **Not Computed**.

Attribute	Description
Mean Time To Recovery	The time taken to restore the status of the selected VRF from Down to Up divided by the total number of occurrences when the status of the VRF was changed from Down to Up. When the iSPI Performance for Metrics is not installed, value is **Not Computed**.
L3 VPN	The selected VRF belongs to the specified L3VPN. Access the L3 VPN form from the  LookUp icon.

For more information about the tabs, see PE Interfaces Tab, CE Interfaces Tab, Neighbors VRFs Tab, Route Targets Tab, MVRF Tab, Upstream MDTs, Downstream MDTs, MVRF Status, Status Tab, Conclusions Tab, Incidents Tab, andRegistration Tab.

VRF Form: PE Interfaces Tab

The VRF form provides details about the selected VRF.

The PE Interface tab provides details of the Provider Edge interfaces associated with the current VRF. Use this table to determine the attributes of the interfaces as derived from NNMi. For more information, see *NNMi Interface Form*.

General Attributes

Attribute	Description
PE Interfaces Attributes	The attributes listed in the PE interface tab are same as available in NNMi Interface form. For more information, see the Help for *NNMi Interface Form.*

VRF Form: CE Interfaces Tab

The VRF Form provides details about the selected VRF. The Customer Edge (CE) Interface tab provides details of all the CE interfaces associated with the selected PE node in the current VRF.

Basic Attributes

Attribute	Description
Status, IfName, IfAlias	The attributes listed in the CE Interface tab are same as available in NNMi Interface form. For more information, see the Help for *NNMi Interface Form.*
CENode	The name of the CE node where the CE interface is configured.
PE IfName	The name of the associated PE interface.

VRF Form: Neighbor VRFs Tab

The VRF form provides details about the selected VRF.

The Neighbor VRF tab lists the VRF neighbors of the selected VRF. A VRF neighbor is a VRF configured on a remote PE router that exports at least one route target imported by the selected VRF. If an RT belongs to more than one VRF, then all the VRFs are grouped by the named L3 VPN.

Basic Attributes

Attributes	Description
Neighbor VRFs	Table view of the neighbor VRFs associated with the current VPN. Use this table to determine all neighbor VRFs. The attributes listed in the tab are same as available in VRF form. For more information, see VRF Form.

VRF Form: Route Target Tab

The VRF Form provides details about the selected VRF. The Route Target (RT) tab provides details about the attributes of the RTs participating in the VRF.

Each VRF includes a list of import and export route targets that identify the VRFs grouping to form an MPLS L3 VPN in the network. The iSPI for MPLS reads the route targets from the import (routing information received from the target VPN) and export (routing information sent to the target VPN) list. This list helps to identify the VRF neighbors. These relationships determine the routes through the network. Configure the RTs to group the VRFs to form an MPLS L3 VPN **from the MPLS Configuration** workspace. The following options are available from the MPLS Configuration workspace:

- Add a new RT
- Edit the existing RT
- Delete the RT

Whenever you update the list of RTs, the iSPI for MPLS discovers the route targets and forms the new L3 VPNs to keep your topology up-to-date. For more information, see Configuring the iSPI for MPLS.

Basic Attributes

Attribute	Description
Route Target	The list of RTs (imported and exported) for the selected VRF. Example, 100:20, 100:10
Exported	The selected RT that is exported for the selected VRF. True is represented by ☑.
Imported	The selected RT that is imported for the selected VRF. True is represented by ☑.
Excluded	The selected RT that is ignored for the selected VRF.

VRF Form: QA Probes Tab

The VRF form provides details about the selected VRF. The QA Probes tab provides details of the tests configured for the selected VRF. For more information, see *iSPI Performance for QA Form*.

General Attributes

Attribute	Description
QA Probes	The attributes listed in the PE interface tab are same as available in iSPI Performance of QA form. For more information, see the Help for *NNMi Interface Form.*

VRF Form: MVRF Tab

The VRF form provides details about the selected MVRF. The Multicast VRF (MVRF) tab lists the details of the MVRFs and Data MDTs participating to form an MVPN.

MVRF Details

Attribute	Description
Default MDT, Data MDT Range, Data MDT Threshold, Multicast Tunnel IF, Status, Status Last Modified	The attributes listed are same as available in the MVRF tab. For more information about the attributes, see MVPN Form: MVRF Tab.
MVPN	The selected MVRF participates in the named MVPN.

VRF Form: Upstream MDTs Tab

The VRF form provides details about the selected MVRF. The Upstream MDT tab lists the MDT flow details starting from the selected VRF. The selected VRF on the PE router is the source to send all the multicast flows.

MDT Attributes

Attribute	Description
MDT Attributes	The attributes listed in the VRF Form are same as available in MVPN form. For more information, see MVPN form: MDT Tab.

VRF Form: Downstream MDTs Tab

The VRF form provides details about the selected MVRF. The Downstream MDT tab provides the MDT flow details received by the selected VRF. The selected VRF on the PE router receives all the multicast flows.

MDT Attributes

Attribute	Description
MDT Attributes	The attributes listed in the VRF Form are same as available in MVPN form. For more information, see MVPN form: MDT Tab

VRF Form: Status Tab

The VRF Form provides details about the selected VRF. You can use the Status tab to view the status summary the selected VRF.

Overall Status Table

Attribute	Description
Status	Overall status for the current VRF. Possible values are:

Attribute	Description
	No Status - The VRF is newly created and not polled, status of the VRF is No Status. **Normal** - The operstatus of the VRF is Up, status of the VRF is Normal. **Unknown** - The VRF is not reachable or not responding, status is Unknown. **Critical** - The operstatus of the VRF is Down, status of the VRF is Critical.
Last Modified	Date and time when the status was last set.

Status History

Attribute	Description
Status History	List of last thirty status updates for the selected VRF. For more information, see *NNMi Status tab.*

VRF Form: MVRF Status Tab

The VRF form provides details about the selected VRF. The MVRF Status tab is useful for obtaining a quick summary of the selected MVRF status. The MVRF tab only appears if the selected VRF is configured with MVRF capabilities.

Overall Status Table

Attribute	Description
Status	Overall status of an MVRF. The status of the MVRF is derived from the status of the VRF which is polled at the regular intervals. In addition, the MVRF status is also calculated based on the status of Multicast Tunnel interface (MTI) and the status of the PIM neighbors. Possible values are: **Normal** - The status of the VRF is Normal and MTI is Up, status of the MVRF is Normal. **Unknown** - The status of the VRF is Unknown and MTI is Up, status of the MVRF is Unknown. **Critical** - The status of the VRF is Unknown, the status of MTI is Down, or both, status of the MVRF is Critical.
Last Modified	Date and time when the status was last set.

Status History

Attribute	Description
Status History	List of last thirty status updates for the selected MVRF. For more information, see *NNMi Status tab.*

VRF Form: Conclusions Tab

The VRF form provides details about the selected VRF. The Conclusions tab shows the results of the overall derived status. You can view a quick summary of the status and problem description for the selected VRF.

Conclusions Table

Attributes	Description
Status	The status of the selected VRF is dependent on the status of the interface on the selected VRF. For more information, see VRF Form: Status tab.
Time Stamp	The Time Stamp data is the time when the status of the VRF is last set.
Conclusions	The conclusions are set by the Causal Engine after the status calculation. Possible conclusions are: • **MplsVRFDown** • **MplsVRFUp** • **MplsVRFUnknown** Example: The conclusion MplsVRFDown sends an MplsVRFDown incident.

VRF Form: Incidents Tab

The VRF form provides details about the selected VRF. The Incidents tab provides details about the problem description for the selected VRF.

Incidents Table

Attribute	Description
Incidents Attributes	The attributes listed in the incidents tab are same as available in NNMi Incidents form. For more information for the attributes, see the Help for *NNMi Incidents Form*.

VRF Form: Registration Tab

The VRF form provides details about the selected VRF.

Registration Table

Attribute	Description
Create Time	Date and time the selected VRF was created.
Status Last Modified	Date the selected VRF was last modified.

MVPN Form

The MVPN form provides details about the selected Multicast VPN (MVPN).

Use the MVPN form for the following tasks:

- Monitor the MVRFs participating in the selected MVPN.
- Check the MVRFs tab to view the status of the MVRFs participating in the selected L3 VPN.
- Navigate to the VRF form to check more details about the selected MVRF.
- Check the MVPN tab to view the status of the available MVRFs participating in the selected MVPN.
- Check the Incidents tab to view the cause of the change in the status.
- Access an L3 VPN topology map view of the network

Basic Attributes

Attribute	Description
Name, Status, Default MDT, L3 VPN Name, Number of MVRFs	The attributes listed in the MVPN form are same as available in the MVPN Inventory view. Click the **LookUp** icon to access the node. For more information about MVPN attributes, see MVPN Inventory.
Create Time	The time when the selected MVPN was formed and created.
Status Last Modified	The Status Last Modified is the time when the status was last set.

For more information about the tabs, see MVRFs Tab, MDTs Tab, Status Tab, Conclusions Tab, and Registration Tab.

MVPN Form: MVRFs Tab

The MVPN form provides details about all the MVRFs participating in the selected MVPN. The Multicast VRF (MVRF) tab provides details of the MVRFs participating in the MVPN. Each row represents one MVRF. If there are five MVRFs participating in the MVPN, there are five rows available in the form. To navigate to the MVRF form, click the **Open** icon.

MVRF Attributes

Attribute	Description
Status	Overall status of an MVRF. The status of the MVRF is derived from the status of the VRF which is polled at the regular intervals. In addition, the MVRF status is also calculated based on the status of Multicast Tunnel interface (MTI) and the status of the PIM neighbors. Possible values are: **Normal** - The status of the VRF is Normal and MTI is Up, status of the MVRF is Normal. **Unknown** - The status of the VRF is Unknown and MTI is Up, status of the MVRF is Unknown. **Critical** - The status of the VRF is Unknown or MTI is Down, or both, status of the MVRF is Critical.
Name	The name of the selected MVRF.
PE Node	The router name in the database. The name can be hostname or IP address. The PE node is the Provider Edge router on the edge of the service provider's network that communicates with other provider nodes and the customer nodes.

Attribute	Description
Multicast Tunnel IF	The name of the Multicast tunnel interface.
Default MDT	The MDT group address used for forwarding the multicast packets in the MVPN network.
Data MDT Range	The range of the group addresses for a specific MVPN group.
Data MDT Threshold	The maximum bandwidth value configured on the selected MVRF for the MVPN traffic using the Data MDT.

MVPN Form: MDTs Tab

The MVPN form provides details about the Multicast Distribution Tree (MDT) flows passing through the selected MVPN. Navigate to the iSPI for IP Multicast from MDT tab.

MDTs Attributes

Attribute	Description
Customer Source	The IP address of the source which receives the multicast flows.
Customer Group	The group IP address used to encapsulate the multicast flows of the customer.
Provider Source	The IP address of the source PE node.
Provider Group	The group IP address of the PE node.
Type	The kind of MDT flow such as Default MDT flow and Data MDT flow.
MVRF Name	The name of the selected MVRF. This MVRF is the source to start all the multicast flows.

MVPN Form: StatusTab

The MVPN form provides details about the selected MVRF. You can use the Status tab to view the status summary the selected MVPN.

Overall Status Table

Attribute	Description
Status	The status of the selected MVPN. The status of the MVPN is derived and calculated based on the status of all the MVRFs participating to form an MVPN. Possible values are:  **Normal** - The status of the MVPN is Normal if the status of all the MVRFs participating in the MVPN is Normal.  **Unknown** - The status of the MVPN is Unknown if the status of all the MVRFs participating in the MVPN is Unknown.  **Warning** - The status of the MVPN is Warning if the status of one or more

Attribute	Description
	MVRFs participating in the MVPN are Unknown but none of them is Critical.  **Minor** - The status of the MVPN is Minor if one or more MVRFs participating in the MVPN is Critical.  **Critical** - The status of the MVPN is Critical if the status of all the MVRFs participating in the MVPN is Critical.
Last Modified	Date and time when the status was last set.

Status History

Attribute	Description
Status History	List of last thirty status updates for the selected MVPN.

MVPN Form: Conclusions Tab

The MVPN form provides details about all the MVRFs participating in the MVPN. The Conclusions tab shows the results of the overall derived status. You can view a quick summary of the status and problem description for the selected MVPN.

Conclusions Table

Attribute	Description
Status	The derived status of the selected MVPN. For more information, see MVPN Form: Status tab.
Time Stamp	Current status is calculated and set by the Causal Engine. The Time Stamp data is the time when the status of the MVPN is calculated and last updated in the view.
Conclusions	The conclusions are set by the Causal Engine after the status calculation. Possible conclusions are: • **MVPNNormal** • **MVPNCritical** • **MVPNUnknown** • **MVPNMinor** • **MVPNWarning**

MVPN Form: Registration Tab

The MVPN form provides details about the selected MVPN.

Registration Table

Attribute	Description
Create Time	Date and time the selected MPLS object instance was created.
Status Last Modified	Date the selected object instance was last modified.

Attribute	Description

PseudoWire VC Form

The PseudoWire VC form provides details about the selected PseudoWire Virtual Circuit (VC).

