



**Hewlett Packard**  
Enterprise

# HPE Network Node Manager iSPI for MPLS Software

Software Version: 10.30  
for the Windows® and Linux® operating systems

Online Help

Document Release Date: June 2017  
Software Release Date: June 2017

## Legal Notices

### Warranty

The only warranties for Hewlett Packard Enterprise 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. HPE 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 HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright Notice

© Copyright 1995-2017 Hewlett Packard Enterprise Development LP

### Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Apple is a trademark of Apple Computer, Inc., registered in the U.S. and other countries.

AMD is a trademark of Advanced Micro Devices, Inc.

Google™ is a registered trademark of Google Inc.

Intel®, Intel® Itanium®, Intel® Xeon®, and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Internet Explorer, Lync, Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Red Hat® Enterprise Linux Certified is a registered trademark of Red Hat, Inc. in the United States and other countries.

sFlow is a registered trademark of InMon Corp.

UNIX® is a registered trademark of The Open Group.

This product includes software developed by the Apache Software Foundation.  
(<http://www.apache.org>).

This product includes software developed by the Visigoth Software Society (<http://www.visigoths.org/>).

## Documentation Updates

The title page of this document contains the following identifying information:

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to:  
<https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=>

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

## Support

Visit the HPE Software Support web site at: <https://softwaresupport.hpe.com>

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

HPE Software Support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to <https://softwaresupport.hpe.com> and click **Register**.

To find more information about access levels, go to:

<https://softwaresupport.hpe.com/web/softwaresupport/access-levels>

## About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

# Contents

Chapter 1: Network Node Manager iSPI for MPLS Software .....	8
Chapter 2: Understanding MPLS Objects .....	10
MPLS L3 VPN .....	10
L3 VPN, VRFs, VRF-Lite, Shadow Routers, and Route Targets .....	11
VRFs Grouping for an L3 VPN .....	11
L3 VPN Topology .....	12
L3 VPN Naming .....	12
Inter-Provider VPN .....	13
MPLS L2 VPN .....	15
Virtual Private LAN Service (VPLS VPN) .....	15
Virtual Private Wire Service VPN (VPWS VPN) .....	16
MPLS TE Tunnels .....	17
MPLS PseudoWire VC .....	18
Label Switch Path .....	19
LSP Service Mapping .....	20
MPLS Customer Edge (CE) Management .....	20
Multitenant Architecture .....	22
Chapter 3: Help for NNM iSPI for MPLS Operators .....	24
Monitoring Your Network with MPLS Inventory .....	24
LSR (Label-Switched Routers) Inventory .....	25
Actions Available in LSR Inventory .....	27
L3 VPN Inventory .....	28
MVPN Inventory .....	32
VPLS VPN Inventory .....	34
VPWS VPN Inventory .....	37
PseudoWire VC Inventory .....	39
Monitoring LSPs .....	42
TE Tunnel Inventory .....	43
Monitored LSP Inventory .....	46
Actions Available for Monitored LSP Inventory .....	46
SDP Inventory .....	49
Monitoring your network with MPLS Forms .....	51
L3 VPN Form .....	52
L3 VPN Form: VRFs Tab .....	53
Monitoring LSPs .....	53
L3 VPN Form: Status Tab .....	54
L3 VPN Form: Conclusions Tab .....	55
L3 VPN Form: Incidents Tab .....	56
L3 VPN Form: RAMS Traps Tab .....	56
L3 VPN Form: Custom Attributes .....	57
L3 VPN Form: QA Probes Tab .....	57

L3 VPN Form: Registration Tab .....	58
VRF Form .....	59
VRF Form: PE Interfaces Tab .....	63
VRF Form: CE Interfaces Tab .....	63
VRF Form: Neighbor VRFs Tab .....	64
VRF Form: Route Targets Tab .....	65
VRF Form: QA Probes Tab .....	65
VRF Form: MVRF Tab .....	67
VRF Form: Upstream MDTs Tab .....	67
VRF Form: Downstream MDTs Tab .....	68
VRF Form: Status Tab .....	68
VRF Form: MVRF Status Tab .....	69
VRF Form: Conclusions Tab .....	69
VRF Form: Incidents Tab .....	70
VRF Form: Custom Attributes .....	70
VRF Form: Registration Tab .....	71
MVPN Form .....	71
MVPN Form: MVRFs Tab .....	72
MVPN Form: MDTs Tab .....	73
MVPN Form: Status Tab .....	73
MVPN Form: Conclusions Tab .....	74
MVPN Form: Custom Attributes .....	74
MVPN Form: Registration Tab .....	75
PseudoWire VC Form .....	75
LSP-PseudoWire Mapping .....	76
PseudoWire VC Form: VC LSPs Tab .....	77
PseudoWire VC Form: Status Tab .....	77
PseudoWire VC Form: Conclusions Tab .....	78
PseudoWire VC Form: Incidents Tab .....	78
PseudoWire VC Form: Custom Attributes .....	79
PseudoWire VC Form: Registration Tab .....	79
VPLS VPN Form .....	79
VPLS VPN Form: VFIs Tab .....	80
VPLS VPN Form: PseudoWire VCs Tab .....	81
VPLS VPN Form: PE Routers .....	82
VPLS VPN Form: Status Tab .....	82
VPLS VPN Form: Conclusions Tab .....	83
VPLS VPN Form: Custom Attributes .....	84
VPLS VPN Form: Registration Tab .....	84
VFI Form .....	84
VFI Form: ACs tab .....	86
VFI Form: Neighbor VFIs tab .....	87
VFI Form: PseudoWire VCs tab .....	87
VPLS VPN Form: Route Targets Tab .....	88
VFI Form: SDP Binds tab .....	88
VFI Form: Status tab .....	88
VFI Form: Conclusions tab .....	89
VFI Form: Incidents tab .....	90

VFI form: Custom Attributes Tab .....	90
VFI Form: Registration tab .....	90
SDP Form .....	91
SDP Form: SDPbinds Tab .....	92
SDP Form: Status Tab .....	93
SDP Form: Conclusions Tab .....	94
SDP Form: Incidents Tab .....	95
SDP Form: Registration Tab .....	95
SDPBind Form .....	95
SDPBind Form: Status Tab .....	98
SDPBind Form: Conclusions Tab .....	99
SDPBind Form: Incidents Tab .....	99
SDPBind Form: Registration Tab .....	100
VPWS VPN Form .....	100
VPWS VPN Form: PseudoWire VC Tab .....	101
VPWS VPN Form: VC ID Tab .....	101
VPWS VPN Form: PE Routers Tab .....	101
VPWS VPN Form: Status Tab .....	102
VPWS VPN Form: Conclusions Tab .....	103
VPWS VPN Form: Custom Attributes .....	104
VPWS VPN Form: Registration Tab .....	104
TE Tunnel Form .....	104
TE Tunnel Form: Attributes Tab .....	106
TE Tunnel Form: Hops Tab .....	108
TE Tunnel Form: Status Tab .....	109
TE Tunnel Form: Conclusions Tab .....	110
TE Tunnel Form: Incidents Tab .....	110
TE Tunnel Form: Custom Attributes .....	111
TE Tunnel Form: Registration Tab .....	111
VC LSPs Form .....	112
VC LSP Form: ACs Tab .....	114
VC LSP Form: Status Tab .....	114
VC LSP Form: Conclusions Tab .....	115
VC LSP Form: Registration Tab .....	116
Monitored LSP Form .....	116
Monitored LSP Form: Status Tab .....	117
Monitored LSP Form: Conclusions Tab .....	118
Monitored LSP Form: Incident Tab .....	118
Interface Form .....	120
MDT Form .....	120
Node Form: VRF Tab .....	121
Node Form: TE Tunnel Tab .....	121
Node Form: PseudoWire VC LSP Tab .....	122
Node Form: VPLS VPNs Tab .....	122
Node Form: VPWS VPNs Tab .....	123
Node Form: L3 VPN PE Interfaces Tab .....	123
Node Form: LDP Attributes Tab .....	124
PE Interface Form: L3 VPN Tab .....	124

CE Interface Form: L3 VPN Tab .....	125
Viewing the NNM iSPI for MPLS Incidents .....	126
MPLS Incidents .....	127
Incidents Generated for MPLS-enabled Nodes and Objects .....	127
Service Impact Incidents .....	128
MPLS Pairwise Incidents .....	129
Viewing the MPLS SNMP Traps .....	129
Viewing the MPLS Topology Maps .....	132
TE Tunnel Path View .....	133
MPLS L3 VPN Topology View .....	135
Using the L3 VPN Map View Toolbar .....	137
MPLS Inter-Provider VPN Topology Map View .....	138
MPLS L2 VPN Topology View .....	138
MPLS Path View .....	141
LSP Path View .....	143
VRF-LSP Service Mapping .....	144
MPLS LDP Neighbors .....	144
IP Multicast Map View .....	146
IP Multicast Reverse Path View .....	147
MPLS Map Symbols .....	147
Monitoring Your Network by using the NNM iSPI for MPLS Global Network Manager .....	150
Duplicate IP Address Support with the NNM iSPI for MPLS .....	151
<b>Chapter 4: Help for NNM iSPI for MPLS Administrator .....</b>	<b>153</b>
Discovering Your Network .....	154
Configuring the NNM iSPI for MPLS .....	154
Configure the Polling Frequency .....	155
Configure the Exclude Route Targets .....	157
Configure the VPWS VPNs .....	158
Non-SNMP Framework and Blacklisted Devices .....	159
Configure Device Credentials .....	160
Wildcard Support for Device Authentication .....	161
Configure an MPLS Regional Manager Connection .....	163
Configure the NNM iSPI for MPLS Regional Manager Connection .....	164
Managing Nodes .....	165
NNM iSPI for MPLS System Health Report .....	166
Launching the MPLS Health Report .....	166
Using Single Sign-On with NNM iSPI for MPLS .....	167
Integrating the NNM iSPI for MPLS with Route Analytics Management Software (RAMS) .....	167
Integrating the NNM iSPI for MPLS with the iSPI for IP Multicast .....	168
Integrating the NNM iSPI for MPLS with the NNM iSPI Performance for QA (Quality Assurance) ...	169
Troubleshooting the NNM iSPI for MPLS .....	170
Glossary .....	173
Send Documentation Feedback .....	176

# Chapter 1: Network Node Manager iSPI for MPLS Software

The Network Node Manager iSPI for MPLS Software is a smart plug-in that is integrated with NNMi. For enterprises that work on MPLS network, the NNM iSPI for MPLS provides effective and user friendly ways of monitoring MPLS objects and services. After successful integration with NNMi, the NNM iSPI for MPLS is displayed as a separate workspace among the NNMi workspaces. (See, *About Workspaces* in *NNMi Online Help: Using the Console*). From this workspace you can access the MPLS Inventory. Each MPLS object has a separate inventory.