Basic Attributes

Attribute	Description
Id, Encapsulation Type, PE 1, PE 1 Address, PE 2, PE 2 Address, L2VPN Type, and Status	The attributes listed in the PseudoWIre VC Form are same as available in the PseudoWIre VC Inventory. For more information, see PseudoWire VC Inventory.
VPLS Name	The name of the VPLS VPN. Click the **Lookup** icon to show more information about the VPLS VPN.
VPWS Name	The name of the VPWS VPN. Click the **Lookup** icon to view more information about the VPWS VPN.
Discovery State	The state of the PseudoWire VCs. Possible values are: **Fully Discovered** - Both the endpoints (PE1 and PE2) are discovered and the status of both the LSPs is normal. **Partially Discovered** - One of the endpoint is discovered and other endpoint is unknown, unmanaged, or not discovered. For example, if PE1 is discovered and PE2 is unknown, unmanaged, or not discovered. You can only get PE1 information and PE2 IP Address. This state is partially discovered.
Create Time	The time when the PseudoWire VCs was discovered.
Status Last Modified	The status of the PseudoWire VC is calculated whenever there is a change in topology. The Status Last Modified is the time when the status was last updated.

PseudoWire VC Form: VC LSP Tab

The PseudoWire VC Form provides details about the selected PseudoWire VC. The VC LSP tab provides the list of the VC LSPs participating to form a PseudoWire VC.

Basic Attributes

Attribute	Description
Attributes	The attributes listed in the VC LSP tab are available in the VC LSP form. For more information, see VC LSP Form.

PseudoWire VC Form: Status Tab

The PseudoWire VC form provides details about the selected PseudoWire VC. You can use the Status tab to view the status summary the selected PseudoWire VC.

Overall Status Attributes

Attribute	Description
Status	Overall status of the PseudoWires VC. The overall status is derived by the status of the VC LSPs participating to form a PseudoWire VC. Possible values are :  **Normal** - The status of both the LSPs is Normal.  **Critical** - The status of any one or both the LSPs is Critical.  **Unknown** - The status of any one or both the LSPs is Unknown.
Last Modified	Date and time when status was last set.

Status History

Attribute	Description
Status History	List of last thirty status updates for the selected PseudoWire VC.

PseudoWire VC Form: Conclusions Tab

The PseudoWire VC Form provides details about the selected PseudoWire VC. The Conclusions tab shows the results of the overall derived status. You can view a quick summary of the status and problem description for the selected PseudoWire VC.

Conclusions Table

Attribute	Description
Status	Overall status of the PseudoWire VC. For information about the possible status values, see PseudoWire VC Form: Status Tab.
Time Stamp	The time when the status of the PseudoWire VC is last set.
Conclusions	The conclusions are set by the Causal Engine after the status calculation. Possible conclusions are: • **MplsPseudoWireVCDown** • **MplsPseudoWireVCNormal** • **MplsPseudoWireVCUnknown** The PseudoWire VC down conclusion generates the incident to send the alert for the status attribute. For example, MplsPseudoWireVCDown generates MplsPseudoWireVCDown incident

PseudoWire VC Form: Incidents Tab

The PseudoWire VC Form provides details about the selected PseudoWire VC. The Incidents tab is useful for obtaining a quick summary of the incident and problem description for the PseudoWire VC.

Incidents Table

Attribute	Description
Incidents Attributes	The attributes listed in the incidents tab are same as available in NNMi Incidents form. Click the  **Open** icon to view the details of the incident. The left pane shows the basic information such as Severity, Priority, Message, and so on. The right pane shows details of the incident such as name, family and so on. For more information, see the Help for *NNMi Incidents Form.*

PseudoWire VC Form: Registration Tab

The PseudoWire VC Form provides details about the selected PseudoWire VC.

Registration Table

Attribute	Description
Create Time	Date and time the selected PseudoWire VC was created.
Last Modified	Date the selected object instance was last modified.

VPLS VPN Form

The VPLS VPN form provides details of the PseudoWires VCs participating to form a VPLS VPN.

Use the VPLS VPN form for the following tasks:

- Determine the health of the VPWS VPNs.
- Check the Incidents tab to view the cause of the change in the status.

Basic Attributes

Attribute	Description
Attributes	The attributes listed in the VPLS VPN form are available in the VPLS VPN inventory view. For more information, see VPLS VPN Inventory.

VPLS VPN Form: PseudoWire VC Tab

The VPLS VPN form provides details about the selected VPLS VPN. In addition, you can view the PseudoWires VCs participating to form a VPLS VPN.

Basic Attributes

Attribute	Description
Attributes	The attributes listed in the PseudoWire VC tab are same as available in PseudoWire VC Form. For more information, see PseudoWire VC Form.

VPLS VPN Form: PE Routers

The VPLS VPN form provides details about the selected VPLS VPN. The PE Routers tab provides the attributes of the PE routers participating in the selected VPLS VPN.

Basic Attributes

Attribute	Description
Status	The status of a PE node. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical
Name	The name of the PE router. This name is same as available from NNMi.
Device Profile	The name of the device, device type, model number, and vendor information that forms a unique profile. For more information, see *NNMi Help for Operator, Device Profile Form.*

VPLS VPN Form: Status Tab

The VPLS VPN form providesdetails about the selected VPLS VPN. You can use the Status tab to view the status summary the selected VPLS VPN.

Overall Status Table

Attribute	Description
Status	The status of the VPLS VPN is derived and calculated based on the status of all the PseudoWires VCs participating in the VPLS VPN. Possible values are: **No Status** - A VPLS VPN is newly formed and not polled, status of the L2 VPN is No Status. When all the PseudoWires VCs participating to form an L2VPN are in an unmanaged mode, the derived status of the VPN is No Status. **Normal** - The status of all the PseudoWires VCs participating to form a VPLS VPN is Normal. **Unknown** - The status of all the PseudoWires VCs participating to form a VPLS VPN is Unknown. **Warning** - The status of one or more PseudoWires VCs participating to form a VPLS VPN is Unknown. In addition, the status of none of the PseudoWire VC is Critical.

Attribute	Description
	Minor - The status of one or more PseudoWires VCs participating to form a VPLS VPN is Critical. **Critical** - The status of all the PseudoWires VCs participating in a VPLS VPN is Critical.
Last Modified	Date and time when the status was last set.

Status History

Attribute	Description
Status History	List of the last thirty status updates for the selected MPLS object. For more information, see *NNMi Status tab.*

VPLS VPN Form: Conclusions Tab

The VPLS VPN form provides details about the selected PsuedoWire VC. The Conclusions tab shows the results of the overall derived status. You can view a quick summary of the status and problem description for the selected VPLS VPN.

Conclusions Table

Attribute	Description
Status	The derived status of the selected VPLS VPN. For more information, see VPLS VPN Form: Status tab.
Time Stamp	The time when the status of the PseudoWires VC was last set.
Conclusions	The conclusions are set by the Causal Engine after the status calculation. Possible conclusions are: • **VPLSCritical** • **VPLSNormal** • **VPLSUnknown** • **VPLSMinor** • **VPLSWarning**

VPLS VPN Form: Registration Tab

The VPLS VPN form provides details about the selected VPLS VPN.

Registration Table

Attribute	Description
Create Time	Date and time the selected VPLS VPN was created.
Status Last Modified	Date and time the selected VPLS VPN was last set.

VPWS VPN Form

The VPWS VPN form provides details the PseudoWire VCs participating in the selected VPWS VPN.

Use the VPLS VPN form to complete the following tasks:

- Determine the health of the VPLS VPNs.
- Check the Incidents tab to view the cause of the change in the status.
- Navigate to the tabs associated with the VPWS VPN.

Basic Attributes

Attribute	Description
Attributes	The attributes listed in the VPWS VPN form are same and available in the VPWS VPN inventory view. For more information, see VPWS VPN Inventory.

VPWS VPN Form: PseudoWire VC Tab

The VPWS VPN form provides details about the selected VPWS VPN. The PseudoWire VC tab lists the details of the PseudoWires VCs participating to form a VPWS VPN.

Basic Attributes

Attribute	Description
Attributes	The attributes listed in the PseudoWire VC tab are same as available in PseudoWire VC Form. For more information about the attributes, see PseudoWire VC Form.

VPWS VPN Form: VC ID Tab

The VPWS VPN form provides details about the selected VPWS VPN. The VC ID tab provides details of the VC IDs participating to form a VPWS VPN.

Basic Attributes

Attribute	Description
ID	The list of VC Ids participating to form a VPWS VPN.

VPWS VPN Form: PE Routers Tab

The VPWS VPN form provides details about the selected VPWS VPN. The PE Routers tab provides the attributes of the PE routers participating in the selected VPWS VPN.

Basic Attributes

Attribute	Description
Status	The status of a PE node. Possible values are:  No Status

Attribute	Description
	Normal Disabled Unknown Warning Minor Major Critical
Name	The name of the PE router.
Device Profile	The name of the device, device type, model number, and vendor information that is assigned to the router to form a unique profile. For more information, see *NNMi Help for Operator, Device Profile Form.*

VPWS VPN Form: Status Tab

The VPWS VPN form provides details about the selected VPWS VPN. You can use the Status tab to view the status summary the selected VPWS VPN.

Overall Status Table

Attribute	Description
Status	The status of an L2VPN is derived and calculated based on the status of all the PseudoWire VCs that participates to form the VPWS VPN. Possible values are: **No Status** - A VPWS VPN is newly formed and not polled, status of the L2VPN is No Status. In addition, when all the PseudoWires VCs participating to form an L2VPN are in an unmanaged mode, the derived status of the VPWS VPN is No Status. **Normal** - The status of all the PseudoWires VCs participating to form a VPWS VPN is Normal. **Unknown** - The status of all the PseudoWires VCs participating to form a VPWS VPN is Unknown. **Warning** - The status of one or more PseudoWires VCs participating to form a VPLS VPN is Unknown. In addition, the status of none of the PseudoWire VC is Critical. **Minor** - The status of one or more PseudoWires VCs participating to form a VPWS VPN is Critical. **Critical** - The status of all the PseudoWires VCs participating to form a VPWS VPN is Critical.
Last Modified	Date and time when the status was last set.

Status History

Attribute	Description
Status History	List of last thirty status updates for the selected MPLS object. For more information, see *NNMi Status tab*.

L3 VPN Form: Conclusions Tab

The VPN Form contains details about the all the VRFs participating in the VPN. The Conclusions tab shows the results of the overall derived status. You can view a quick summary of the status and problem description for the selected L3 VPN.

Conclusions Table

Attribute	Description
Status	The derived status of the selected L3 VPN. For more information, see VPN Form: Status tab.
Time Stamp	Current status is calculated and set by Causal Engine. The Time Stamp data is the time when the status of the VPN is calculated and last updated in the view.
Conclusions	The conclusions are set by the Causal Engine after the status calculation. Possible conclusions are: • **VPNCritical** • **VPNNormal** • **VPNUnknown** • **VPNMinor** • **VPNWarning** • **VPNHubVRFUp**

VPWS VPN Form: Registration Tab

The VPWS VPN provides details about the selected VPWS VPN.

Registration Table

Attribute	Description
Create Time	Date and time the selected VPWS VPN was created.
Status Last Modified	Date and time he selected VPWS VPN was last modified.

TE Tunnel Form

The TE Tunnel form provides details about the selected TE tunnel. The TE Tunnel form shows the tunnel properties and attributes.

Use the TE Tunnel form for the following tasks:

- Monitor the TE Tunnels in the network.
- Check the Incidents tab to view the cause of the change in the status.
- Navigate to the Hops tab to check all the intermediate routers available in the TE Tunnel.
- Access the TE Tunnel Path view.

Basic Attributes

Attribute	Description
Name, Head, Tail, Tail IP Address, Description, Status, and Bandwidth	The attributes listed in the TE Form are same as available in the TE Tunnel Inventory. For more information, see TE Tunnel Inventory.
Management Mode	Used to indicate whether the current node is being managed. This field also lets you specify whether a node is temporarily out of service. The iSPI for MPLS shows the same values as NNMi. Possible values are: **Managed** – The node, interface, or address is managed by NNMi. **Not Managed** – The node is intentionally not managed. For example, the node might not be accessible because it is in a private network. NNMi does not update discovery information or monitor these nodes. **Out of Service** – A node is unavailable because it is out of service. NNMi does not update discovery information or monitor these nodes. This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed. For more information, see Help for NNMi, *View the Management Mode for an Object in Your Network.*
Head Interface	The interface of the head node where the selected TE Tunnel is configured. To view the Head interface details, click the LookUp icon.
Setup Priority	The priority used to determine if the selected TE Tunnel is eligible to be preempted. The value specifies the priority used when you are setting up the tunnel. A value of 0 shows the highest priority and enables the tunnel to preempt all other tunnels except those with a holding priority of 0. A value of 7 shows the lowest priority and does not enable a new tunnel to preempt any existing tunnel.
Hold Priority	The holding priority value specifies the priority used when protecting the tunnel from preemption by other tunnels. A value of 0 shows the highest priority and protects this tunnel from preemption by all other tunnels. A value of 7 shows the lowest priority and allows all tunnels with a higher priority to preempt this tunnel.
Create Time	The time when the TE tunnel was created.
Status Last Modified	The status of the TE tunnel is calculated whenever there is a change in topology. The Status Last Modified is the time when the status was last updated.

For more information, see Attributes Tab, Hops Tab, Status Tab, Conclusions Tab, Incidents Tab, and Registration Tab.

TE Tunnel Form: Attributes Tab

The TE Tunnel Form provides details about the selected TE Tunnel. The Attributes tab provides the TE Tunnel details listing the capabilities for Cisco and Juniper routers. The listed attributes are available from the Cisco and Juniper MIBs.

Supported Table for Cisco Nodes

Attribute	Description
record Route	If the tunnel is configured with the recordRoute attribute, the value is true. True is represented by ☑
fastReroute	If the tunnel is configured with the fastReroute attribute, the value is true. True is represented by ☑.
mergingPermitted	If the tunnel is configured with the MergingPermitted attribute, the value is true. True is represented by ☑.
isPersistent	If the tunnel is configured with the isPersistent attribute, the value is true.True is represented by ☑.
isPinned	If the tunnel is configured with the isPinned attribute, the value is true. True is represented by ☑.
isComputed	If the tunnel is configured with the isComputed attribute, the value is true. The status of the flag is either true or false. True is represented by ☑.

Supported Table for Juniper Nodes

Attribute	Description
record-route	If the tunnel is configured with the record-route attribute, the value is true. The status of the flag is either true or false. True is represented by ☑.
fast-reroute	If the tunnel is configured with the fast-reroute attribute, the value is true otherwise it is false. This is valid for both Cisco and Juniper routers. True is represented by ☑.
mergeable	If the tunnel is configured with the mergeable attribute, the value is true. The status of the flag is either true or false. True is represented by ☑.
preemptable	If the tunnel is configured with the preemptable attribute, the value is true. The status of the flag is either true or false. True is represented by ☑.
preemptive	If the tunnel is configured with the preemptive attribute, the value is true. The status of the flag is either true or false. True is represented by ☑.
cspf	If the tunnel is configured with the cspf attribute, the value is true. The status of the flag is either true or false. True is represented by ☑.
adaptive	If the tunnel is configured with the adaptive attribute, the value is true. The status of the flag is either true or false. True is represented by ☑.

TE Tunnel Form: Hops Tab

The TE Tunnel Form provides details about the selected TE Tunnel.

The Hops tab provides details of the intermediate routers of the selected tunnel. The hop is an inter-mediate router in the tunnel path. The hop details are available only when the TE Tunnel is managed and status is Normal, Minor, Major, or Warning. When the status of the head router from where the TE Tunnel starts is Unknown or Critical, the hop details of the selected TE Tunnel are not available. The hop details are updated in every 5 minutes.

Basic Attributes

Attribute	Description
Hops #	The sequential number assigned to the segment of the tunnel. The segment of the tunnel is a part that connects two consecutive routers. For example, the hop is a part between the head router and the next intermediate router, or the intermediate router and the destination router. Each hop number represents each row in the form.
From-Node	The name of a node. The name is a fully-qualified hostname or an IP address. The segment of the hop starts from this node.
Outgoing-IfName	The name of an interface on the node. The segment of the hop starts from this interface. Possible values are: • **No Data Available** - Whenever an interface is not managed by NNMi or the MIB value is unknown or the interface is not discovered by NNMi, the value is No Data Available. • **Virtual Interface** - Whenever an interface on the head node is not discovered, the value is Virtual Interface. This value is applicable only for the Cisco devices. Click the **Open** icon to view details about the selected Outgoing-IfName.
Outgoing-IfAddress	The IP address of an interface on the node. The segment of the hop starts from this interface.
To-Node	The name of a node. The name is a fully-qualified hostname or an IP address. The segment of the hop terminates at this node. Whenever the MIB reports the value as unknown or the node is not discovered by NNMi, the value is **Unknown**.
Incoming-IfName	The name of interface on the node. The segment of the hop terminates at this interface. When the MIB value is unknown or the interface is not discovered by NNMi, the value is **Unknown**.
Incoming-IfAddress	The IP address of interface on the node. The segment of the hop terminates at this interface. Whenever the MIB value is unknown or the interface is not discovered by NNMi, the value is **Unknown**.

TE Tunnel Form: Status Tab

The TE Tunnel Form provides details about the selected TE Tunnel. You can use the Status tab to view the status summary the selected TE Tunnel.

Status Table

Attribute	Description
Status	Overall status of the TE Tunnel. Possible values are : **Normal** - If the status of the TE Tunnel is Up, the status of the TE Tunnel is Normal. **Critical** - If the status of the TE Tunnel is Down, the status of the TE Tunnel is Critical.

Attribute	Description
	Unknown - If there is no SNMP response for the selected node and the selected TE Tunnel is configured on this node, the status of the TE Tunnel is Unknown.
Last Modified	Date and time when status was last set.

Status History

Attribute	Description
Status History	List of the last thirty status updates for the selected MPLS object. For more information, see *NNMi Status tab*.

TE Tunnel Form: Conclusions Tab

The TE Tunnel Form provides details about the selected TE Tunnel. The Conclusions tab shows the results of the overall derived status. You can view a quick summary of the status and problem description for the selected TE Tunnel.

Basic Attributes

Attribute	Description
Status	Overall status of the TE Tunnel. For information about the possible status values, see TE Tunnel: Status Tab.
Time Stamp	The time when the status of the TE tunnel is last updated.
Conclusions	The conclusions are set by the Causal Engine after the status calculation. Possible conclusions are: • **MplsTunnelDown** • **MplsTunnelUp** • **MplsTunnelUnknown**

TE Tunnel Form: Incidents Tab

The TE Tunnel Form provides details about the selected TE Tunnel. The Incidents tab is useful for obtaining a quick summary of the problem description of the selected TE Tunnel.

Incidents Table

Attributes	Description
Incidents Attributes	The attributes listed in the incidents tab are same as available in NNMi Incidents form. Click the **Open** icon to view the details of the incident . The left pane shows the basic information such as Severity, Priority, Message, and so on. The right pane shows details of the incident such as name, family and so on. For more information, see Viewing MPLS Incidents.

TE Tunnel Form: Registration Tab

The TE Tunnel Form provides details about the selected TE Tunnel.

Registration Table

Attributes	Description
Create Time	Date and time the selected TE Tunnel was created.
Last Modified	Date the selected TE Tunnel was last modified.

VC LSP Form (Virtual Circuit Label Switching Path Form)

The VC LSP form provides details about the selected VC LSP.

Basic Attributes

Attribute	Description
PseudoWire VC ID	The unique index identifier for each virtual circuit.
PSN Type	The kind of Packet Switched Network (PSN) for the selected VC LSP.
Source	The name of a node. The selected PseudoWire VC starts from this node. Click the **Lookup** icon to view more information about the source node.
Source Address	The IP Address of the source node. The source node is one of the endpoints of the PseudoWire VC.
Destination	The name of a node. The selected PseudoWire VC terminates at this node. Click the **Lookup** icon to view more information about the node.
Destination Address	The IP Address of the destination node.
Status	The status of the PseudoWire VC. Possible values are: **Normal** - The status of both the LSPs is Normal. **Critical** - The status of any one or both the LSPs is Critical. **Unknown** - The status of any one or both the LSPs is Unknown.
Attachment Circuit (AC) Name	The name of the attachment circuit or the data link of the selected VC LSP.
AC Description	Additional information about the selected AC.
Encapsulation Type	The kind of service carried in the selected PseudoWire VC. For example, the services are ATM, Frame Relay, or Ethernet. If both the endpoints (PE1 and PE2) are discovered but the status of the LSPs is not Normal, the value of Encapsulation Type is **Others**.
Management Mode	The current node is managed by NNMi. In addition, this field specifies whether a node is temporarily out of service or managed or not managed by NNMi. Possible values are: **Managed** – The node, interface or address is managed by NNMi. **Not Managed** – The node is not managed by NNMi. For example, the node might not be accessible because it is in a private network. NNMi does not update discovery information or monitor these nodes. **Out of Service** – A node is unavailable because it is out of service. NNMi does not update discovery information or monitor these nodes. This node is not discovered by the iSPI for MPLS. This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed. For more information, see the Help for NNMi, *View the Management Mode for an Object in Your Network.*
Create Time	Date and time the selected VC LSP was created.
Status Last Modified	Date and time the selected VC LSP was last modified.

VC LSP Form: Status Tab

The VC LSP Form provides details about the selected VC LSP. You can use the Status tab to view the status summary the selected VC LSP.

Overall Status

Attribute	Description
Status	The status of the VC LSP. Possible values are:  **Normal**  **Critical**  **Unknown**
Last Modified	Date and time when status was last set.

Status History

Attribute	Description
Status History	List of the last thirty status updates for the selected VC LSP. For more information, see *NNMi Status tab*.

VC LSP Form: Conclusions Tab

The VC LSP Form provides details about the selected VC LSP. The Conclusions tab shows the results of the overall derived status. You can view a quick summary of the status and problem description for the selected VC LSP.

Conclusions Table

Attribute	Description
Status	The status of the VC LSP. For information on how the current status is determined, see the VC LSP Form: Status Tab.
Time Stamp	Current status is set by Causal Engine. The Time Stamp data is the time when the status of the PseudoWire VC is last updated.
Conclusion	The conclusions are set by the Causal Engine after the status calculation. Possible conclusions are: • **MplsVCLSPUp** • **MplsVCLSPDown** • **MplsVCLSPUnknown** The VC LSP down conclusion generates the PseudoWire VC incident to send the alert for the status. For example, MplsVCLSPDown generates the MplsPseudoWireVCDown incident.

VC LSP Form: Registration Tab

The VC LSP Form provides details about the selected VC LSP.

Registration Table

Attribute	Description
Create Time	Date and time the selected MPLS object instance was created.
Last Modified	Date the selected VC LSP was last modified.

Node Form: VRF Tab

The NNMi Node form provides details about the selected node. In addition, the form provides details of the VRF-enabled interfaces participating to form an L3 VPN.

Basic Attributes

Attribute	Description
VRF	Table view of all the VRFs associated with the current node. Use this table to determine all VRFs in which this node participates. For more information, see VRF Form.

Node Form: TE Tunnel Tab

The NNMi Node form provides details about the selected node. In addition, the form provides details about the available TE Tunnels associated with the selected node.

Basic Attributes

Attribute	Description
TE Tunnel	Table view of all of the TE Tunnels associated with the current node. Use this table to determine all TE tunnels in which this node participates. For more details, see TE Tunnel Form.

Node Form: PseudoWire VC LSP Tab

The Node form provides details about the selected node. In addition, the form provides details about the available PseudoWire VCs associated with the selected node.

Basic Attributes

Attribute	Description
PseudoWire VC LSP	Table view of all of the PseudoWire VC LSPs starting from the current node. Use this table to determine all the PseudoWire VCs configured in the selected node. For more information, see PseudoWire VC Form.

Node Form: VPLS VPNs Tab

The Node form provides details about the selected node. In addition, the form provides details about the available VPLS VPNs associated with the selected node.

Basic Attributes

Attribute	Description
VPLS VPN	Table view of the available VPLS VPNs for the selected node. For more information, see VPLS VPN view.

.

Node Form: VPWS VPNs Tab

The NNMi Node form provides details about the selected node. In addition, the form provides details about the available VPWS VPNs associated with the selected node.

Basic Attributes

Attribute	Description
VPWS VPN	Table view of the available VPWS VPNs for the selected node. For more information, see VPWS VPN view.

.

Node Form: L3 VPN PE Interfaces Tab

The NNMi Node form provides details about the selected node. The L3 VPN PE Interfaces tab provides details of the PE interfaces on the selected node.

Basic Attributes

Attribute	Description
St, IfName, IfAlias, IfType	The attributes listed in the CE Interface tab are same as available in NNMi Interface form. For more information for the attributes, see the Help for *NNMi Interface Form.*
VRF Name	The name is obtained from the PE router during the iSPI for MPLS discovery.
VPN Name	The subsystem generated name. You can update the system generated VPN Name from the forms. For more details, see L3 VPN Form.

To view the PE interfaces participating in the L3VPN, follow the steps:

1. From NNMi Workspace and click **Inventory-> Nodes view**.
2. Click the  Open icon to view the detailed information about a MPLS node. The Node form opens.
3. Click the **L3 VPN PE Interfaces** tab to view the details of the PE interface**.**)

PE Interface Form: L3 VPN Tab

The NNMi Interfaces form provides details about the selected node. The selected interface is a PE interface.

The L3 VPN tab provides details of all the CE interfaces associated with the selected PE interface. This tab provides summarized details of the current PE interface participating in an L3VPN.

L3VPN Attributes

Attribute	Description
L3 VPN Name	The subsystem-generated L3 VPN name. You can update the system generated VPN Name from the forms. For more details, see VPN Form.
VRF Name	The name of a VRF.

L3VPN CE Attributes

Attribute	Description
Status, IfName, IfAlias, IfType	The attributes listed in the CE Interface tab are same as available in the NNMi Interface form. For more information about attributes, see the Help for *NNMi Interface Form*.
CENode	The name of the CE node where the CE interface is configured.

To start the PE Interface Form: L3 VPN Tab, follow the steps:

(1. From MPLS Workspace and click **MPLS- > MPLS L3VPN view**).

2. Click the Open icon to view the detailed information about a VPN. The VPN form opens and shows the information specific to the VRFs associated with a selected VPN.

3. From the VPN form, click the **Open** icon to view the detailed information about a VRF. The VRF form opens.

4. From the VRF form, select **PE Interfaces** tab to view the details of a PE interface and click **L3 VPN** tab to view all the CE interfaces associated with the selected PE interface.)

CE Interface Form: L3 VPN Tab

The NNMi Interfaces form contains details about the selected node. The selected interface is the CE interface.

The L3 VPN tab provides details about all the PE interfaces associated with the selected CE interface. This tab provides summarized details of the current CE interface participating in VRF and VPN.

L3 VPN Attributes

Attribute	Description
L3 VPN Name	The system-generated L3 VPN name. You can update the system-generated VPN Name from the L3 VPN form. For more information, see L3 VPN Form.
VRF Name	The name of selected VRF.