The NNM iSPI for MPLS discovers MPLS objects and services like Layer 3 Virtual Private Networks (L3 VPNs), Layer 2 Virtual Private Network (L2 VPNs), Multicast VPNs (MVPNs), PseudoWires (PW), TE Tunnels and Service Distribution Points (SDPs). In addition, discovers Label Switch Paths (LSPs) in MPLS core network. After the discovery, the NNM iSPI for MPLS monitors and generates incidents. The NNM iSPI for MPLS also provides visual representation of all the objects and services, enabling an operator or a network administrator to detect faults quickly and reduce the Mean Time to Repair (MTTR).

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

- Discovering and monitoring the Layer 3 Virtual Private Network (L3 VPNs) configured on the provider edge devices of the network.
- Discovering third-party Inter-Provider MPLS clouds, and discovering and monitoring Customer Edge (CE) routers at customer sites.
- Discovering and monitoring the Virtual Private LAN Service VPNs (VPLS VPNs) on the network.
- Discovering and monitoring the Virtual Private Wire Service VPNs (VPWS VPNs) on the network.
- Discovering and monitoring the TE tunnels on the network.
- Discovering and monitoring the PseudoWire VCs on the network.
- Discovering and monitoring Label Switch Paths (LSPs).
- Discovering and monitoring Service Distribution Points (SDPs) on the network.
- Discovering and monitoring the Provider Edge (PE) - Customer Edge (CE) relationship on 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.
- Visual representation of MPLS services and convenient troubleshooting of problems using graphical views provided by the NNM iSPI for MPLS.
- Investigating the problems of the network by viewing the incidents and service impact incidents.
- Configuring devices for non-SNMP framework support.
- Investigating incoming and outgoing traffic within an MPLS network by generating reports. This is only possible after you integrate the NNM iSPI for MPLS with NNM iSPI Performance for Metrics.
- Discovering and monitoring the Multicast VPNs (MVPNs) on the network by using the [NNM iSPI for IP Multicast capabilities](#) . This is only possible after you integrate the NNM iSPI for MPLS with NNM iSPI for IP Multicast.
- [Monitoring and troubleshooting an L3 VPN by using Route Analytics Management Software \(RAMS\) capabilities](#) . This is only possible after you integrate the NNM iSPI for MPLS with RAMS.



- [Setting up the MPLS related probes by using the NNM iSPI Performance for Quality Assurance \(QA\) capabilities](#) . By integrating with the NNM iSPI performance for QA you can manage end-to-end services on the MPLS nodes.

You can monitor your MPLS network by:

- Accessing form view of each MPLS object
  - A form view provides detailed information about MPLS objects.
  - Different tabs under each form make it easier for you to view specific data .
  - You can perform following tasks from the form views:
    - Access analysis pane (see, *About Analysis Pane in NNM Online Help: Using the console*).
    - Launch topology view, using **Actions** (see, *Actions Available in NNM iSPI for MPLS in NNM iSPI for MPLS Online Help*).
    - View incidents from the incidents tab.
- Launching Topology Map views for layer 3 and layer 2 topologies.  
A topology map view provides a visual representation of the MPLS network. You can launch a layer 3 or a layer 2 topology map to view the connectivity and status of each MPLS object or a service in the MPLS network.
- Viewing incidents generated for MPLS objects  
The NNM iSPI for MPLS actively notifies you when an important event occurs by generating incidents. You can troubleshoot your MPLS network based on incidents generated for MPLS objects and services.

The NNM iSPI for MPLS supports the following environments/frameworks:

- [Multitenant Architecture](#)
- Overlapping Address Domain

The NNM iSPI for MPLS supports the following device types:

- Cisco routers
- Cisco IOS-XR routers
- Juniper( M/T/J ) series routers
- Ericsson Redback
- Alcatel 7750 and 7710 series routers
- Huawei

For information about the supported combinations of devices for the NNM iSPI for MPLS objects and services, see *NNM iSPI for MPLS 10.00 Support Matrix* document.

After you install (and configure) the NNM 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 NNM iSPI for MPLS.

# Chapter 2: Understanding MPLS Objects

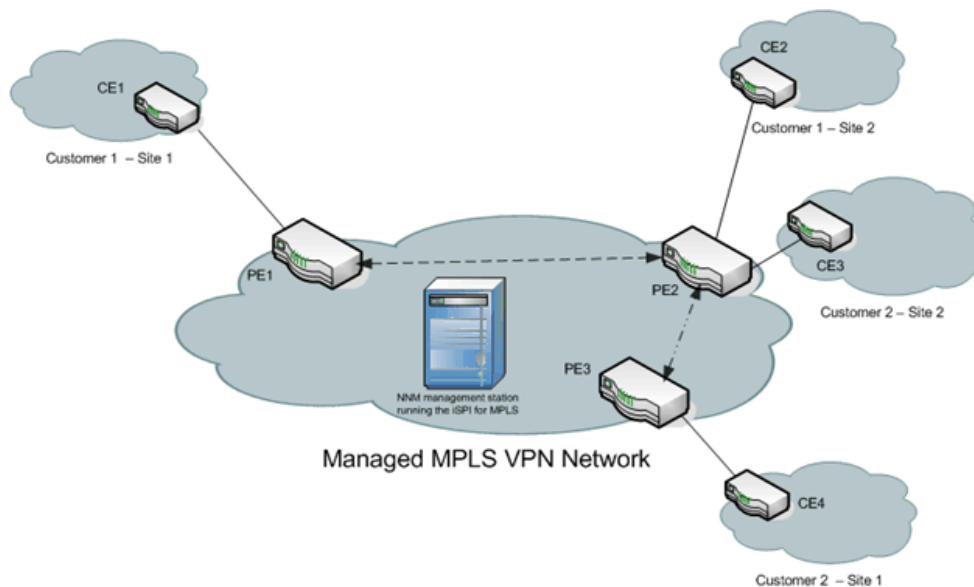
## MPLS L3 VPN

The NNM iSPI for MPLS helps you to monitor an L3 VPN services in MPLS network.

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 types of routers—routers inside the MPLS cloud that belong to the service Provider routers (P routers) and Customer Edge (CE) routers that are located and monitored 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 NNM iSPI for MPLS helps you to perform the following tasks:

### Monitor L3 VPNs and VRFs

You can discover the Virtual Routing and Forwarding (VRF) tables and Route Targets (RTs) participating to form an Layer 3 VPN on the network. A VPN is formed by the set of VRFs on a Provider 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 that VPN. 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 L3 VPN network such as the status of the VRF changing from *Up* to *Down* by using the NNM iSPI for MPLS views. The NNM iSPI for MPLS provides a quick way to view the enriched incidents that help you understand and resolve a problem in your network. For more information, see *MPLS Incidents*.

For more information about the L3 VPN, VRFs, Route Targets, and Shadow Routers, see *L3 VPN, VRF, Route Targets, VRF-Lite, and Shadow Routers*.

## L3 VPN, VRFs, VRF-Lite, Shadow Routers, and Route Targets

In a Multi-Protocol Label Switching network (MPLS network), Provider Edge (PE) routers communicate with each other by using the label-switched paths. Each PE router maintains a Virtual Routing and Forwarding (VRF) table to transfer traffic towards the correct Customer Edge (CE) router or on correct Label Switched Path (LSP). An L3 VPN is formed by a set of VRFs. A VRF can communicate with other VRFs on the network based on the Route Targets (RTs). All the VRFs that can communicate with each other, form an L3 VPN.

A Route Target (RT) identifies route import and export within VRFs that helps in routing traffic. Every VPN route is associated with one or more than one RT that is exported or imported from other VRFs.

A VRF-Lite router is a traffic classifier that is achieved on the CE by defining multiple VRFs. With VRF-Lite, multiple customers or different departments within the same organization, can share one CE, but only one physical link exists between the CE and the PE. The shared CE maintains separate VRF tables for each VPN. VRF-Lite extends limited PE functionality to a CE device by giving the CE the ability to maintain separate VRF tables.

A shadow router is a low-end router that offloads router testing work from the PE router. Like VRF-Lite, shadow routers extend PE functionality by giving limited workload capabilities to the shadow router connected to the PE.

### VRFs Grouping for an L3 VPN

Each VRF includes a list of import and export route targets that determine connection with other VRFs on the network. The NNM iSPI for MPLS reads the route targets from the import and export list to identify groups of VRF neighbors. A VRF exports its route targets to one or more 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.

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

You can opt to ignore the Route Targets by using the **MPLS Configuration** workspace. This results in regrouping of VRFs to form an L3 VPN in the next discovery cycle. In addition, the status of the L3 VPN is recomputed based on participating VRFs.

## L3 VPN Topology

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

- **Full-Mesh** - Full Mesh VPN is formed if all participating VRFs communicate with each other. This is achieved by each VRF exporting its route targets that are in turn, imported by all the other VRFs in same L3 VPN.
- **Isolated** - An isolated VPN has a single VRF participating to form an L3 VPN, in other words, Route Target (RT) exported by this VRF is not imported by any other VRFs neither does this VRF import any RTs from other VRFs participating to form the L3 VPN.
- **Hub and Spoke** - A hub and spoke VPN is a star-shaped topology where the Hub VRF is in the center. In a Hub and Spoke VPN, all spoke VRFs can only communicate with Hub-VRF directly.
- **Other** - Any VPN that does not match the above mentioned types is shown as 'Other'. For example, a hybrid topology.