L3 VPN PE Attributes

Attribute	Description
Status, IfName, IfAlias, IfType	The attributes listed in the PE Interface tab are same as available in the NNMi Interface form. For more information about the attributes, see the Help for *NNMi Interface Form.*
PE Node	The name of the PE node where the PE interface is configured.

Launching the CE Interface Form: L3 VPN Tab

To launch the CE Interface Form: L3 VPN Tab, follow these steps:

(1. From MPLS Workspace and click **MPLS-> MPLS L3 VPN view**).

2. Click the **Open** icon to view the detailed information about a VPN. The VPN form opens and displays the information specific to the VRFs associated with a selected VPN.

3. From the VPN form, click the Open icon to view the detailed information about a VRF. The VRF form opens.

4. Select **CE Interfaces** tab to view the details of the CE interface and click **L3 VPN** tab to view all the PE interfaces associated with the selected CE interface.)

Monitoring Your Network by using the iSPI for MPLS Global Network Manager

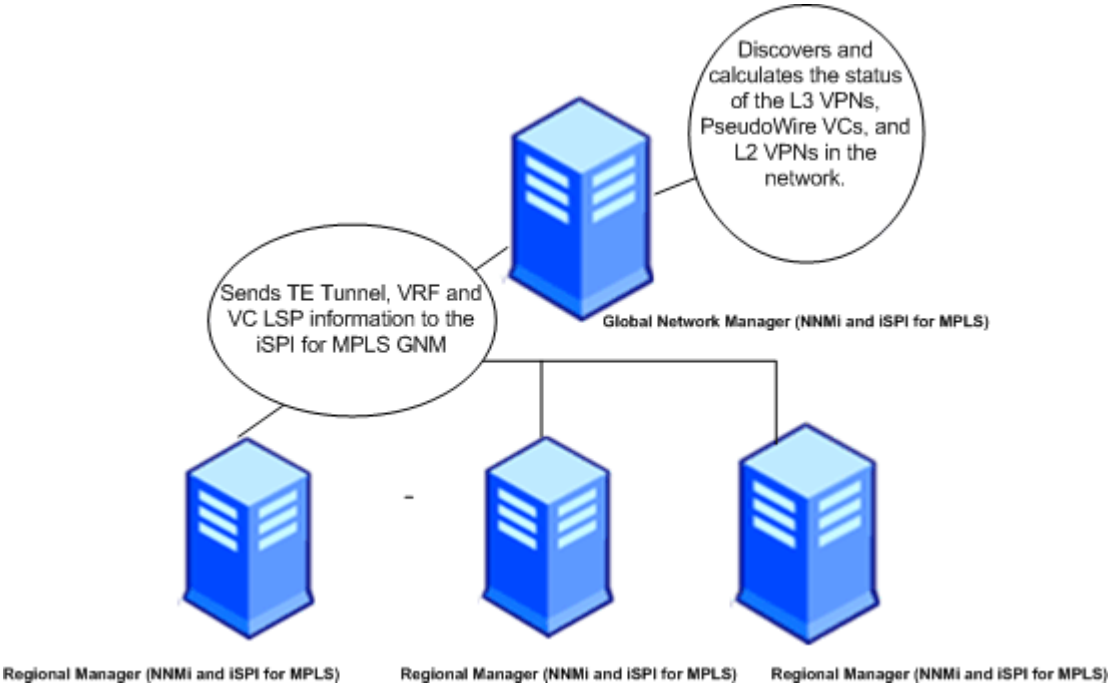
The iSPI for MPLS uses the capabilities of NNMi Global Network Manager (NNMi GNM) and provides a centralized view to monitor the multiple sites. You can configure the Regional Manager connections by using the **MPLS Configuration** workspace. After the connection is established, view and monitor the MPLS-enabled nodes, interfaces, MPLS objects from the iSPI for MPLS inventory.

Use the iSPI for MPLS view (GNM) for the following tasks:

- Monitor the MPLS-enabled routers in the network.
- View the problem MPLS objects such as VRFs, TE Tunnels, and VC LSP in the network. Check the status of the MPLS objects.
- Access the MPLS forms to check the other attributes of the MPLS object.
- Access the map views of the network.
- Access the available MPLS reports.

The iSPI for MPLS Regional Manager monitors and sends the topology update and status information of the MPLS objects such as VRFs, TE Tunnels, and VC LSPs in the network to the iSPI for MPLS (GNM).

Click here to know about the iSPI for MPLS GNM and Regional Manager.



The Regional Manager sends the updated information according to the polling interval set for the MPLS objects at the regional level. The iSPI for MPLS GNM uses the consolidated information of the VRFs and VC LSPs to discover, regroup, and compute the status of the L3 VPNs, PseudoWire VCs, and L2 VPNs in the network.

Use the iSPI for MPLS inventory (GNM) for the following tasks:

- Monitor the L3 VPN topology. Uses the VRFs information from the Regional managers to regroup and form the L3 VPNs. Calculates and derives the status of the available L3 VPNs in the network.
- Monitor the consolidated PE-CE link connectivity in the L3 VPN topology. Make sure that both the PE and CE nodes and interfaces are discovered in a Regional Manager. If the PE node is discovered in one Regional Manager and CE node in another Regional Manager, the consolidated PE-CE connection does not appear in the MPLS inventory (GNM).
- Monitor the L2 VPN topology. Uses the VC LSPs information from the Regional managers to regroup and form the L2 VPNs. Calculates and derives the status of the available L2 VPNs in the network.
- Monitor the MVPN topology. Uses the MVRFs information to regroup and form the MVPNs. Calculates and derives the status of the available MVPNs in the network.
- Monitor the Pseudowire VCs in the network. Uses the VC LSPs information from the Regional managers to regroup and form the L2 VPNs. Calculates and derives the status of the available L2 VPNs in the network.
- Monitor and generate the MPLS reports from the MPLS inventory (GNM). The MPLS LSR Node and Interface report are only available for the MPLS-enabled nodes that are seeded locally in the iSPI for MPLS (GNM). The L3VPN_VRF report is available for the local nodes of the Regional Manager that appears in the iSPI for MPLS inventory (GNM) and also for the nodes seeded locally in the iSPI for MPLS (GNM).

The iSPI for MPLS inventory (GNM) gets updated according to the polling interval set for the MPLS objects in the Regional Manager inventory. If the polling interval for the MPLS nodes in the Regional Manager is 10 minutes, the MPLS nodes in the iSPI for MPLS inventory (Global Network Manager) get updated in every 10 minutes.

Use the **MPLS Configuration** workspace to configure the polling interval, Route Targets, and VPWS VPNs again from the iSPI for MPLS GNM. The configuration settings are limited to a local Regional Manager and do not get transferred to the iSPI for MPLS GNM.

To verify that the Regional Manager connection is working *see NNMi Help, Determine the State of the Connection to a Regional Manager.*

Related Topics:

Configure the Regional Manager Connections

MPLS Processes and Services

After you install iSPI for MPLS, the following processes are running on the server.

Process Name	Description
mplsjboss	The process that controls the jboss Application Server that contains all of the MPLS Services.
nmsdbmgr	Postgress Database

The iSPI for MPLS do not show the status of Oracle database.

You can stop and start the iSPI for MPLS processes from the start and stop commands.

Start and Stop the MPLS Process

- To start the MPLS processes, type: **ovstart –c mplsjboss.** This command starts the MPLS processes and checks whether the NNMi processes (ovjboss, nmsdbmgr) are running or not.
- To stop the MPLS processes, type: **ovstop - c mplsjboss.** This command stops the MPLS processes and not the NNMi processes (ovjboss, nmsdbmgr).

To verify that all NNMi and MPLS processes are running, do the following at the command line:

- For the basic status, type: **ovstatus –c mplsjboss**
- For the detailed status, type: **ovstatus -v mplsjboss**

Verify that MPLS Services are Running

After you install MPLS, a group of services are running on the server. MPLS services run inside the mplsjboss process. The mplsjboss process controls the jboss application server that contains all the MPLS services.

To verify that all MPLS services are running, type one of the following:

- For the basic information, at the command line, type **ovstatus -c mplsjboss**
- For the detailed information, at the command line, type **ovstatus -v mplsjboss**

Log files for the MPLS Services

Log files are found in the following location:

- UNIX: `$OVINSTALLDIR/log/mpls`
- Windows: `%OVINSTALLDIR%\log\mpls`

Discovering Your Network

You can monitor the MPLS nodes and objects from the MPLS inventory after you complete the MPLS discovery process.

You can discover the MPLS nodes and objects by the following:

- Install NNMi and then install the iSPI for MPLS to monitor the network. The nodes are added after installing NNMi and the iSPI for MPLS.
- Install the iSPI for MPLS on an NNMi management server that is already managing the network.

After you install NNMi and iSPI for MPLS, seed the nodes from the NNMi console. The NNMi discovery process starts and discovers the nodes in the network. The iSPI for MPLS discovery process starts automatically after the completion of NNMi discovery process. Use the command to start the complete MPLS discovery. When you add an MPLS node in the topology, NNMi discovery process detects the change in network and sends a notification to the iSPI for MPLS discovery process to start. Similarly, when you delete a node, NNMi discovery process detects the interfaces residing on the node and deletes the corresponding dependencies for the deleted node in all the views. By default, the discovery schedule for NNMi and iSPI for MPLS is set to 24 hours.

After installing the iSPI for MPLS on an NNMi management server, you can wait for the next discovery cycle of NNMi, or you can perform the **Configuration Poll** to discover the MPLS nodes immediately. The iSPI for MPLS discovery process does not discover the nodes that are already discovered by NNMi.

To start the complete discovery for the iSPI for MPLS, use `nmsmplsdisco.ovpl -all`. For more information, see MPLS reference pages (*Help -> NNMi iSPI Documentation Libraray -> iSPI for MPLS Reference Pages)*.

Duplicate IP Address Support with the iSPI for MPLS

You can monitor the PE-CE link connectivity in the network by using the MPLS inventory.

The iSPI for MPLS discovers the PE-CE connections correctly in a duplicate IP address environment in the following conditions:

- Protocols used are BGP, OSPF, RIP, EIGRP, or Static routes for PE-CE connection.
- When the duplicate IP addresses appear for the MPLS-enabled nodes participating in the L3 VPN topology.
- When the duplicate IP addresses appear at the subnet level.
- When the duplicate IP address appear for the L2 connections that are CDP-enabled.

- When the duplicate IP address appear for the PE interface that is a VLAN interface.
- When the duplicate IP address appear for Ethernet or Point to Point media.

The iSPI for MPLS does not support the following conditions:

- An IP address used by the CE node that is not manageable (no SNMP response) by NNMi. But, the IP address of these CE nodes match the subnet address, thereby the CE nodes still appear in multiple L3 VPNs.
- If Ethernet is used for PE-CE communication and for a long duration there is no data transfer then ARP Cache does not contain any data and times out. If the iSPI for MPLS discovery process starts when ARP Cache is down, no information is found for the PE-CE communication. In this case, the iSPI for MPLS does not resolve the duplicate IP address.

Viewing the Network Connectivity

With the iSPI for MPLS, you can view the complete connectivity of the network by using the map views.

The iSPI for MPLS presents three additional map views that help you visualize your topology to view the network connectivity. You can access the map views from the **Actions** menu. The iSPI for MPLS includes the following map views:

- MPLS Path View
- MPLS TE Tunnel Path View
- MPLS L3 VPN Topology View

Use the map views for the following:

- Monitor the MPLS-enabled nodes and MPLS objects (VRFs and TE Tunnels). Navigate to the node and interface inventory from the map views.
- Monitor the PE-CE nodes and interfaces participating to form an L3VPN. Check the MPLS L3 VPN Topology Map view.
- Monitor the Label Switched Path (LSP) path between the two LSR nodes. Check the MPLS Path view.
- Monitor the path between the two TE tunnels. Check the MPLS TE Tunnel Path view.
- Troubleshoot and investigate the status change and loss of connectivity of the MPLS nodes or interfaces.

Related Topics:

Actions Available in the iSPI for MPLS

MPLS Path View

The MPLS Path view shows the Label Switched Path (LSP) between the two LSR nodes. View the states and status of Provider Edge (PE) and Provider nodes participating in the LSR path in the MPLS cloud.

You can view the most accurate MPLS path known as the best effort path only for Cisco nodes. The iSPI for MPLS supports only OSPF[1] protocols for the path calculation. When the iSPI for MPLS is integrated with RAMS, you can view the complete path. For more information, see NNMi Help.

Use this view to perform the following tasks:

- Find the MPLS Label Switched Path (LSP) between two LSR nodes.
- Troubleshoot the connectivity problems in the path view.

To launch an MPLS Path view from the MPLS LSR view, follow these steps:

1. From the **Workspaces** navigation pane, click **MPLS-> MPLS LSR view**. The **MPLS LSR View** opens in the right pane.
2. In the **MPLS LSR** view, click the ☑ selection box representing the LSR node as the starting-point in the path. Similarly, select another LSR node as the destination-point to view the path between these nodes.
3. From the menu bar, select **Actions-> MPLS Path View.** The **MPLS Path View** opens.
4. Click the **Status Refresh** icon to update the status of the MPLS objects. Click the **Refresh** icon to update the map view.

The map view contains the following information:

- Node name and status
- Interface name and status
- Quick View
- Last update time and date

For more information about the node symbols, icons, and status color, see *NNMi Map Symbols*.

Troubleshooting the network connectivity from the MPLS Path View, follow these steps:

1. Navigate to the **MPLS Path View**.
2. To open the node or interface, use any one of the following: Double-click the node or interface which is down.
3. Select the node, click the **Open** icon.
4. Navigate to the Incidents tab to view the incident and troubleshoot the cause of loss of network connectivity.

Related Topics:

MPLS Map Symbols.

[1]Open Shortest Path First

TE Tunnel Path Map View

The MPLS TE Tunnel Path View shows an active network path between a source and destination end point that forms a TE Tunnel. The map view shows the head router, tail router, intermediate routers, direction of the flow, and status of the nodes and interfaces participating in the TE Tunnel. The TE Tunnel map views shows both the Cisco or Juniper routers configured with TE Tunnel. The TE Tunnel path is the dynamic traffic flow path where the hops are updated in every 5 minutes.

On the TE Tunnel maps, the nodes and interfaces are represented as symbols on the map. The lines between nodes indicate the connections. For each status color for a node, interface, or IP address that might appear on a map, see *NNMi Help, Understand Maps*.

Use the map view to perform the following tasks:

- Find and view the nodes and interfaces participating to form a TE tunnel path.
- Determine and troubleshoot the root cause of the interface or node status by Quick View.
- Determine the head, tail and intermediate routers of the TE Tunnel.

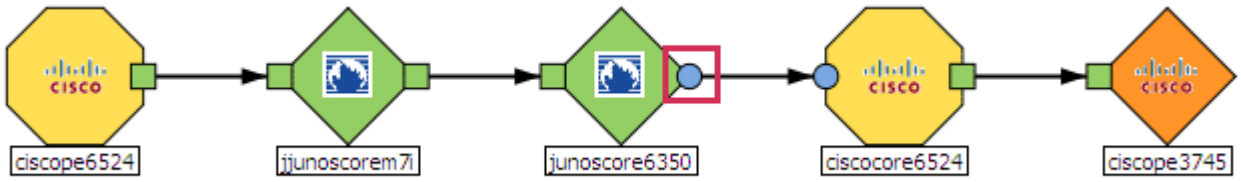
To launch a TE Tunnel Path view, follow these steps:

1. From the **Workspaces** navigation pane, click **MPLS-> TE Tunnel Inventory**. The MPLS TE Tunnel view opens in the right pane.
2. In the **TE Tunnel Inventory**, click the selection box to select a row representing the TE Tunnel.
3. From the menu bar, select **Actions-> MPLS TE Tunnel Path view**. The TE Tunnel graph opens in a new window.
4. Click the **Status Refresh** icon to update the status of the MPLS objects. Click the **Refresh** icon to update the map view.

To launch a TE Tunnel Path view from the TE Tunnel Form view, follow these steps:

1. From the **Workspaces** navigation pane, click **MPLS-> TE Tunnel Inventory**. The MPLS TE Tunnel view opens in the right pane.
2. To open the TE Tunnel form, click the **Open** icon.
3. From the menu bar, select **Actions-> MPLS TE Tunnel Path View**. The TE Tunnel graph opens in a new window.

Example of the TE Tunnel Path Map View:



In this example, the TE Tunnel starts from the head node *ciscope6524* to the tail node ciscope3745. The intermediate routers are Juniper and Cisco routers. Double-click the node to open the node form. Click the square boxes attached to the node to open the interface form. The marked outgoing interface of the junoscore6350 is Unknown. Alternatively, you can view the interface details from the Quick View window. For more information about the node symbols, icons, and status color, see MPLS Map Symbols.

Troubleshooting the network connectivity from the TE Tunnel Path View, follow these steps:

1. Navigate to the **MPLS TE Tunnel Path view**.
2. To open the node or interface, use any *one* of the following:
   - Double-click the node or interface whose status is Critical.
   - Select the node, click the **Open** icon.
3. From the TE Tunnel form, click the **Incidents** tab to view the incident.

Related Topics:

MPLS Map Symbols.

MPLS L3 VPN Topology Map view

You can troubleshoot the faults associated in your L3VPN topology by using the MPLS L3 VPN map view. This map view is a service-centric map view. You can monitor the status of the CE nodes, interfaces, VRFs, and PE nodes participating to form an L3 VPN.

In an MPLS L3 VPN topology map view, VRFs, VPNs, CE nodes, and PE nodes are represented as symbols on the map. The lines between the MPLS objects such as VRFs indicate the communication connections. For each status color for a VRF, interface, or IP address that might appear on a map, see MPLS Map Symbols and NNMi Help, *Maps Symbols.*

Use this view to perform the following tasks:

- Find the VRFs participating to form an L3 VPN.
- Find the CE nodes and interfaces in the L3 VPN. For more information, see L3 VPN Map Toolbar.
- Find out the PE-CE link connectivity for the selected L3 VPN.
- Determine the status of the VRFs residing on the PE node connected to the CE node.
- Troubleshoot the root cause of the L3 VPN status. Navigate to the MPLS object form and view the incidents tab.
- Check the status of all the VRFs that participates to form an L3 VPN.
- Check the status of the PE and CE interface and PE and CE node.

To launch an MPLS L3 VPN view, follow these steps:

1. From the **Workspaces** navigation pane, click **MPLS-> MPLS L3 VPN**. The MPLS L3 VPN view opens in the right pane.
2. In the **MPLS L3 VPN** view, click the selection box to select a row representing the L3 VPN.
3. Click **Actions-> MPLS L3VPN Topology View** The L3 VPN graph opens in a new window.
4. Click the **Compute Path** icon to display the map of the path. Click the **Status Refresh** icon to update the status of MPLS objects. Click the **Refresh** icon to update the map view.

The MPLS L3 VPN maps show the near real-time status of all the VRFs participating in the selected L3 VPNs. The following types of L3 VPN topologies are shown in the map view:

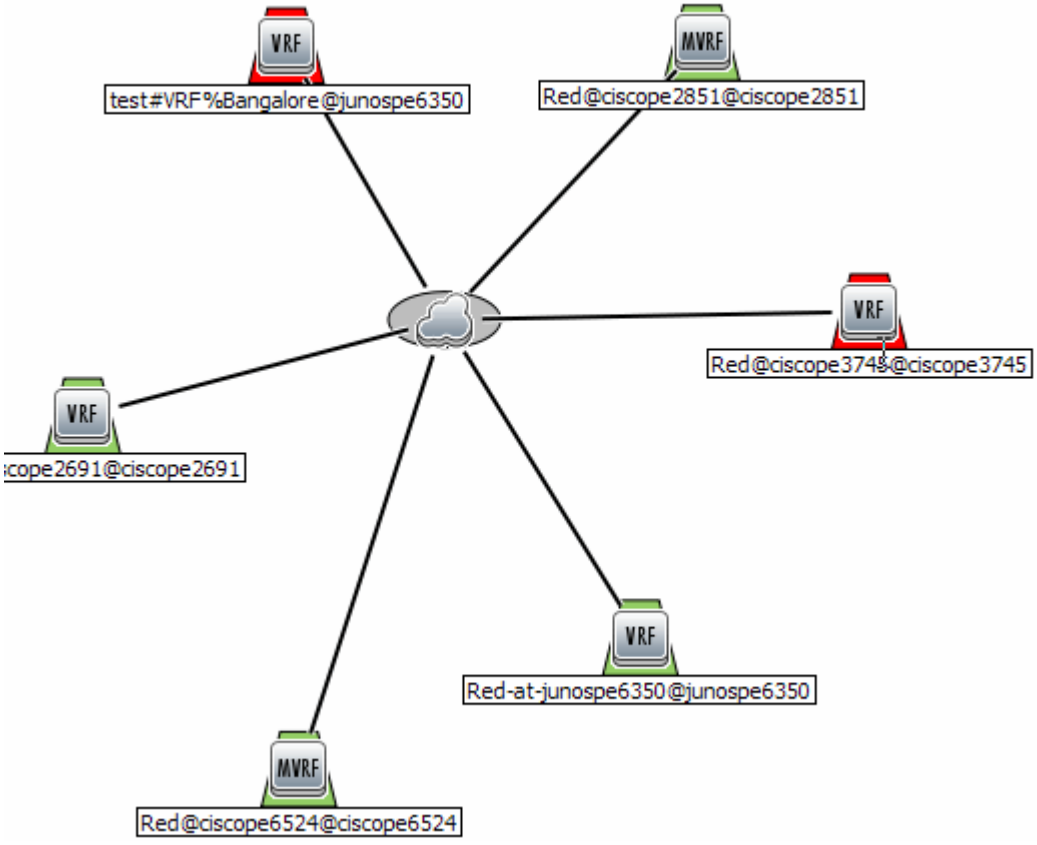
- Full-Mesh
- Other

- Isolated
- Hub and Spoke

Start the following from an MPLS L3 VPN map view:

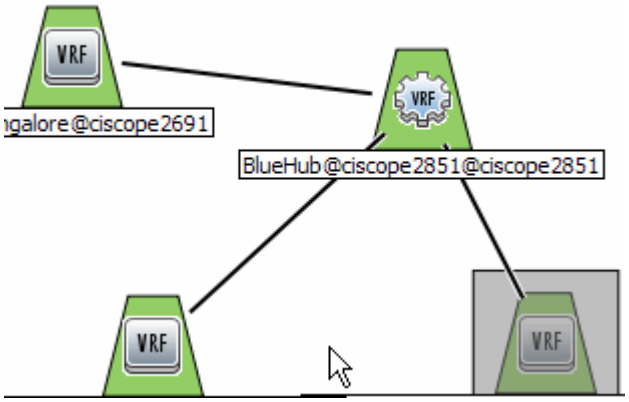
- Double - click the L3VPN or VRF icon to open the L3 VPN or VRF form. To troubleshoot the loss of connectivity, check the status or incidents associated with the selected VPN or the VRFs participating to form an L3VPN.
- Double - click the CE node to open the CE node form.
- Double - click the CE interface to open the CE interface form.
- Show all the CE nodes in the selected L3 VPN topology.
- Show all the CE nodes for the selected VRF.
- Find the type of PE-CE link connectivity in the network.

Examples of the MPLS L3 VPN map view



This is an example of a Full Mesh L3 VPN.

Double-click the VRF or VPN icon to open the VRF or L3VPN form.



This is an example of a Hub and Spoke L3 VPN. All the VRFs are communicating with the Hub VRF.

Double-click the Hub VRF icon to open the Hub VRF form.

This is an example of a Full Mesh L3 VPN.

Troubleshooting the network connectivity from the MPLS L3 VPN View, follow these steps:

1. Navigate to the **MPLS L3 VPN view**.
2. To open the node or interface, use any *one* of the following:
   - Double-click the VRF or L3 VPN or CE node which is down.
   - Select the VRF or L3 VPN, click the **Open** icon.
3. From the VRF or L3 VPN form, click the **Incidents** tab to view the incident.

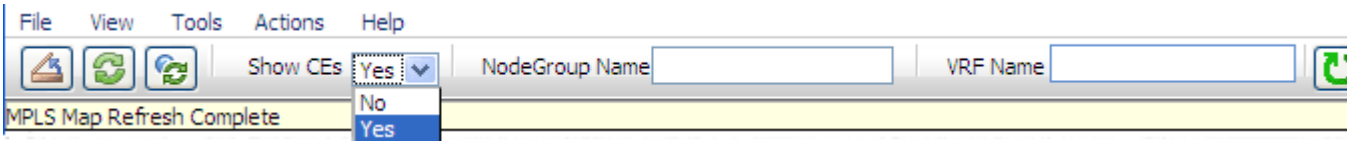
Related Topics:

MPLS Map Symbols

MPLS L3 VPN toolbar

Using the L3 VPN Map View Toolbar

The iSPI for MPLS provides the L3 VPN map view toolbar to help you customize your map views.



The L3 VPN Map view toolbar lets you customize your map views for the following tasks:

- Shows the CE nodes and interfaces on the L3 VPN map view.
- Shows the CE nodes associated with the selected VRF and Node Group Name.

The MPLS L3 VPN map view appears with the VRFs participating in the L3 VPN. The map view toolbar contains the NNMi icons such as Open, Refresh, Status Refresh, and Quick view. The following table lists the MPLS icons.

MPLS L3 VPN Map Toolbar Icons

Icon	Description
Show CEs	Select the option **Yes** or **No** to display the CE nodes on the MPLS L3 VPN map view.
NodeGroup Name	Type the Node Group Name. The CE nodes associated with the selected Node Group appears in the map view. As you type, the iSPI for MPLS provides a selection list of all current valid entries matching your criteria. You must use one of the suggested values. The Node Group name helps you customize your map views.
VRF Name	Type the VRF Name. The CE nodes associated with the selected VRF name appears in the map view.

To view the CE nodes available in the map view, follow the steps:

1. Select the option **Yes** from the Show CEs list.
2. Type the NodeGroup Name. The CE nodes participating in the selected NodeGroup appears. Type the **VRF Name**. The CE nodes associated with the VRF Name appears in the map view. If you provide both the options such as VRF Name and Node Group Name, the map view shows the CE nodes passing through the NodeGroup or VRF or both. If the conditions such as VRF Name and Node Name does not match the requirement, the map view shows the appropriate messages.

IP Multicast Map View

The IP Multicast map view shows the actual multicast path taken by the data packets over the MPLS cloud. Launch the IP Multicast Map view to troubleshoot the problems in your network.

Use the map view to perform the following tasks:

- Find the IP Multicast traffic flow in the downstream direction.
- Monitor the multicast traffic flow rate.
- Monitor the tree used by the packet to reach the receiver.

The URL action to launch the IP Multicast map view only appears after you install the iSPI for IP Multicast and verify that all NNMi and IP Multicast processes are running. For more information, see the *iSPI for IP Multicast Installation Guide* and *Online Help*.