## L3 VPN Naming

The NNM iSPI for MPLS uses the internal system naming convention to provide the L3 VPN names.

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

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 the Id
- If there is no common VRF name, the NNM iSPI for MPLS creates a new L3 VPN name based on the following rules:
  - If at least 65 percent of the VRFs in the group have the same name and the name is 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 the name is already a L3 VPN name for another VRF list, assign the L3 VPN name as the VRF name appended with an underscore followed by the VPN internal identification number for the 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	Green	Select the majority name.

### Examples, continued

VRFs in the VPN	Selected L3 VPN Name	Explanation
VRF 3- Green VRF 4- Green		
Red_East Red_West	Red	The common initial characters.

You can use the MPLS views to update the system-generated L3 VPN name.

#### To update the L3 VPN name, follow these steps:

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

#### VPWS VPN and VPLS VPN

The L2 VPN topology includes the VPLS VPNs and VPWS VPNs on 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. If any PseudoWire VC is not participating to form a VPLS or a VPWS, it appears under the **Default Group**.

## Inter-Provider VPN

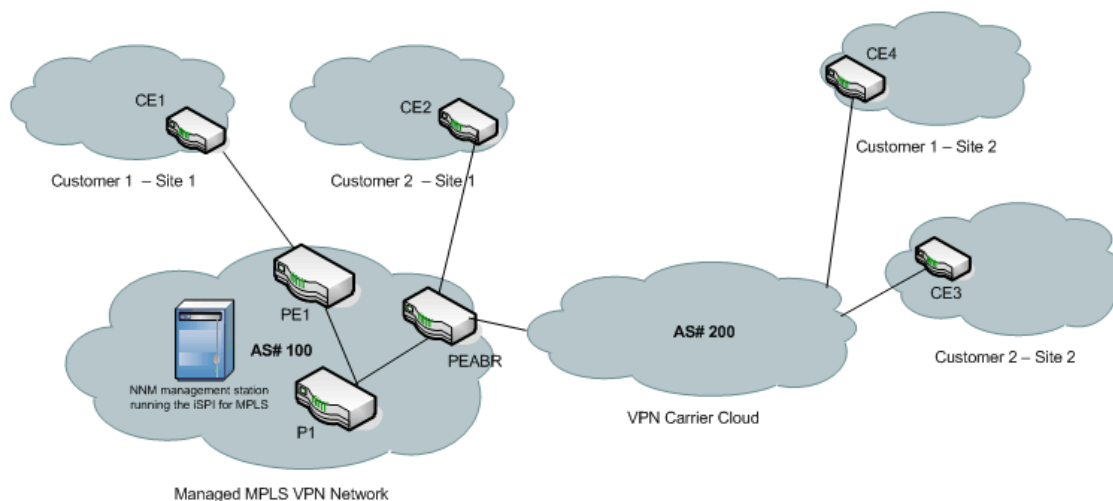
The NNM iSPI for MPLS supports Inter-provider VPN technology.

Inter-provider technology allows data transmission between MPLS VPN providers and CE routers residing in remote MPLS client sites by using a third-party VPN provider. PEs residing within the MPLS VPN provider, function as Area Border Routers<sup>1</sup> (ABRs). The LSP paths of these ABRs interconnect with the third-party MPLS network cloud through IP forwarding. The third party MPLS network cloud is called a carrier cloud. This carrier cloud is identified by a unique Autonomous System Number<sup>2</sup> (AS#) assigned to it.

<sup>1</sup>Area Border Routers connect the main backbone network to one or more areas.

<sup>2</sup>Autonomous System Numbers are IP routing prefixes designated by the Internet Assigned Numbers Authority (IANA).

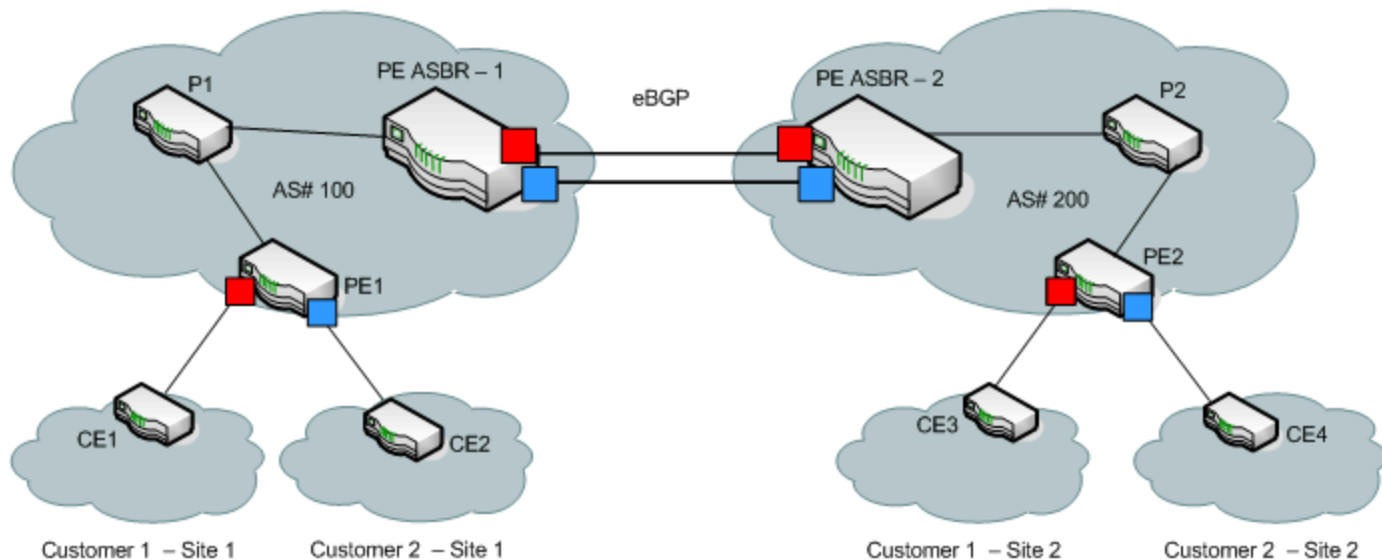
### Example of an Inter-Provider VPN



The NNM iSPI for MPLS supports Back-to-Back VRF methodology.

Back-to-Back VRF is one of the common implementations of the Inter-Provider VPN technology. A back to back VRF setup can have multiple carrier service provider networks (carrier clouds), each assigned with a unique AS#. PE routers residing within a carrier service provider network function as Autonomous System Boundary Routers<sup>1</sup> (ASBRs).

### Example of a Back-to-Back VRF Network



<sup>1</sup>An autonomous system boundary router is used to establish routes with external autonomous systems and carry out data transmission using Border Gateway Protocol (BGP)

The NNM iSPI for MPLS discovers CE nodes that are located outside the MPLS VPN Network. The NNM iSPI for MPLS detects and manages all the nodes participating in the back-to-back VRF setup. You can monitor the connectivity between the PE node residing in the MPLS VPN Network, the IP addresses and AS#s of carrier service provider network, and geographically dispersed CE nodes residing within the client sites. The NNM iSPI for MPLS helps you to view the following:

- PE-CE connectivity
- Name and AS# of the carrier service provider networks
- Next Hop IP
- Next Hop AS
- AS Path

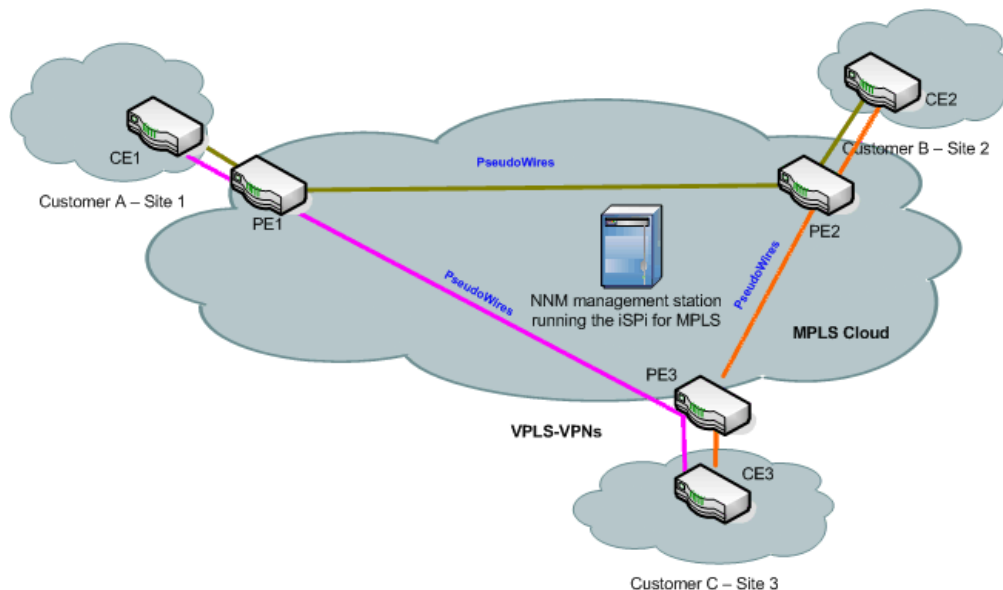
## MPLS L2 VPN

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

### Virtual Private LAN Service (VPLS VPN)

A VPLS VPN is formed by PseudoWire VCs with the same VPN ID. In a VPLS VPN or a Layer 2 VPN, 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) to communicate within the VPLS VPNs.