To launch the iSPI for IP Multicast map view, follow these steps:

1. Navigate to the MVPN form[1]
    a. From the **Workspaces** navigation pane, click **MPLS-> MPLS MVPN Inventory**. The MVPN Inventory view opens in the right pane.
    b. Click the **Open** icon to view the MVPN form.
2. From the MVPN form, select the **MDTs Tab**.
3. Click the Open icon to view the MDT form. From MDT form, select the Data MDT.
4. Click **Actions-> Show the Multicast Flow**. The IP Multicast map view appears and starts from the selected source.
5. Click the Refresh icon to update the map view. Click the **Status Refresh** icon to update the status of MPLS objects.

To launch the iSPI for IP Multicast map view from the VRF form, follow these steps:

1. Navigate to the MVRF Form[2]
    a. From the **Workspaces** navigation pane, click **MPLS-> MPLS L3 VPN Inventory**. The L3VPN Inventory view opens in the right pane. Select the MVPN tab.
    b. Click the **Open** icon to view the MVRF form.
2. From the MVRF form, select the **Downstream MDTs** Tab. Select the Data MDT. *Donot select the Default MDT*.
3. Click **Actions-> Show the Multicast Flow**. The IP Multicast map view appears and starts from the selected source.
4. Click the **Refresh** icon to update the map view. Click the **Status Refresh** icon to update the status of MPLS objects.

MPLS Map Symbols

The map views provide you with the graphical representation of the MPLS objects participating in the network. Map symbols are used to represent nodes, interfaces, and MPLS objects such as VRFs, MVRFs, Hub VRF, and Hub MVRFs, The lines between the nodes and interfaces represent the connection or relationship between these objects.

The iSPI for MPLS uses NNMi shapes for the nodes and interfaces. The iSPI for MPLS introduces only one shape to represent a VRF on the map. The iSPI for MPLS uses the NNMi status colors to represent the status of the MPLS object. For more information, see *NNMi Help, About Status Colors*. The icons used to show the MPLS objects are as follows:

Icons Used By MPLS

Icons	Meaning
	Used in maps to represent a VRF.

1
2

Icons	Meaning
	Used in maps to represent a Hub VRF.
	Used in maps to represent an MVRF.
	Used in maps to represent a Hub MVRF.
	Used in map view to represent a CE node.
	Used in L3 VPN map views to show the following: • A full mesh L3 VPN topology in the network. • A PE interface connected to an unknown CE interface. The CE interface on the node is indicated on the map by a cloud symbol. • Multiple PE interfaces connected to one CE interface. This path is detected by the Hot Standby Router Protocol (HSRP) link connectivity. This HSRP connection is indicated on the map by a cloud symbol. • Multiple CE interfaces connected to one PE interface. This path is connected by a switch. This is indicated on the map by a cloud symbol.

Shapes Used By MPLS

Icons	Meaning
	Used to show the Full Mesh L3 VPN. This shape is superimposed with the cloud icon.
	Used to show an unknown CE node. When the shape is superimposed with the cloud icon, it shows the represents the following: • A PE interface connected to an unknown CE interface. The CE interface on the node is indicated on the map by a cloud symbol. • Multiple PE interfaces connected to one CE interface. This path is detected by the Hot Standby Router Protocol (HSRP) link connectivity. This HSRP connection is indicated on the map by a cloud symbol. • Multiple CE interfaces connected to one PE interface. This path is connected by a switch. This is indicated on the map by a cloud symbol.
	Used to represent a VRF. The color of the selected VRF is the status color.

Viewing the iSPI for MPLS Incidents

The iSPI for MPLS generates the incidents if any fault or change is detected in the network. You can monitor your critical MPLS-enabled nodes and MPLS objects by checking the inventory views and incidents

tab. In addition, all the MPLS incidents appear in the NNMi Incident management or Incident Browsing workspace.

To view the MPLS incidents, follow any one of the steps:

1. From the Left navigation panel, select the **MPLS** workspace and click <MPLS> view (for example, **MPLS- > MPLS L3 VPN view**).
2. Click the  **Open** icon and check the Incident tab to view an incident of your interest.

OR

1. From the workspace navigation pane, select the **Incident Management** or **Incident Browsing** workspace.
2. Select the view and incident of your interest. (For example, select **All incidents** view and sort the incidents by the column **Family (MPLS)**).

The iSPI for MPLS generates the following types of incidents:

- MPLS-specific Incidents
- Service Impact Incidents
- Pairwise MPLS Incidents

MPLS Incidents

You can view the following MPLS incidents from the NNMi console or MPLS inventory:

- Incidents generated for the MPLS-enabled nodes and objects
- Service Impact Incidents
- Pairwise Incidents for the MPLS objects

MPLS Incidents

MPLS Incident Name	Description
MplsTETunnelDown	The TE Tunnel incident appears when the status of the TE Tunnel is down. This incident is a part of the MPLS Traffic Engineering family.
MplsVRFDown	The VRF incident appears when the status of the selected VRF is down. This incident belongs to the MPLS L3 VPN family. This incident includes the description if the VRF is a hub and the status of the Hub VRF is down.
MplsVRFWarning	The VRF incident is generated when the status of one of the PE interfaces but not all the interfaces associated with the VRF is Down.
MplsPseudoWireVCDown	The Pseudowire VC incident appears when the PseudoWire VC is Down. This incident belongs to the MPLS PseudoWire VC family.

Service Impact Incidents

You can view the Service Impact incidents from the **NNMi Workspaces-> Service Impact incidents**. The iSPI for MPLS lists the Service Impact incidents for the selected L3 VPNs. The service impact incidents does not change the status of the L3 VPNs.

The root-cause incident generated by NNMi for a CE node generates a service impact incident. This incident provides details of the affected L3VPNs in the network. For example, an Interface Down incident can change the status of a CE node participating in an L3VPN. This incident is useful to identify and troubleshoot the service.

For example, when the status of the Hub VRF is Down, a service impact incident **MplsL3VPNCritical** is generated. The correlation nature of this incident is **Service Impact** incident.

MPLS Service incidents

MPLS Incident Name	Description
MVRFCritical	Generated when the status of an MVRF is Critical. The status of the MVRF is Critical when the VRF is down or the MTI associated with the MVRF is down. This is a service impact incident.
MplsL3VPNCritical	Generated when the status of an L3 VPN is critical because the status of the hub VRF is critical. This is a service impact incident.
MplsL3VPNImpacted	Generated when a fault (NodeDown,InterfaceDown Or Connection Down) is detected on a CE node. This is a service impact incident.

MPLS Pairwise Incidents

You can view the following MPLS Pairwise incidents in the Incidents tab. For more information about Pairwise Incidents, see *NNMi help, Incident Pairwise Configuration*.

Pairwise MPLS Incidents

Name	Description
CiscoMplsVRFIfDownUpPair	Cancels a CiscoMPLSVRFDown incident with a CiscoMPLSVRFUp incident from the same node and interface.
JnxMplsTETunnelDownUpPair	Cancels a Juniper MPLS TE Tunnel down incident with a Juniper MPLS TE Tunnel up incident from the same node and TE Tunnel.
JnxMplsVpnIfDownUpPair	Cancels a down incident with an up incident from the Juniper- enabled interface participating to form an L2VPN and L3VPN from the same node and VPN.

Viewing the MPLS SNMP Traps

The SNMP traps are generated from the MPLS-enabled devices. The iSPI for MPLS supports the trap driven polling. When the traps are generated, the State Poller starts polling the devices, updates the status, and generates the incidents. The SNMP traps (Down traps) are correlated under the MPLS incidents. There is a one minute delay to correlate the root cause with the symptom.

For example, the CiscoMplsPseudoWireVCDown trap starts the poll on the associated Pseudowire VC. After polling, correlates the root cause with the trap and generates MplsPseudoWireVCDown incident.

SNMP Traps

Name	Family	Correlation Type	Description
CiscoMplsTETunnelUp	MPLS Traffic Engineering	-	Generated when the status of the configured TE Tunnel returns from Down to Up. This trap is generated by a Cisco node.
CiscoMplsTETunnelDown	MPLS Traffic Engineering	MplsTETunnelDown	Generated when the status of the configured tunnel is Down. This trap is generated by a Cisco node.
CiscoMplsTETunnelRerouted	MPLS Traffic Engineering	-	Generated when the status of the configured tunnel is Rerouted. This trap is generated by a Cisco node.
CiscoMplsVRFIfUp	MPLS Interface	-	Generated when the status of the VRF interface returns from Down to Up. This trap is generated by a Cisco node.
CiscoMplsVRFIfDown	MPLS Interface	MplsVRFDown	Generated when the status of the VRF interface is Down. This trap is generated by a

Name	Family	Correlation Type	Description
			Cisco node.
CiscoMplsL3VpnVrfUp	MPLS L3VPN	-	Generated when the status of the VRF associated with an L3VPN returns from Down to Up. This trap is generated by a Cisco node.
CiscoMplsL3VpnVrfDown	MPLS L3VPN	-	Generated when the status of the VRF associated with an L3VPN returns from Down to Up. This trap is generated by a Cisco node.
CiscoMplsPseudoWireVCUp	MPLS PseudoWire VC	-	Generated when the status of the configured PseudoWire VC returns from Down to Up. This trap is generated by a Cisco node.
CiscoMplsPseudoWireVCDown	MPLS PseudoWire VC	MplsPseudowireVCDown	Generated when the status of the configured PseudoWire VC is Down. This trap is generated by a Cisco node.
JnxMplsTETunnelUp	MPLS Traffic Engineering	-	Generated when the status of the configured tunnel is Up. This trap is generated by a Juniper node.

Name	Family	Correlation Type	Description
JnxMplsTETunnelDown	MPLS Traffic Engineering	MplsTETunnelDown	Generated when the status of the configured tunnel is Down. This trap is generated by a Juniper node.
JnxMplsVpnIfUp	MPLS Interface	-	Generated when the status of the VPN-enabled interface is Up. This trap is generated by a Juniper node.
JnxMplsVrfIfDown	MPLS Interface	MplsVRFDown	Generated when the status of the VRF interface is Down. This trap is generated by a Juniper node..
JnxMplsPseudoWireVCDown	MPLS PseudoWire VC	MplsPseudowireVCDown	Generated when the status of the configured PseudoWire VC is Up.This trap is generated by a Juniper node.
JnxMplsPseudoWireVCUp	MPLS PseudoWire VC	-	Generated when the status of the configured PseudoWire VC is Down. This trap is generated by a Juniper node.

The following SNMP traps are generated by the Cisco IOS-XR devices:

- CiscoMplsL3VpnVrfUp
- CiscoMplsL3VpnVrfDown
- CiscoIOSXRMplsTETunnelUp
- CiscoIOSXRMplsTETunnelDown
- CiscoIOSXRMplsTETunnelRerouted

By default, the Cisco IOS-XR traps are disabled.

Actions Available in the iSPI for MPLS

With the iSPI for MPLS, view the complete connectivity of the network that you want to monitor. If you log on to the NNMi console with an operator (level 1 or level 2) or guest credentials, view your network by using additional user actions.

The iSPI for MPLS presents three additional map views—**MPLS Path view, MPLS L3 VPN Map view,** and **MPLS TE Path view**—that help you construct, visualize and troubleshoot the network. With the iSPI for MPLS, you can view the graphical representation of your network connectivity by using the following actions:

MPLS Actions

Action	Description
MPLS Path view	Shows an MPLS path map view from source to destination in the network. This action is available from the MPLS LSR view.
MPLS L3 VPN Map view	Shows an MPLS L3 VPN map. The MPLS L3 VPN Topology Map view shows the VRFs participating to form an L3 VPN. This action is available from the MPLS L3 VPN view.
MPLS TE Tunnel Map view	Shows the TE Tunnel Path from the source to the destination. The TE Tunnel Path view provides the real-time routing data flow path from source to destination. This action is available from the MPLS TE Tunnel view.
Show Multicast Data Flow	Displays a Multicast forwarding tree for the selected MDT. The action is available from the MDT form.

Related Topics:

MPLS Path view

MPLS L3 VPN map view

MPLS TE Tunnel map view

Show Multicast Data Flow

Integrating the iSPI for MPLS with Route Analytics Management System (RAMS)

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.

The iSPI for MPLS shares and sends the L3 VPN information such as L3 VPN name and RT list to RAMS appliances by using the following script:

`/opt/OV/bin/nmsmplsvpnandrtlist.ovpl`

With an administrative privileges to the NNMi console, send the L3 VPN and RT list to the RAMS appliance. After the integration with RAMS, you can monitor and view the SNMP traps from the RAMS appliance in the RAMS tab in the L3 VPN form. The trap list shows the most recent 100 traps.

To monitor the L3 VPN inventory by using RAMS, the L3 VPN names should be same as sent to the RAMS appliance. If you modify the L3 VPN names, send the names again to the RAMS appliance by using the `nmsmplsvpnandrtlist.ovpl`. For more information, see *MPLS reference pages*.

Related Topic:

L3 VPN Form: RAMS Tab

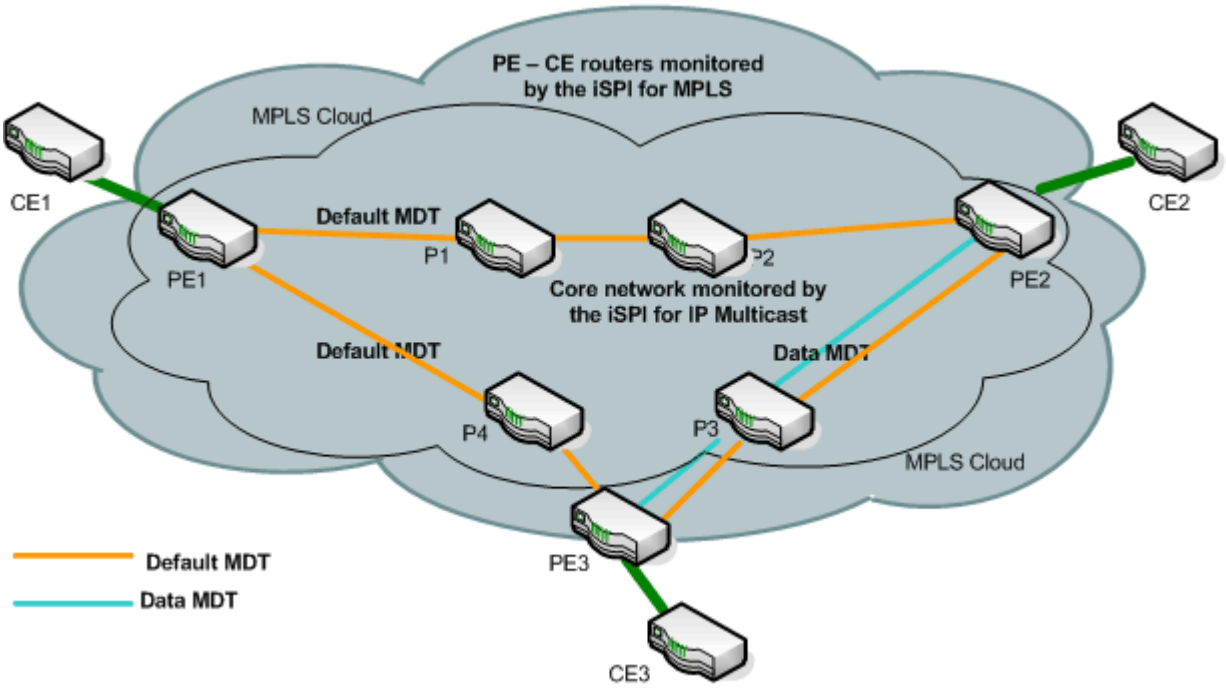
Integrating the iSPI for MPLS with the iSPI for IP Multicast

The iSPI for MPLS helps you to monitor the Provider Edge (PE) routers discovered in an MVPN topology. The PE routers are configured with the multicast-enabled VRF (MVRF) capabilities and use the multicast services to transmit data. To view the list of MVPN inventory, see MVPN Inventory. The iSPI for IP Multicast helps you monitor the multicast traffic flows in the core network over the MPLS cloud.

Navigate 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 MDTs. For more information about MVPN, see Overview of the Multicast VPN (MVPN).

For more information about launching the IP Multicast views, see IP Multicast map view. For more information about the iSPI for IP Multicast, see *Help for IP Multicast.*

Monitoring the network using the iSPI for MPLS and iSPI for IP Multicast



In the example, the iSPI for MPLS monitors the PE routers (PE1, PE2 and PE3) and the PE-CE link (PE1-CE1, PE2-CE2, and PE3-CE3). The core network consists of the PE1, PE2, and PE3 and provider routers (P1, P2, P3, and P4). The iSPI for IP Multicast monitors the traffic flowing from and into the core routers. View the downstream path and upstream path to find multicast flow in the network.

Integrating the iSPI for MPLS with the iSPI Performance for QA (Quality Assurance)

The iSPI for MPLS helps you to monitor the traffic passing through the VRFs in 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 performance capabilities for the following tasks:

- Find the delay or packet loss for the traffic passing through the selected VRF.
- Troubleshoot the connectivity for the selected VRFs on basis of the configured tests.
- Troubleshoot the PE-PE connectivity.
- Helps in site management.

You can monitor the tests configured for the selected VRF by using the VRF form. The attributes in the QA probes tab helps you to 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*.

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

Related Topic:

VRF: QA Probes Tab

Introduction to the iSPI for MPLS Administrator

As an administrator, you can perform the following tasks by using **MPLS Configuration** workspace:

- Configure Polling Intervals
- Configure Router Targets
- Configure VPWS VPN
- Configure Regional Manager

Manage and Unmanage Nodes

The iSPI for MPLS discovers the MPLS-enabled nodes and interfaces. The nodes or interfaces that are not managed by NNMi are not discovered by the iSPI for MPLS.

You cannot specifically manage or unmanage the MPLS objects (TE Tunnels, VRFs, MVRFs, and VC LSPs) as the management mode attribute for an MPLS node is inherited from NNMi. If a node is unmanaged, all the MPLS objects such as TE Tunnels, VRFs, and VC LSPs are in an unmanaged state but the derived objects such as L3VPN, L2VPNs or PseudoWire VC does not have the settings.

If an unmanaged node returns into a managed mode in NNMi inventory, the MPLS discovery process starts and updates the management mode of the MPLS objects. Also, a notification is sent to the State Poller about the updated management mode. The state of the MPLS object is set to *Not Polled* and the status is set to *No Status*.

Backup and Restore Actions

You can perform the backup and restore command for the iSPI for MPLS by using NNMi Backup and Restore actions. For more information, see *Back Up and Restore NNMi*. Check the MPLS file in the location provided for backup. For example: *C:/tmp/nnm-bak-20080924095922-mplsdb.pgd*.

Start the Configuration Poll Command

Use the **Actions** -> **Configuration Poll** to start the Configuration poll for the selected MPLS nodes. For more information, see *Launch the Actions: Configuration Poll Command*

Log on to the iSPI for MPLS Configuration workspace

After installing NNMi, use the URL to log on to the NNMi console. For more information, see *Configure Sign-In Access*.

To access the **MPLS Configuration** workspace, no additional log on and password is required if your user role defines that you can access the NNMi configuration workspace. For more information about the user roles, see Help for NNMi, *Determine Account Roles*.

Log on to the MPLS Configuration Workspace:

- Open the URL with Fully Qualified Name (FQDN), and log on as a non-system admin user. When you access the MPLS Configuration workspace, no username or password is required to view the interface.
- Open the URL with hostname/localhost and Single Sign On (SSO) works when you log on as a non-system admin privileged user. Follow the steps for the Single Sign On to work:

1. From the **User Configuration Interface**, click the **Enable URL Re-direct** checkbox and save the settings.
2. Log on again, and check the localhost and hostname automatically shows the FQDN in the URL. The MPLS Configuration opens. Do not type the username and password again.

If you are using system as username to log on, SSO is disabled. You have to type the username and password again to view the MPLS Configuration.

Related Topics:

Configuring the iSPI for MPLS

Introduction to the iSPI for MPLS Administrator

As an administrator, you can perform the following tasks by using **MPLS Configuration** workspace:

- Configure Polling Intervals
- Configure Router Targets
- Configure VPWS VPN
- Configure Regional Manager

Manage and Unmanage Nodes

The iSPI for MPLS discovers the MPLS-enabled nodes and interfaces. The nodes or interfaces that are not managed by NNMi are not discovered by the iSPI for MPLS.

You cannot specifically manage or unmanage the MPLS objects (TE Tunnels, VRFs, MVRFs, and VC LSPs) as the management mode attribute for an MPLS node is inherited from NNMi. If a node is unmanaged, all the MPLS objects such as TE Tunnels, VRFs, and VC LSPs are in an unmanaged state but the derived objects such as L3VPN, L2VPNs or PseudoWire VC does not have the settings.

If an unmanaged node returns into a managed mode in NNMi inventory, the MPLS discovery process starts and updates the management mode of the MPLS objects. Also, a notification is sent to the State Poller about the updated management mode. The state of the MPLS object is set to *Not Polled* and the status is set to *No Status*.

Backup and Restore Actions

You can perform the backup and restore command for the iSPI for MPLS by using NNMi Backup and Restore actions. For more information, see *Back Up and Restore NNMi*. Check the MPLS file in the location provided for backup. For example: *C:/tmp/nnm-bak-20080924095922-mplsdb.pgd*.

Start the Configuration Poll Command

Use the **Actions** -> **Configuration Poll** to start the Configuration poll for the selected MPLS nodes. For more information, see *Launch the Actions: Configuration Poll Command*

Log on to the iSPI for MPLS Configuration workspace

After installing NNMi, use the URL to log on to the NNMi console. For more information, see *Configure Sign-In Access*.

To access the **MPLS Configuration** workspace, no additional log on and password is required if your user role defines that you can access the NNMi configuration workspace. For more information about the user roles, see Help for NNMi, *Determine Account Roles.*

Log on to the MPLS Configuration Workspace:

- Open the URL with Fully Qualified Name (FQDN), and log on as a non-system admin user. When you access the MPLS Configuration workspace, no username or password is required to view the interface.
- Open the URL with hostname/localhost and Single Sign On (SSO) works when you log on as a non-system admin privileged user. Follow the steps for the Single Sign On to work:

1. From the **User Configuration Interface**, click the **Enable URL Re-direct** checkbox and save the settings.
2. Log on again, and check the localhost and hostname automatically shows the FQDN in the URL. The MPLS Configuration opens. Do not type the username and password again.

If you are using system as username to log on, SSO is disabled. You have to type the username and password again to view the MPLS Configuration.

Related Topics:

Configuring the iSPI for MPLS

Monitoring MPLS Network Health

You can monitor the health of your network by using the iSPI for MPLS. Before you start monitoring the network, ensure that NNMi and iSPI for MPLS are running and the discovery process is working.

You can the monitor and manage the network by using services such as State Poller and Causal Engine. The real-time monitoring of the network periodically helps you to manage and detect the faults in the network.

For more information about how the iSPI for MPLS monitors the network, see State Poller and Causal Engine . For more information about NNMi, see *NNMi State Poller and Causal Engine.*

Related Topics:

State Poller

Causal Engine

State Poller

The MPLS State Poller service checks each discovered and managed MPLS node, interface, VRFs, TE tunnel, and VC LSP that is monitored in the management station.

The MPLS State Poller gathers information from the discovered devices such as nodes, interfaces, and SPI objects and reports the results of the state of the devices in the database. The State Poller is configured to do periodic polling of devices. The polling is dynamic as the State Poller identifies the topology changes and polls newly discovered devices and MPLS objects such as TE tunnels, VRFs, and VC LSPs. The poller starts polling of the devices and notifies the Causal Engine for any network changes.

The default value of the State Poller is five minutes.

You can change the polling duration from the **MPLS Configuration** workspace.

Causal Engine

The Causal Engine gathers information from the State Poller, scheduled discovery, SNMP traps, and incidents. Causal Engine collects information to calculate the *Status* of the nodes and MPLS objects configured on the nodes. Thus, the Causal Engine helps in monitoring the health of the network.

Causal Engine updates the status attributes in the respective MPLS views and forms. You can view the updated status information for the following MPLS objects:

- L3 VPN status
- MVPN status
- VRF status
- TE Tunnel status
- PseudoWire VC status
- VPWS VPN status
- VLPS VPN status

The health status is dynamic. For more information, see *NNMi Causal Engine and Monitoring*.

On-Demand Status Poll

The status poll command starts a real-time check of the state of the selected device. If the state is changed since the last monitoring cycle then the iSPI for MPLS calculates an updated status reading for the selected device.

You can start the status poll for all the MPLS-enabled objects. You can start the polling for any node from NNMi views. The status poll starts the poll for NNMi nodes. This poll display does not contain the iSPI for MPLS information explicitly but the starts the discovery process for the MPLS-enabled nodes.

To start the status poll, see *Help for NNMi console, Verify Current Status of a Device.*

Configuring the iSPI for MPLS

With an administrative privileges to NNMi console, you can use the **MPLS Configuration** workspace to perform the following tasks:

- Configure Polling Intervals
- Configure Router Targets
- Configure VPWS VPN
- Configure Regional Manager

The MPLS Configuration workspace consists of the following tabs:

Configuration Tab	Description
Polling Frequency	Used to set the time in minutes or seconds between the two consecutive polls for the MPLS object. By default, the State Poller polls the MPLS nodes periodically for every five minutes for the status of the MPLS objects such as TE Tunnels.
Exclude Route Target	Used to add, delete or edit the list of Route Targets (RTs) to be ignored for the discovery process.
VPWS VPN Configuration	Used to add, delete or edit the PseudoWire VC attributes to form a VPWS VPN.
Regional Manager Connections	Used to configure the Regional manager. This Regional manager configuration helps you to monitor the Regional manager inventory. After configuration, you can start communication between Global Network Manager and Regional Manager.

Related Topics:

Configure Polling Frequencies

Configure Exclude Route Targets

Configure VPWS VPN Configurations

Configure MPLS Regional Manager Connections

Configure the Polling Frequency

After the iSPI for MPLS discovers the available MPLS nodes and interfaces in the network, you can modify the default polling interval by using the **Polling Frequencies** tab to keep your topology up-to-date.

To configure the polling frequencies for the MPLS objects, follow these steps:

1. Navigate to the MPLS Configuration form.[1]
2. In the **Poller Frequencies** tab, specify the following details:
   - **TE Tunnel Polling Frequency**: Sets the time in minutes, seconds between the two consecutive polls for TE tunnel. By default, the State Poller polls periodically every 5 minutes for the status of TE tunnels.
   - **VRF Polling Frequency**: Sets the time in minutes, seconds between the two consecutive polls for VRF. By default, the State Poller polls periodically every 5 minutes for the status of VRFs.
   - **PseudoWire VC Frequency**: Sets the interval (in minutes) between the two consecutive polls for PseudoWire VC. The default value is 5 minutes.
   - **VRF Performance Frequency**: Sets the interval (in minutes) between the two consecutive polls for the selected VRF. The default value is 5 minutes.
   - **LSR Performance Frequency**: Sets the interval (in minutes) between the two consecutive polls for the selected LSR node. The default value is 5 minutes.
3. Click the **Save** icon.