#### Example of a VPLS VPN

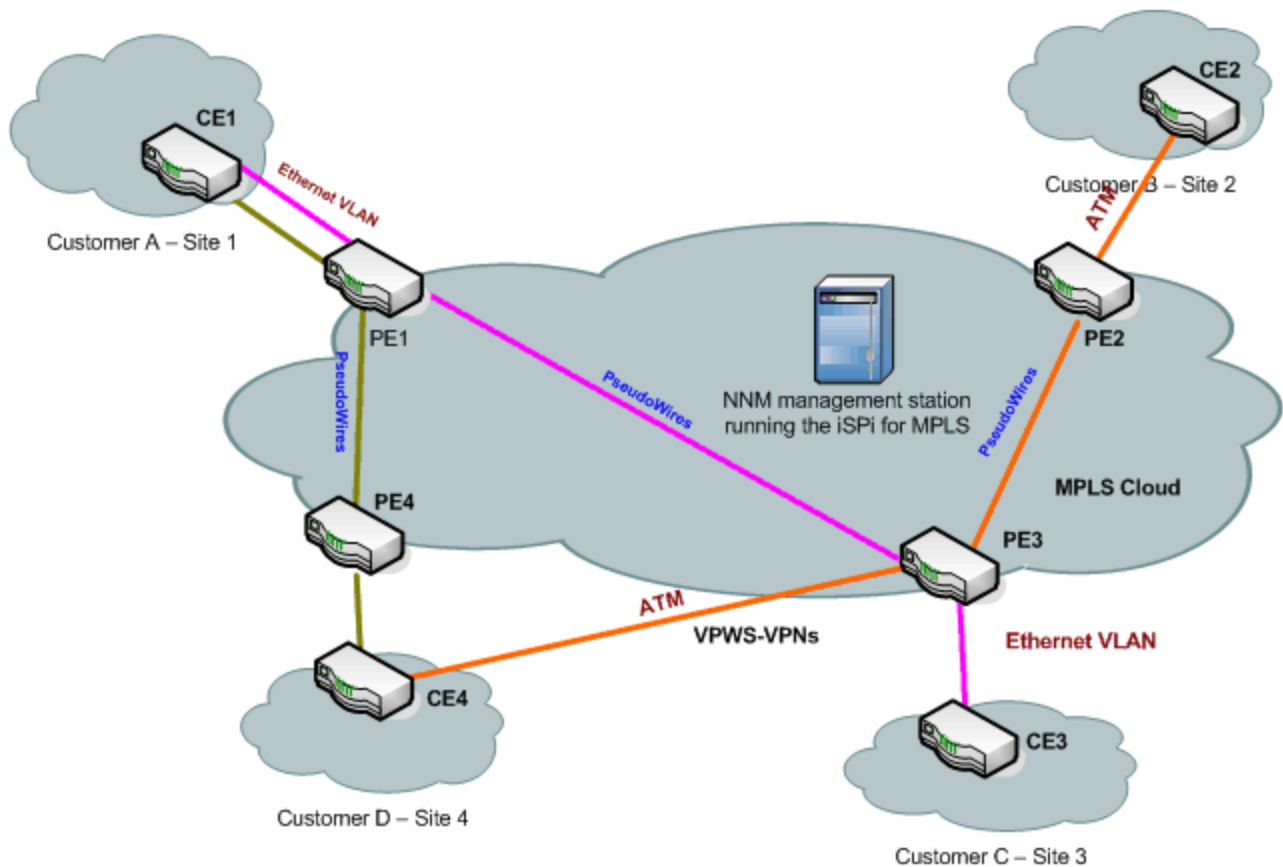


## Virtual Private Wire Service VPN (VPWS VPN)

A VPWS VPN is formed by VC LSPs with the same VPN ID. In a VPWS VPN or Layer 2 VPN, 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.

In a VPWS VPN or Layer 2 VPN, point-to-point link connects the CE devices through a Packet Switched Network (PSN) using PseudoWires VCs. You can change the configuration for the VPWS VPNs from the **MPLS Configuration** workspace.

### Example of a VPWS VPN



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

#### Monitor PseudoWire VCs

You can discover the PseudoWire VCs participating to form an L2 VPN. You can monitor and view the status of the L2 VPNs. You can navigate to L2 VPN forms to view the attributes and incidents-related to that L2 VPN.

In addition, you can monitor Attachment circuits (ACs), Virtual forwarding Interfaces (VFIs) for VPLS VPN and VPWS VPN. These VFIs are named as *L2VPNName@NodeName* and *GroupName@NodeName* respectively.

#### Manage Faults




You can detect the changes in the topology such as PseudoWire VC is *Down* or *Up* by using the NNM iSPI for MPLS views. In addition, the NNM iSPI for MPLS generates enriched incidents that help you understand and resolve a problem in your network. For more information, see *MPLS Incidents*.

### L2 VPN Renaming


The NNM 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. If any PseudoWire VC is not participating to form a VPLS or a VPWS, it appears under the **Default Group**.

#### To update the VPLS VPN name, follow these steps:

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

#### To update the VPWS VPN name, follow these steps:

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

## MPLS TE Tunnels

In MPLS network, you can setup Traffic Engineering tunnels for better quality of service between desired source and destination

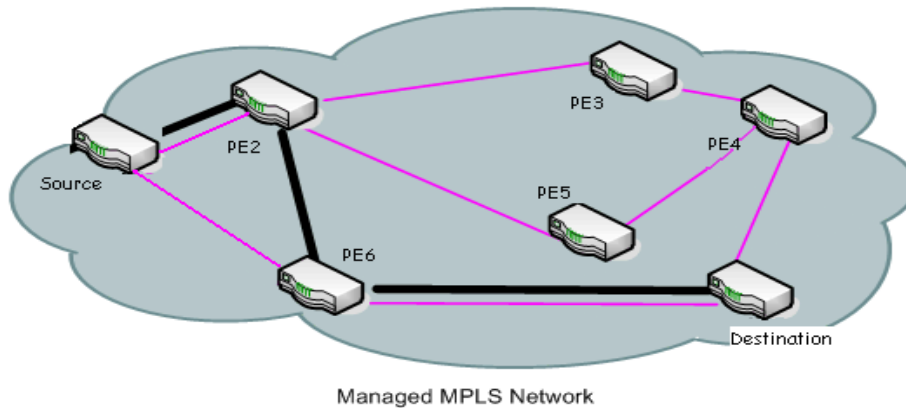
MPLS Traffic Engineering (MPLS TE) is the process of selecting and reserving the path between the nodes to optimize network resources for better bandwidth utilization and ensure better Quality of Service (QoS). Traffic Engineering (TE) is essential for service provider backbones. Usually, the shortest path is chosen for data transfer.

In an MPLS Traffic Engineering network, the routers can communicate by using TE tunnels. The TE Tunnels are one of the mediums through which you can manage the data transmission from a source to a destination as well as maintain a quality of service.

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. The network administrator configures the TE Tunnels to ensure the desired bandwidth usage and to provide better quality of service. Usually the shortest path is chosen for data transfer but TE tunnels allow traffic to be routed through a specific path (tunnel) thus, maintaining the required quality of service and bandwidth.

The NNM iSPI for MPLS discovers the TE tunnels in the MPLS core and provides a **TE Tunnel Inventory** with all the TE Tunnels discovered, along with their status. In addition, you can find the faults in MPLS traffic engineering tunnels using the **Incidents** and **Status** tabs.

### Example of the TE Tunnels on the network



 TE Tunnel

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

#### Monitor TE Tunnels

You can monitor using TE Tunnel inventory which lists all the discovered TE Tunnels with their status. Any change in TE tunnel would be indicated by the status on inventory. For further details on a particular TE Tunnel, you can open TE Tunnel form from the inventory to view the attributes and incidents related to the network. This helps in isolating a fault quickly and reduces the Mean Time To Repair (MTTR).

#### Manage Faults

You can detect the changes in the topology such as the status of the TE Tunnel changing from *Up* to *Down* or when it is Rerouted. The NNM iSPI for MPLS provides generates enriched incidents that help you understand and resolve a problem in your network. For more information, see *MPLS Incidents*.

## MPLS PseudoWire VC

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)<sup>1</sup> and Virtual Private LAN Service (VPLS)<sup>2</sup>. 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 VC 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) of the PseudoWire VC.

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

- **Monitor PseudoWire VC**

<sup>1</sup>A Virtual Private Wire Service VPWS is a point-to-point link through a packet switched network connecting two Customer Edge devices.

<sup>2</sup>A VPLS connects several LAN segments over a packet switched network (PSN).

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

- **Manage Faults**

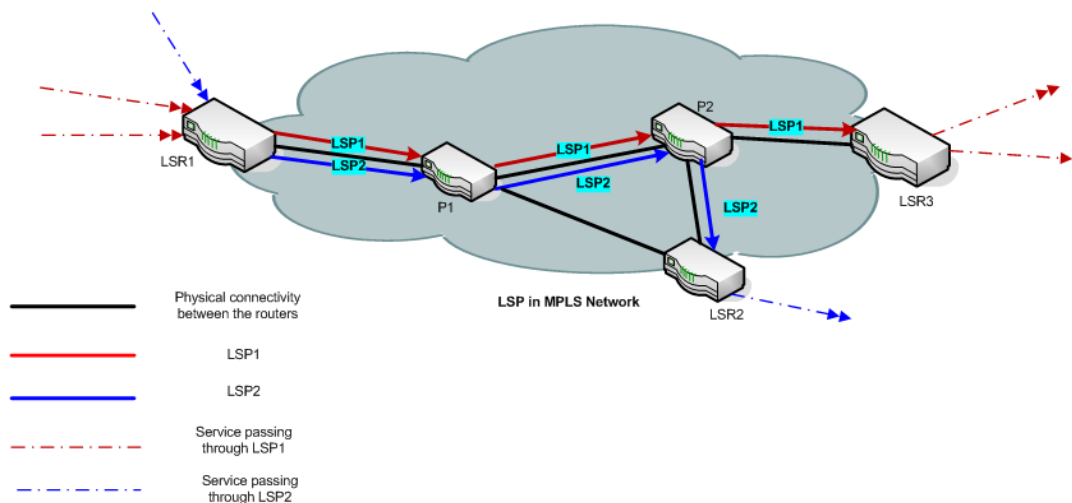
The NNM iSPI for MPLS identifies the changes in the topology such as the status of the PseudoWire VC is *Down*. The NNM iSPI for MPLS generates incidents that help you understand and resolve a problem in your network. For more information, see *MPLS Incidents*.

## Label Switch Path

Label Switch Paths (LSPs) play the most important role in data transfer within an MPLS network. LSPs are set up by Label Distribution Protocol (LDP) to trace a path from a source to destination device within an MPLS network. These source and destination devices are known as Label Switch Routers (LSRs) or Provider Edge (PE) routers. An LSP path originates from an Label Switched Path (LER) and based on the prefixed label, transfers the data to the intermediate router in the path. The intermediate routers are also known as Provider Routers (P Routers). When a P Router receives a data packet, it swaps the prefix label and pushes the data forward to the next P Router. This process continues till the data reaches the destination LER. The destination LER then drops the label.

The NNM iSPI for MPLS services utilize LSPs and therefore, any impact on LSP has a direct effect on these services. The NNM iSPI for MPLS has introduced Service Mapping. Service Mapping is where, an LSP path can be traced between various services residing on two different MPLS-enabled nodes. Using the NNM iSPI for MPLS, you can discover LSPs in MPLS core network and monitor MPLS services for to determine any service impact because of LSP related issue.

### Example of a Label Switch Path



In the example above, there are two LSPs passing through an MPLS cloud. The first one connects the the Edge Routers LER1 and LER3 by passing through P Routers (P1 and P2). The second originates from edge router LER1 and passes through the P Routers P1 and P2, and ends at Edge Router LER2. In this example, LSP1 is mapped to two services and LSP2 is mapped to one service.

## LSP Service Mapping

In addition to discovering the LSPs in core MPLS network, iSPI for MPLS also maps these LSPs to respective layer 3 and layer 2 services. This LSP service mapping is useful to detect impacts on these services caused because of faults in the core (corresponding LSP).

### **Prerequisite to Enable LSP Mapping:**

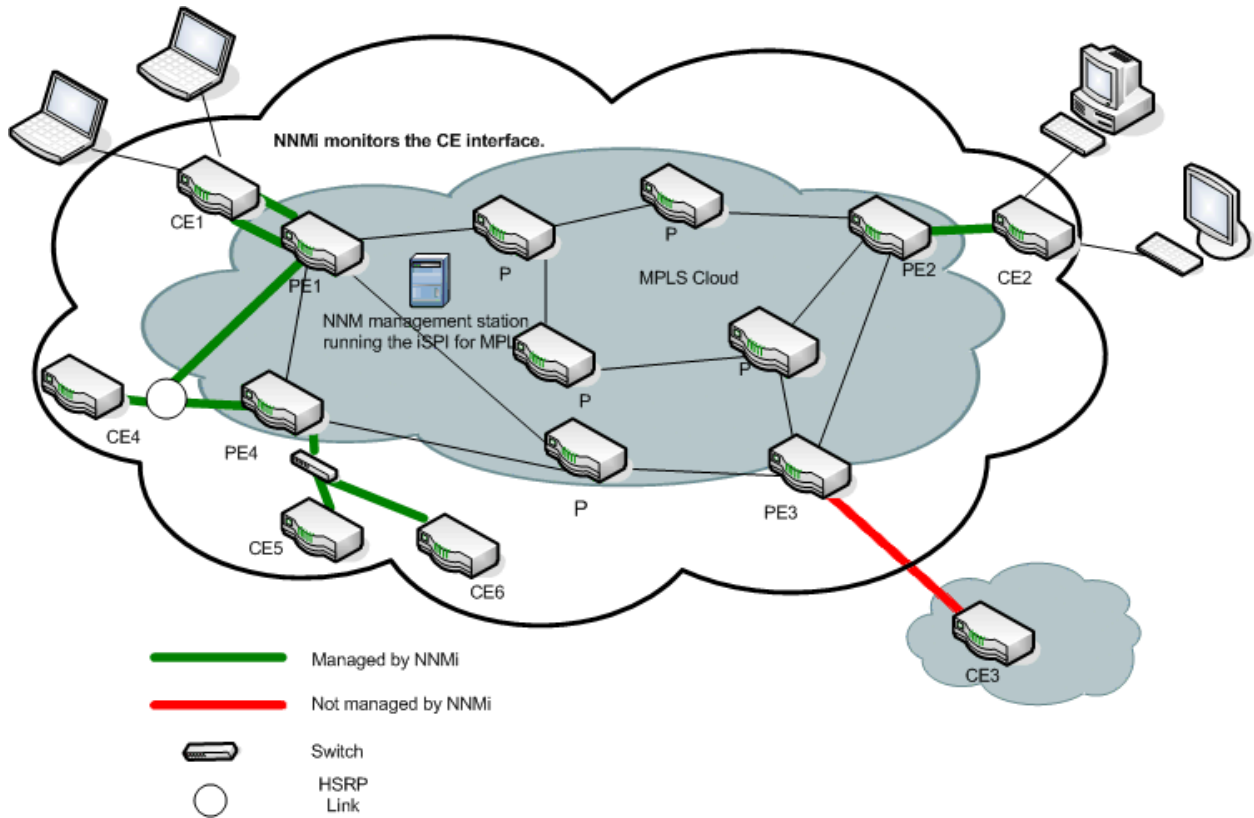
LSP service mapping is available for services configured on LSRs for which, SSHv2 credentials are provided in **iSPI for MPLS Configuration** under **Configuration** workspace. For more information about how to configure devices, see *Configure Device Credentials*.

## MPLS Customer Edge (CE) Management

You can monitor the logical link connectivity between the PE node and CE node in an L3 VPN topology. The NNM iSPI for MPLS helps you monitor the following:

- One PE interface connected to one CE interface on the network.
- One PE interface connected to multiple CE interfaces on the network. This PE-CE links are connected by using a hub on the network.
- Multiple PE interfaces connected to one CE interface on node on the network. This PE-CE link connectivity is using the Hot Standby Routing Protocol (HSRP) or equivalent.
- Multiple PE interfaces connected to multiple CE interfaces on the network.

### Example of the PE - CE connectivity on the network



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

You can 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*.



The discovery of CE nodes participating in an L3 VPN 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 NNM iSPI for MPLS.

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

The NNM 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 NNM iSPI for MPLS listens to the incident and updates the status of the CE interface in the MPLS views.

To use the CE management feature, 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 or edit an interface group to include the MPLS PE and CE capabilities from NNMi Configuration workspace:

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).
4. In the Interface Group form, select the **Additional Filters** tab.
5. Add the following MPLS capability to monitor the PE interfaces `capability = com.hp.mpls.capability.iface.l3vpnpeiface`.
6. Add the following MPLS capability to monitor the CE interfaces `capability = com.hp.mpls.capability.iface.l3vpnceiface`.
7. 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*.

## Multitenant Architecture

The NNM iSPI for MPLS, in conjunction with HPE Network Node Manager supports Multitenant architecture. You can create Tenants or partition your network across multiple users. A tenant can also be defined as a security group to which a node or an MPLS object belongs. As an administrator, you can restrict operators to view and control a set of nodes and MPLS objects, if they do not belong to the same security group as that of this set.

As a tenant, a user can view all the nodes and MPLS objects participating in a network in the map view. However, the inventory and the form views will display only those objects that the user has permission to access. For example, if a user has access to three nodes out of five in a network, the map view will show the five nodes, however the other two nodes are not 'clickable' and no information is available for those two nodes. Moreover, the inventory and form view will list only three accessible nodes.

Following is the list of the NNM iSPI for MPLS objects supporting multitenant architecture:

- *TE Tunnel Inventory*: A user can monitor only those tunnels that are associated with the nodes in the user's security group
- *VRF Inventory in VPN*: A user can monitor only those VRFs that are associated with the nodes in the user's security group
- *VRF neighbors in VRF*: A user can monitor only those VRFs that are associated with the nodes in the user's security group
- *VPN Inventory*: A user can monitor a VPN, if at least one VRF participating in that VPN belongs the user's security group
- *PseudoWire Inventory*: A user can monitor only those PseudoWire virtual circuits (VCs) that are associated with the nodes in the user's security group

- *VPLS Inventory*: A user can monitor a VPLS if at least one PsuedoWire VC participating in that VPLS are associated with the nodes in the user's security group
- *VPWS Inventory*: A user can monitor a VPWS if at least one PsuedoWire VC participating in that VPWS are associated with the nodes in the user's security group
- *Monitored LSP Inventory*: A user can monitor only those LSPs that are associated with the nodes in the user's security group
- *SDP Inventory*: A user can monitor only those SDPs that are associated with the nodes in the user's security group
- *Maps*: For L3 VPN, L2 VPN, LSP, TE Tunnel path, a user can view all the nodes participating in the VPN or TE tunnel but can monitor only those nodes that belong to the user's security group

Security group is also applicable to incidents, MPLS related probes (applicable only if, the NNM iSPI for MPLS is integrated with NNM iSPI Performance for QA), and reports. This means, a user can view incidents for accessible objects, probes for accessible VRFs, and reports for accessible nodes alone.

Multi tenancy can be configured in NNMi workspace through **Configuration** -> **Security**. For more details, see Online Help for NNMi.

# Chapter 3: Help for NNM iSPI for MPLS Operators

The NNM iSPI for MPLS helps you monitor, detect, and troubleshoot abnormal behavior on the network.

To perform a basic monitoring of the MPLS services on 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 NNM iSPI for MPLS. MPLS capabilities on node discovered by NNMi, build various relationships among them to determine various MPLS services and present them to operator. You can access the MPLS views for visual representation of the MPLS network topology and to monitor the status and necessary details for all the MPLS objects.

The following table describes tasks you can perform.