Configure the Route Targets

To discover the L3 VPNs, you can add, edit or delete the RTs from the MPLS Configuration workspace. Whenever you update the list of RTs, the iSPI for MPLS discovers and re-computes the L3 VPNs.

To configure the route targets, follow the steps:

1. Navigate to the MPLS Configuration form.[2]
2. In the **Exclude Route Targets** tab, specify a list of Route Targets to be excluded, click **Add**. To update the database with the list of RTs to be ignored in the discovery process, click **Save**. The add or remove action starts the L3 VPN topology recalculation.

---

1 From the workspace navigation panel, select the **MPLS Configuration** workspace.

Select the **Poller Frequencies** tab.

2 From the workspace navigation panel, select the **MPLS Configuration** workspace.

Select the **Exclude Route Targets** tab.

3. To delete a Route Target, click **Remove**. The remove action specifies the list of RTs to be ignored in the discovery process.
4. Click **Select All** to select all the RTs to perform actions such as remove or add.
5. Click the **Save** icon.

Configure the VPWS VPNs

To monitor a VPWS VPN, configure the PseudoWires VC attributes in the **VPWS VPN Configuration** tab. The VPWS VPNs appear in the inventory view only after you complete the configuration steps.

The **Enable VC_ID based VPWS VPNs**option enables the discovered PseudoWire VCs to be grouped with VC_Id to form a VPWS VPN. If the option is true, all the VPWS VPNs appear as VPWS_VCId. By default, the option is always false. To form a VPWS VPN with a unique name as provided by you, check if the option is disabled. If the PseudoWire VC does not participate in any of the VPWS VPNs, appears as **Default Group**.

To add a new VPWS VPN in the MPLS Inventory, follow the steps:

1. Navigate to the MPLS Configuration form.[1]
2. In the **VPWS VPN Configuration** section, click the **New** icon and specify the following details:
   - **VPWS VPN Name:** Type the name of the VPWS VPN. This option is mandatory. This name is unique and the VPWS-VPNs names are used to identify the L2 VPN.
   - **Include VC ID:** Type the VC IDs of the Pseudo Wires VCs. Click **Add**. To remove the VC ID from the list, click **Remove**. To select all the VC IDs, click **Select All.**
   - **Node Group Names**: Select the name of the nodes forming the group.
   - **Encapsulation Type:** Select the mode of data transmission from the drop-down list.
3. Click the **Save** icon**.** To clear the configuration, click **Clear**. To close the configuration, click **Close**

To edit or delete the configured VPWS VPNs, follow the steps:

1. Navigate to the MPLS Configuration form.[2]
2. To update or delete a VPWS VPN, select a row, click the edit icon or delete icon.
3. Click the **Save and Close** icon. To clear the configuration, click **Clear**.To close the configuration, click **Close**.

---

1 From the workspace navigation panel, select the **MPLS Configuration** workspace.

Select the **VPWS VPN Configuration** tab.

2 From the workspace navigation panel, select the **MPLS Configuration** workspace.

Select the **VPWS VPN Configuration** tab.

Connect to an MPLS Regional Manager Connection

As an administrator, you can configure the iSPI for MPLS Global Manager to communicate with other Regional Managers across the globe by using the **MPLS Configuration** workspace. For more information about NNMi Global Manager and Regional Manager connections, see *NNMi Help, Connecting Multiple NNMi Management Servers.*

To enable the iSPI for MPLS Regional Manager connection, follow the steps:

1. Navigate to the Regional Manager form.[1]
2. Perform the following task as per your requirement.
   - To create a new configuration, click the **New** icon.
   - To edit a configuration, select a row, click the **Open** icon.
   - DO NOT delete a configuration (the Delete icon). For more information, see NNMi Help, *Disconnect Communication with a Regional Manager.*
3. Select the **Regional Manager Configuration** form, type the basic configuration settings. For more information, see basic settings.
4. From the **Connections** tab, navigate to the **Regional Manager Connections** form. For more information, see Configure the iSPI for MPLS Regional Manager.
5. Click **Save** to the Regional Manager form.
6. Click **Save**. The iSPI for MPLS Global Network Manager establishes communication with the specified Regional Manager.

Basic Settings

Attributes	Description
Name	Type a meaningful name for this configuration record about the Regional MPLS management server. The iSPI for MPLS Regional Manager name should be same as NNMi Regional Manager name.
Description	Provide relevant information about your Regional Manager connection. This field is optional.

Related Topics:

Configure to the iSPI for MPLS Regional Manager.

1

From the workspace navigation panel, select the **MPLS Configuration** workspace.

Select the **MPLS Regional Manager Connections** tab.

Configure the iSPI for MPLS Regional Manager

As an administrator, you can configure the iSPI for MPLS Global Manager to communicate with other Regional Managers across the globe by using the **MPLS Configuration** workspace. You can only configure the Regional Manager connection if the iSPI for MPLS is already up and running.

Before you configure the iSPI Regional Manager connection, make sure that NNMi Regional Manager is already configured. The name of the iSPI for MPLS Regional Manager should be same as the NNMi Regional Manager to establish the connection.

To configure the iSPI for MPLS Regional Manager connection, follow the steps:

1. Navigate to the Regional Manager Connection form.[1]
2. Type the connection configuration settings for the iSPI for MPLS Regional Manager connection. See connection configuration settings. If the Regional Manager is configured for high-availability, enter configuration settings for each server in the high-availability group (application fail-over).
3. Click **Save** to return to the Regional Manager form.
4. Click **Save** to return to the MPLS Configuration form. The iSPI for MPLS establishes communication with the Regional iSPI for MPLS management server. The Regional Manager forwards information about discovery and monitoring results.

To verify that the Regional Manager connection is working, *see NNMi Help, Determine the State of the Connection to a Regional Manager.*

Connection Configuration Settings for a Regional Manager of the iSPI for MPLS

Attribute	Description
Hostname	The fully-qualified hostname of the Regional iSPI for MPLS management server. The iSPI for MPLS uses this hostname for communication with the Regional iSPI for MPLS management server and to construct URL Actions. See *NNMi Help, Authentication Requirements for launch URLs* . **Note**: If you want iSPI for MPLS to use secure sockets layer encryption (HTTPS) to access this Regional MPLS management server, the value is case-sensitive and must match the hostname as specified in that server's SSL Certificate.
Use Encryption	If ☐ disabled, the iSPI for MPLS uses hypertext transfer protocol (HTTP) and plain sockets to access the iSPI for MPLS Regional management server. If ☑ enabled, the iSPI for MPLS uses secure sockets layer encryption (HTTPS / SSL) to access the the iSPI for MPLS Regional management server.
HTTP(S) Port	Default value for HTTP is 24040. Default value for HTTPS 24043. If ☐ Use Encryption is disabled, enter the port number for HTTP access to the NNMi and MPLS console on the Regional NNMi management server. If ☑ Use Encryption is enabled (previous attribute), enter the port number for HTTPS

1

From the workspace navigation panel, select the **MPLS Configuration** workspace.

Select the **Regional Manager Connections** tab.

Attribute	Description
	access to the NNMi console on the Regional NNMi management server. For MPLS ports, check the port numbers from the `nms-mpls-ports.properties` file. Open the nms-mpls-ports.properties file from the `%NnmDataDir%\shared\mpls\conf` or `$NnmDataDir/shared/mpls/conf` directory on the management server, and then note down the iSPI for MPLS HTTP and HTTPS values if you are not using the default values.
User Name	Type the user name required for the iSPI for MPLS sign-in for the account on the iSPI for MPLS Regional management server. The user name should be same as the name provided while installing the iSPI for MPLS.
User Password	Type the password for the iSPI for MPLS account on the iSPI for MPLS Regional management server. Note: The iSPI for MPLS encrypts the password and displays asterisks for this attribute. If you want to change the password, first clear the asterisks displayed in the Password attribute and enter the new Password value.
Ordering	A numeric value. The iSPI for MPLS checks for configuration settings in the order you define (lowest number first). The iSPI for MPLS uses the first match found for each address. Provide a unique connection ordering number for each Regional Manager configuration.

Tracking Your MPLS Licenses

To assist you in tracking your MPLS licenses, the iSPI for MPLS shows a report of the current number of discovered nodes and the current MPLS licensed capacity limit, access **View Licensing Information** from either of the following locations:

- **Help-> System Information**
- **Help -> About HP Network Node Manager i Software.**

For more information about the iSPI for MPLS licenses and point usage, see **Help for NNM iSPIs → iSPI for MPLS System Information**

The three types of the iSPI for MPLS licenses are:

- **Instant-on**: The Instant-on license is an evaluation license. The valid period of this license is sixty days.
- **Points Based**: The Points based license is the actual point consumption by the iSPI for MPLS. The points used appear in the iSPI for MPLS system information.
- **Migration**: The update licenses are valid only for the user updating from pervious versions (7x.x) of MPLS SPI.

The following tabs appear in the **iSPI for MPLS System Information**:

Licensing Tabs

Name	Purpose
License Report	Shows the total points used by the iSPI for MPLS.
Topology Statistics	Shows the total number of MPLS objects monitored by the iSPI for MPLS. The MPLS objects monitored are Label Switched Routers, L3 VRF Interfaces, and L2 Forwarding Interfaces.

Extend a Licensed Capacity:

To extend the licensed capacity, purchase and install an additional iSPI for MPLS License. Contact your HP Sales Representative or your Authorized Hewlett-Packard Reseller for information about the iSPI for MPLS licensing structure, and to learn how to add license tiers for enterprise installations.

To obtain additional license keys, go to the HP License Key Delivery Service: https://-webware.hp.com/welcome.asp. For more information, see *MPLS Installation Guide.*

Troubleshooting the iSPI for MPLS

The following information can help you troubleshoot and resolve common problems in the iSPI for MPLS:

Not able to view the TE Tunnels, VRFs, VC LSPs for a node.

Verify the MPLS-enabled node is managed and discovered in the NNMi topology. Select a node and click the **Actions > Configuration Poll**, or use the `nnmconfigpoll.ovpl` command. The iSPI for MPLS uses the NNMi capability to poll the MPLS-enabled nodes. No iSPI for MPLS specific information is displayed.

The iSPI for MPLS objects (TE Tunnels, MVRFs, VRFs, VC LSPs) are available in the views but status is either No-status or out-of-date.

Start the **Status Poll** for the nodes. Select a node and click the **Actions > Status Poll.** No iSPI for MPLS specific information is displayed.

Able to view the node and corresponding MPLS objects, but not accurately. You want to view the correct data for this node.

Delete the node in NNMi. This action deletes the corresponding iSPI for MPLS objects. Add the node in again in the NNMi topology.

The PseudoWire VC shows only one VC LSP.

Make sure that the other VC LSP of the PseudoWire VC is configured in NNMi with the proper community strings. In addition, make sure that the other VC LSP is also discovered.

Not able to view the MPLS objects in the MPLS views. Not able to view the NNMi nodes also.

Reset the database by using the NNMi reset command. For more information, use *NNMi reference pages*. This command must be used with caution and only when you are not able to resolve the issues.

All the VRFs are accurate and visible in the MPLS views. However, the list of VRFs participating to form an

L3 VPN is not accurate.

The VPN discovery is based on the RTs. If you have Management-VPNs, Extranets, the associated RTs are used to form an L3VPN. You can add, ignore, or edit the RTs from the **MPLS configuration** workspace.

In the node form, the Id field in the PseudoWire VC LSP tab is zero.

During the discovery process of PseudoWire VC LSP, sometimes the VC LSPs does not get associated with the PseudoWire VC. Wait for the discovery process to complete and start the Configuration Poll for the selected node.

After you perform the Configuration or Status poll for the selected node, you still do not get any MPLS information.

Limitation in this version of the product. Though the configuration and status poll starts the iSPI for MPLS actions but does not display any message.

You performed various configuration actions on a node such as updated community strings. But, iSPI for MPLS still shows the old data in the views.

Wait till the next discovery cycle. However, you can start the **Configuration Poll** on the node.

The source object in the incidents view appears as none value.

Not all the source objects participate in VC LSP, TE Tunnels or VRF.

The SNMP traps related to Cisco IOS-XR devices are not appearing.

Be default, the Cisco IOS-XR traps are disabled. You have to enable the traps.

Changed community string for a router. You want to use the updated string immediately.

- Update using NNMi SNMP Configuration. For more information, see *Help for NNMi, SNMP Configuration.*
- Start the Configuration Poll.

Update the polling intervals.

Use the MPLS Configuration workspace to configure the polling interval.

Not able to view MPLS Configuration workspace.

Use your administrative privileges to view the **MPLS Configuration** workspace.

Not able to view the PE-CE connection from the GNM inventory.

This version of the iSPI for MPLS supports PE-CE connection only when both the PE and CE nodes and interfaces are discovered in one Regional Manager. If the PE node is discovered in one Regional Manager and CE node in another Regional Manager, the consolidated PE-CE connection does not appear in the MPLS inventory (GNM).

Not able to view the CE nodes in the iSPI for MPLS inventory.

The discovery of CE nodes participating in an L3VPN may require multiple rounds of discovery, even if the CE node and the corresponding PE node are seeded at the same time. The actual number of discovery cycles (one or two) depends on manageability of the CE node and the sequence in which the PE and CE nodes are discovered by NNMi and the iSPI for MPLS.

Index

L

M