Task	Help Topics
Monitoring your network with MPLS Inventories	After successful integration with NNM, NNM iSPI for MPLS is displayed as a separate workspace among the NNM workspaces. (See, <i>About Workspaces</i> in <i>NNM Online Help: Using the Console</i> ). From this workspace you can access the MPLS Inventory. Each MPLS object has a separate inventory. For more information, see <a href="#">Monitoring Your MPLS Inventory</a> .
Monitoring your network with MPLS Forms	A form view provides detailed information about MPLS objects. Different tabs under each form make it easier for you to view specific data. You can perform following tasks from the form views: <ul style="list-style-type: none"><li>• Access analysis pane (see, <i>About Analysis Pane</i> in <i>NNM Online Help: Using the console</i>)</li><li>• Launch topology view, using <b>Actions</b> (see, <i>Actions Available in NNM iSPI for MPLS</i> in <i>NNM iSPI for MPLS Online Help</i>.)</li><li>• View incidents from the incidents tab in each form</li></ul> For more information, see <a href="#">Viewing MPLS Forms</a> .
Viewing the MPLS incidents	For more information, see <a href="#">Viewing the MPLS</a> .
Viewing the topology maps	For more information, see <a href="#">Viewing the MPLS Topology Maps</a> .

## Monitoring Your Network with MPLS Inventory

**Note:** Before you begin with this topic, see *Learning Your Network Inventory* in the *NNM Online Help: Help for Operators*.



After the discovery of the MPLS-enabled nodes, you can access the MPLS views to monitor the status and check the attributes of the MPLS devices.

The NNM iSPI for MPLS adds a new workspace to the NNMi console—the **MPLS** workspace. You can access all the MPLS Inventories from the **MPLS** workspace. The MPLS Inventories 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 Inventories to access the device details.

View Type	Purpose
LSR( Label-Switched Routers) Inventory	Lists all the MPLS-enabled routers managed by the NNM 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 L3 VPNs on the network.
MVPN Inventory	Provides a list of available MVPNs on the network.
VPLS VPN Inventory	Provides a list of available VPLS VPNs on the network.
VPWS VPN Inventory	Provides a list of available VPWS VPNs on the network.
PseudoWire VC Inventory	Provides a list of available PseudoWire VCs on the network.
TE Tunnel Inventory	Provides a list of available Traffic Engineering (TE) tunnels on the network.
Monitored LSP Inventory	<p>Provides a list of monitored LSPs on the network.</p> <p>Monitoring LSPs is different from discovering LSPs in a network. LSPs are discovered in a network irrespective of being monitored or not.</p>
SDP (Service Distribution Point) Inventory	Provides a list of available SDPs on the network.

**To launch the MPLS specific views, follow these steps:**

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

Use the LSR inventory for the following tasks:

- Monitor the LSR routers on the network.
- Check the status of the LSR routers.
- View the LSR nodes and resolve problems, if any, on the network.
- Access the MPLS Path view.
- Navigate to the node form to check the other attributes of the node.

### Basic Attributes

Attribute	Description
Status	<p>The status of the selected LSR. Possible values are:</p> <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul>
Hostname	The name of the router as set by the network administrator.
Device Profile	The device and vendor information of the LSR.
L3 VPN-PE	If the selected MPLS-enabled router participates to form an 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  .
Device Access Mode	<p>Displays the mode of access to a Non-SNMP connection. The possible values are as follows:</p> <ul style="list-style-type: none"> <li>• <b>SNMP, SSHv2</b> - Indicates that the node uses SNMP as well as SSHv2 connections. SSHv2 connection to collect the CLI data.</li> <li>• <b>SNMP, Telnet</b> - Indicates that the node uses SNMP as well as Telnet connections. Telnet to collect the CLI data. This is possible only if Telnet is enabled for the corresponding device. For more information, see <a href="#">Configure Device Credentials</a> and <a href="#">Switch Device Access Mode</a>.</li> </ul>

### Basic Attributes, continued

Attribute	Description
	<ul style="list-style-type: none"><li>• <b>SNMP</b>- Indicates that the node is not connecting CLI data.</li></ul> <p><b>Note:</b> After you upgrade to the NNM iSPI for MPLS 10.10 from 10.00, the values for all the LSR nodes are set to default as "SNMP". In the next discovery cycle, the device access mode values will be updated to the applicable Access Mode for the corresponding LSR node.</p>

### Sort Column Data

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

- Hostname
- L3 VPN-PE
- L2VPN- PE
- TE Tunnel Head
- Device Access Mode

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

Also see, [To Launch LSP Path View](#)

## Actions Available in LSR Inventory

**To Launch MPLS LDP Neighbors View, follow these steps:**

1. Select the LSR for which you want to launch the map.
2. Click **Actions**.
3. Click **MPLS LDP Neighbors**.

**To Launch MPLS Path View, follow these steps:**

Follow these steps to launch MPLS Path View:

1. Select the LSR for which you want to launch map.
2. Click **Actions**.
3. Click **MPLS Path View**.

### Switch Device Access Mode

NNM iSPI for MPLS can connect to the devices within the MPLS network through non-SNMP mode using SSHv2 or Telnet (for more information, see [Configure Device Credentials](#)). You can use Switch Device Access Mode to switch SSHv2 and Telnet for individual devices. To make the switch, follow this step:

- Click **Actions** -> **Switch Device Access Mode**. A window opens that provides the details about the previous and the current access mode for the selected node.

**Note:** Switching between SSHv2 and Telnet is only possible if Telnet is enabled for the select node.

### NNM iSPI for MPLS Node Group filter

You can use the Node group filter option to view the MPLS LSR nodes belonging to the node group of your choice. To perform, follow these steps:

1. Create a node group for the NNM iSPI for MPLS enabled devices.
2. Add the devices that you want to view, to this group.

For more information, see *Create Node groups* in *HPE NNMi Online Help for Administrators*.

To view the LSR nodes belonging to the node group of your choice, follow these steps:

1. From the **Workspace** navigation pane, click MPLS -> LSR Inventory.
2. Click the NNMi Node Group filter drop down option. The autocomplete feature is enabled for this field. For more information on autocomplete feature, see *Use Autocomplete* section under the *HPE NNMi Online Help for Administrators*.
3. Select the created node group from the drop down list.
4. The LSR nodes belonging to the selected node group will be displayed.

### Analysis Pane

Information shown in the Analysis Pane of LSR Inventory is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.







## L3 VPN Inventory

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






Use the L3 VPN Inventory for the following tasks:

- View and check the status of the available L3 VPNs on 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 any particular VPN.

### Basic Attributes

Attribute	Description
Status	<p>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:</p> <ul style="list-style-type: none"><li> <b>No Status</b> - L3 VPN is newly formed and not polled; status of the L3 VPN is No Status. Alternatively, when all the VRFs participating to form an L3 VPN are in a Not Managed mode, the derived status of the VPN is No Status.</li><li> <b>Normal</b> - The status of all the VRFs participating in the L3 VPN is Normal.</li><li> <b>Unknown</b> - The status of all the VRFs participating in the L3 VPN is Unknown.</li><li> <b>Warning</b> - The status of one or more VRFs participating in the L3 VPN is Unknown, however none of them is Critical.</li><li> <b>Minor</b> - The status of one or more, but not all, of the VRFs participating in the L3 VPN is Critical.</li><li> <b>Critical</b> - The status of all the VRFs participating in the L3 VPN is Critical.</li></ul>

### Basic Attributes, continued

Attribute	Description
	<p><b>Note:</b>The status computation of VPN does not include the status of the VRF Lites present in that VPN and VPNs that are not managed.</p>
Name	<p>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  (the <b>Save and Close</b> button) to update the L3 VPN Name.</p> <p>For more information about L3 VPN naming rules, see <i>L3 VPN, VRF, and Route Targets</i>.</p>
VPN Type	<p>The type of connectivity within a VPN. Possible values are:</p> <p><b>Full Mesh</b> - Full Mesh VPN is formed if all PE routers communicate with each other. In addition, 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.</p> <p><b>Isolated</b> - A single VRF forms a single L3 VPN. This VRF does not import or export the route targets from any other VRF.</p> <p><b>Hub and Spoke</b> - A hub and spoke VPN is a star-shaped topology where the Hub VRF is in the center. In a Hub and Spoke VPN, all spoke VRFs communicate with each other by using the Hub-VRF.</p> <p><b>Other</b> - All the VRFs are not communicating with other VRFs belonging to a VPN. For example, hybrid topology.</p> <p><b>Ungrouped VRFs</b> - A VPN formed by VRFs that do not have any Route Targets. In Ungrouped VRFs all Route Targets are excluded.</p>
Number of VRFs	<p>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.</p>
Multicast-Enabled	<p>When the Multicast-enabled router participates to form an L3 VPN and is capable to transmit multicast packets, this value is true. The possible values are true or false. True is represented by .</p>
IPv6 Enabled	<p>When the router participating to form an L3 VPN is IPv6 enabled, this value is true. The possible values are true or false. True is represented by .</p>
Status Last Modified	<p>The status of an L3 VPN is calculated whenever there is a change in topology. The Status Last Modified shows date and time on which the status was last set.</p>
Management Mode	<p>Management mode of the selected VPN. Possible values are:</p> <p> <b>Managed</b> - The selected VPN is managed.</p> <p> <b>Not Managed</b> - The selected VPN is not managed.</p>

### Filter by Attribute Value

The filter option is available on the following attributes:

- Status
- Name
- VPN Type
- Management Mode

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

**To create, modify, or remove filter in the MPLS L3 VPN view:**

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
- Management Mode

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

**Monitoring LSPs**

In addition to monitoring LSRs, NNM iSPI for MPLS monitors LSPs. To enable monitoring LSPs, follow one of the following set of steps:

- [To monitor LSPs from L3 VPN Inventory, follow these steps:](#)
  - a. Click **L3 VPN Inventory** from the **MPLS** workspace.

- b. Select an L3 VPN and open the **L3 VPN** form.
- c. Click  available under the **VRF** tab to open all the VRFs of the L3 VPN in a new window.
- d. Select two VRFs to determine which LSP you want to monitor.
- e. Click **Actions**.
- f. Click **Monitor LSP**.

Similarly, from the L3 VPN topology view you can monitor LSP:

- a. Launch L3 VPN topology view.
- b. Select two VRFs to determine which LSP you want to monitor.
- c. Click **Actions**.
- d. Click **Monitor LSP**.

- **To monitor LSPs from PseudoWire Inventory**

- a. Click **PseudoWire VC Inventory** from the **MPLS** workspace.
- b. Select a PseudoWire VC.
- c. Click **Actions**.
- d. Click **Monitor LSP**.

In addition, you can monitor LSPs from the VC LSPs tab in the PseudoWire VC form:

- a. Select a PseudoWire VC and open the PseudoWire VC form.
- b. Select a VC LSP.
- c. Click **Actions**.
- d. Click **Monitor LSP**.

The monitored LSPs can be viewed in the [Monitored LSP Inventory](#).

**Note:** MPLS LSP Path View shows the source LSR and destination LSR connected by a cloud, if no LSP path exists or discovered between the two selected nodes.

### Analysis Pane

Analysis Pane displays a quick summary of a particular object without opening a form view. The **Analysis Pane** remains blank until an object is selected in the inventory.

The following information is shown in the **Analysis Pane** of L3 VPN Inventory:

- Status
- Create Time
- Custom Attributes
- Management Type
- Management Mode
- **VRF Status Pie Chart** Tab- Shows Pie Chart that represents the status of all the VRFs participating to form the selected L3 VPN

For more information on how to access Analysis Pane, see *About Analysis Pane* in *NNMi Online Help*.







# MVPN Inventory

The MVPN inventory view provides a list of layer 3 Virtual Private Network (VPNs) with multicast services on 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 on the network.
- View the problem MVPNs on the network. Check the status of the available MVPNs on 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 of any particular MVPN.
- Access a map view of an MVPN.

## Basic Attributes

Attribute	Description
Status	<p>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:</p> <ul style="list-style-type: none"> <li> <b>Normal</b> - The status of all the MVRFs participating in the MVPN is Normal.</li> <li> <b>Unknown</b> - The status of all the MVRFs participating in the MVPN is Unknown.</li> <li> <b>Warning</b> - The status of one or more MVRFs participating in the MVPN are Unknown, but none of them is Critical.</li> <li> <b>Minor</b> - The status of one or more, but not all, MVRFs participating in the MVPN is Critical.</li> <li> <b>Critical</b> - The status of all the MVRFs participating in the MVPN is Critical.</li> </ul> <p><b>Note:</b> The status computation of MVPN does not include the status of MVPNs that are not managed.</p>
Name	<p>The system-generated name of the selected MVPN. Update the system-assigned MVPN name from the MVPN form. Type the new name in the <b>Name</b> box. Click  (the <b>Save and Close</b> icon) to update the MVPN Name. For more information about the MVPN naming rules, see <a href="#">MVPN Naming Rules</a>.</p>
L3 VPN Name	<p>The selected MVPN is a part of the named L3 VPN.</p>
Default MDT	<p>The Default MDT ( Multicast Distribution Tree) is the MDT group address used for forwarding multicast packets in an MVPN network.</p>
Number of MVRFs	<p>The total count of MVRFs participating to form an MVPN. The MVRF is the multicast-enabled VRF which participates to form an MVPN.</p>
Status	<p>Shows date and time on which the status was last set.</p>



## Basic Attributes, continued

Attribute	Description
Last Modified	

### 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 NNM 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
- L3 VPN Type

- Default MDT
- Status Last Modified

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

### Analysis Pane

Analysis Pane displays a quick summary of a particular object without opening a form view. The **Analysis Pane** remains blank until an object is selected in the inventory.

The following information is shown in the **Analysis Pane** of MVPN Inventory:

- Status
- Create Time
- L3VPN Name
- Custom attributes
- **MVRF Status Pie Chart** Tab- Shows Pie Chart that represents the status of all the MVRFs participating to form the selected MVPN

For more information on how to access Analysis Pane, see *About Analysis Pane* in *NNMi Online Help*.






## VPLS VPN Inventory

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





Use the MPLS VPLS VPN Inventory for the following tasks:

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

### Basic Attributes

Attribute	Description
Status	<p>The status of the VPLS VPN is derived and calculated based on the status of all the VFIs participating in the VPLS VPN. Possible values are:</p> <ul style="list-style-type: none"> <li> <b>No Status</b> - A VPLS VPN is newly formed and not polled, status of the L2 VPN is No Status. When all the VFIs participating to form an L2VPN are in a Not Managed mode, the derived status of the VPN is No Status.</li> <li> <b>Normal</b> - The status of all the VFIs participating to form a VPLS VPN is Normal.</li> <li> <b>Unknown</b> - The status one or more of all the VFIs participating to form a VPLS VPN is Unknown.</li> <li> <b>Warning</b> - The status of one or more VFIs participating to form a VPLS VPN is Unknown but, none of them is Critical.</li> <li> <b>Minor</b> - The status of one or more VFIs participating to form a VPLS VPN is Critical.</li> </ul>

### Basic Attributes, continued

Attribute	Description
	<p> <b>Critical</b> - The status of all the VFIs participating in a VPLS VPN is Critical.</p> <p><b>Note:</b> The status computation of VPLS VPN does not include the status of VPLS VPNs that are not managed</p>
L2VPN Name	The system-assigned name of the selected VPLS VPN. For example, VPLS_200 is the name of the VPLS VPN and VPN Id is 200. You can change the system-assigned VPN Name from the VPLS VPN form. Type the new name in the <b>Name</b> box. Click  (the <b>Save and Close</b> icon) to update the L2VPN Name.
VPN ID	The unique identifier of the selected VPLS VPN. This field is set to N/A for a BGP-based VPLS.
Number of VFIs	The count of the VFIs participating to form VPLS VPN.
Number of PseudoWiresVCs	The count of the PseudoWires VCs participating to form a VPLS VPN.
Status Last Modified	The status of the VPLS VPN is calculated whenever there is a change in topology. The status Last Modified shows date and time on which the status was last set.
Management Mode	Management mode of the selected VPLS VPN. Possible values are:  <b>Managed</b> - The selected VPLS VPN is managed.  <b>Not Managed</b> - The selected VPLS VPN is not managed.

### Filter by Attribute Value

The filter option is available on the following attributes:

- Status
- L2VPN Name
- VPN ID

**Note:** VPN ID is set to N/A for a BGP-based VPLS.

- Management Mode

You can create, change, or remove a filter at any time. The NNM 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 Inventory view:**

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
- Management Mode

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

### To launch Topology View

Follow these steps to launch VPLS VPN topology view:

1. Select a VPLS VPN for which you want to launch the topology view.
2. Click **Actions**.
3. Click **MPLS L2 VPN Topology View**.

**Note:** You can also right-click the selected VPLS VPN and select **MPLS L2 VPN Topology View** to launch the map view.

### Analysis Pane

Analysis Pane displays a quick summary of a particular object without opening a form view. The **Analysis Pane** remains blank until an object is selected in the inventory.

The following information is shown in the **Analysis Pane** of VPLS VPN Inventory:

- Create Time
- Status
- Custom Attributes
- Management Type
- Management Mode
- **PseudoWire VC Status Pie Chart** Tab- Shows Pie Chart that represents the status of all the PseudoWire VCs participating to form the selected VPLS VPN.
- **VFI Status Pie Chart** Tab- Shows Pie Chart that represents the status of all the VFIs participating to form the selected VPLS VPN.

For more information on how to access Analysis Pane, see *About Analysis Pane* in *NNMi Online Help*.







## VPWS VPN Inventory

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




Use the MPLS VPWS VPN Inventory for the following tasks:

- Monitor the VPWS VPNs on the network.
- View the problem VPWS VPNs on 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	<p>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:</p> <ul style="list-style-type: none"> <li> <b>No Status</b> - 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 Not Managed mode, the derived status of the VPWS VPN is No Status.</li> <li> <b>Normal</b> - The status of all the PseudoWires VCs participating to form a VPWS VPN is Normal.</li> <li> <b>Unknown</b> - The status of all the PseudoWires VCs participating to form a VPWS VPN is Unknown.</li> <li> <b>Warning</b> - The status of one or more PseudoWires VCs participating to form a VPLS VPN is Unknown, but none of them is Critical.</li> <li> <b>Minor</b> - The status of one or more PseudoWires VCs participating to form a VPWS VPN is Critical.</li> <li> <b>Critical</b> - The status of all the PseudoWires VCs participating to form a VPWS VPN is Critical.</li> </ul> <p><b>Note:</b> The status computation of VPWS VPN does not include the status of VPWS VPNs that are not managed.</p>
L2VPN Name	The system-generated name of the selected VPWS VPN. You can update the system-

### Basic Attributes, continued

Attribute	Description
	generated L2VPN Name from the VPWS VPN form. Type the new name in the <b>Name</b> box. Click  (the <b>Save and Close</b> icon) to update the L2VPN Name.
Number of PseudoWires VCs	Lists the count of the PseudoWires VCs participating to form a VPWS VPN.
Status Last Modified	The status of the VPWS VPN is calculated whenever there is a change in topology. Status Last Modified shows date and time on which the status was last set.
Management Mode	Management mode of the selected VPWS VPN. Possible values are:  <b>Managed</b> - The selected VPWS VPN is managed.  <b>Not Managed</b> - The selected VPWS VPN is not managed.

### Filter by Attribute Value

The filter option is available on the following attributes:

- Status
- L2VPN Name
- Management Mode

You can create, change, or remove a filter at any time. The NNM 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:

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
- Management Mode

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

### To launch Topology View

Follow these steps to launch VPWS VPN topology view:

1. Select a VPWS VPN for which you want to launch the topology view.
2. Click **Actions**.
3. Click **MPLS L2 VPN Topology View**.

**Note:** You can also right-click the selected VPWS VPN and select **MPLS L2 VPN Topology View** to launch the map view.

### Analysis Pane

Analysis Pane displays a quick summary of a particular object without opening a form view. The **Analysis Pane** remains blank until an object is selected in the inventory.

The following information is shown in the **Analysis Pane** of VPWS VPN Inventory:

- Create Time
- Status
- Custom Attributes
- Management Type
- Management Mode
- **PseudoWire VC Status Pie Chart** Tab- Shows Pie Chart that represents the status of all the PseudoWire VCs participating to form the selected VPWS VPN

For more information on how to access Analysis Pane, see *About Analysis Pane* in *NNMi Online Help*.




## PseudoWire VC Inventory

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

Use the PseudoWire VC Inventory for the following tasks:



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

### Basic Attributes

Attribute	Description
Status	<p>Overall status of the PseudoWire VCs. Possible values are :</p> <ul style="list-style-type: none"> <li> <b>Normal</b> - The status of both the LSPs (Label Switched Path) is Normal.</li> <li> <b>Critical</b> - The status of any one or both the LSPs is Critical.</li> <li> <b>Unknown</b> - The status of any one or both the LSPs is Unknown.</li> </ul>
Id	The unique index ID for each virtual circuit.
Encapsulation Type	<p>The kind of service carried in the specific PseudoWire VC. For example, the services are ATM, Frame Relay, Ethernet VLAN, or Ethernet.</p> <p>If both the endpoints (PE1 and PE2) are discovered but the status of LSPs is not Normal, the value of Encapsulation Type is <b>Other</b>.</p>
PE 1	<p>The name of the PE router. The selected router is one of the endpoints of the PseudoWire VC.</p> <p>If the status of PE1 is unknown, not managed, 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.</p>
PE 1 Address	The IP address of the PE1 node on which the specific PseudoWire VC is configured.
PE 2	<p>The name of the PE router. This router is one of the endpoints of the PseudoWire VC.</p> <p>If the status of PE 2 is unknown, Not Managed, 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.</p>
PE 2 Address	The IP address of the PE2 on which the specific PseudoWire VC is configured.
L2VPN Type	<p>The selected PseudoWire VC participates to form an L2VPN. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>VPLS</b> - The selected PseudoWire VC participates to form a VPLS VPN.</li> <li>• <b>VPWS</b> - The selected PseudoWire VC participates to form a VPWS VPN.</li> <li>• <b>Unknown</b> - The value is set to Unknown when the Encapsulation Type is not known or the NNM iSPI for MPLS is not able to determine whether the Pseudowire corresponds to the value VPLS or VPWS.</li> </ul>
L2VPN Name	<p>The name of the L2 VPN associated with the selected PseudoWire VC. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>VPLS Name</b> - The name of a VPLS VPN.</li> <li>• <b>VPWS Name</b> - The name of a VPWS VPN.</li> <li>• <b>MPLS Configuration</b> workspace, the same name appears in this field.</li> <li>• <b>Default Group</b> - 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.</li> </ul>



### Basic Attributes, continued

Attribute	Description
Status Last Modified	The status of the PseudoWire VCs is calculated whenever there is a change in the topology. The Status Last Modified shows date and time on which the status was last set.
Management Mode	Management mode of the selected PseudoWire VC. Possible values are:  <b>Managed</b> - The selected PseudoWire VC is managed.  <b>Not Managed</b> - The selected PseudoWire VC is not managed.

### Filter by Attribute Value

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

- Status
- Id
- Encapsulation Type
- L2VPN Type
- Management Mode

You can create, change, or remove a filter at any time. The NNM 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
- ID
- Encapsulation Type
- L2VPN Type
- Management Mode

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

## Monitoring LSPs

In addition to monitoring PseudoWire VCs, NNM iSPI for MPLS monitors LSPs being used by PseudoWire VCs. To enable monitoring LSPs:

1. From the **MPLS** workspace, click **PseudoWire VC Inventory**.
2. Select a PseudoWire for which you want to monitor the LSP.
3. Click **ActionsMonitor LSP>** .

A "LSP set for monitoring." message is shown in a new window.

The monitored LSP can be viewed in the [Monitored LSP Inventory](#).

### To Launch MPLS LSP View:

1. Click **PseudoWire VC Inventory** from the **MPLS** workspace.
2. Select a PseudoWire for which you want to view the LSP path.
3. Click **Actions**.
4. Click **MPLS LSP Path View**.

### Analysis Pane

Analysis Pane displays a quick summary of a particular object without opening a form view. The **Analysis Pane** remains blank until an object is selected in the inventory.

The following information is shown in the **Analysis Pane** of PseudoWire VC Inventory:

- Status
- Create Time
- Management Type
- Management Mode
- Custom Attributes
- PE1 - Source provider edge
- PE2 - Destination provider edge
- **VcLspStatusPieChart** Tab - Shows Pie Chart that represents the status of all the VC LSPs participating to form the PsuedoWire
- **LSP Path View** Tab - Shows a link to Launch LSP Path View. You can click this link to launch an LSP path.

- **Performance** Tab - The Performance Tab enables you to analyze the performance metrics for the selected object in the inventory with the help of graphs. The graph shows the following information:
  - AvailabilityPct - Total duration for which the status of the selected PseudoWire is up and active.

For more information on how to access Analysis Pane, see *About Analysis Pane* in *NNMi Online Help*.



## TE Tunnel Inventory

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




Use the TE Tunnel Inventory to perform the following tasks:

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

### Basic Attributes

Attribute	Description
Status	<p>Overall status of the TE Tunnel. Possible values are :</p> <ul style="list-style-type: none"> <li>✔ <b>Normal</b> - If the status of the TE Tunnel is Up, the status of the TE Tunnel is Normal.</li> <li>✘ <b>Critical</b> - If the status of the TE Tunnel is Down, the status of the TE Tunnel is Critical.</li> <li>❓ <b>Unknown</b> - 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.</li> </ul> <p><b>Note:</b> The status computation of TE Tunnel does not include the status of TE Tunnels that are not managed.</p>
Name	The name of the TE tunnel.
Head	<p>The selected TE Tunnel starts from a node. This node is known as the head node. The head and name together form a unique identification for the selected tunnel. Multiple tunnels originate from the same head router. If a head router is a node that is not managed 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 <b>Lookup</b> icon).</p>
Tail	<p>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. In such cases, the Tail field appears as a blank. To view the tail node details, click  (the <b>Lookup</b> icon) in the <a href="#">TE Tunnel Form</a>.</p>
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.

### Basic Attributes, continued

Attribute	Description
	For Juniper routers, the value is calculated for the following versions: <ul style="list-style-type: none"> <li>• 9.6 and above</li> <li>• 9.3R4, 9.4R3, 9.5R2 maintenance releases.</li> </ul> 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 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.
Management Mode	Management mode of the selected TE Tunnel. Possible values are:   <b>Managed</b> - The selected TE Tunnel is managed.   <b>Not Managed</b> - The selected TE Tunnel is not managed.   <b>Out of Service</b> - The selected TE Tunnel is out of service.

### Filter by Attribute Value

The filter option is available on the following attributes:

- Status
- Name
- Management Mode
- Head
- Tail
- Tail IP Address

You can create, change, or remove a filter at any time. The NNM 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
- Tail
- Management Mode

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

### Analysis Pane

Analysis Pane displays a quick summary of a particular object without opening a form view. The **Analysis Pane** remains blank until an object is selected in the inventory.

The following information is shown in the Analysis Pane of the TE Tunnel Inventory:

- Create Time
- Status
- Last Path Change Time

**Note:** If the status of the selected object in the inventory is down, this field will not be displayed.

- Last Status Change Time
- Custom attributes
- Management Type
- Management Mode
- **Tunnel Hops** Tab- Shows the Head, Tail, and intermediate routers participating to form a tunnel.

**Note:** You must wait for the next configured polling cycle to get the tunnel hops discovered when the TE Tunnel state is changed from down to up. For more information, see "[Configure the Polling Frequency](#)" on page 155.

- **Performance** Tab- The Performance Tab enables you to analyze the performance metrics for the selected

object in the inventory with the help of graphs. The graph shows the following information:




- AvailabilityPct - Total duration for which the status of the selected TE Tunnel is up and active.

For more information on how to access Analysis Pane, see *About Analysis Pane* in *NNMi Online Help*.

## Monitored LSP Inventory

The MPLS Monitored LSP Inventory provides a list of monitored services. The monitored services use LSPs. One or more monitored services may use the same LSP. You can view a list of services in this inventory because you have selected these services to be monitored either for VRFs or PseudoWire VC.

### Basic Attributes

Attribute	Description
Status	<p>Each row in the Monitored LSP Inventory represents a service being monitored. This column shows direct impact of status of an LSP on a service. Possible values are:</p> <ul style="list-style-type: none"><li> Normal - This status occurs when the LSP is up.</li><li> Warning - This status occurs when an LSP is re-routed. For more information see, "<a href="#">LSP Re-route Scenarios</a> " on page 119.</li><li> Critical- This status occurs when a path cannot be computed due to LSP going down.</li></ul>
Source	Source service from where the LSP originates.
Destination	Destination service where the LSP ends.
Service Type	<p>Service object for which the LSP is being monitored. Possible values are:</p> <ul style="list-style-type: none"><li>• VRF</li><li>• VC_LSP</li></ul>
LSP Name	The LSP name between the selected source and destination.
Management Mode	<p>The NNM iSPI for MPLS supports management of LSPs. These values are inherited from the services to which the LSPs are associated. Possible values are:</p> <ul style="list-style-type: none"><li>• <b>Managed</b>– The selected LSP is managed.</li><li>• <b>Not Managed</b>– The selected LSP is not managed.</li></ul> <p>If NNM iSPI for MPLS is unable to discover all the nodes associated with an LSP path, then the path is partially managed. However, the Management mode is shown as <b>Managed</b>.</p>

## Actions Available for Monitored LSP Inventory

### To Launch MPLS LSP Path View

:

1. Select the LSP for which you want to launch the map.
2. Click **Actions**
3. Click **MPLS LSP Path View**.

You can choose to disable monitoring for a selected LSP.

**To stop monitoring an LSP, follow these steps:**

1. Select Monitored LSP Inventory from the **MPLS** workspace.
2. Select the LSP from the list for which you want to disable monitoring.
3. Click **Actions** -> **Disable LSP Monitoring**.

Alternatively,

1. Select Monitored LSP Inventory from the **MPLS** workspace.
2. Double-click the LSP from the list for which you want to disable monitoring. This will open the **Monitored LSP** form.
3. Click **Actions** -> **Disable LSP Monitoring**.

After you disable monitoring for an LSP, it will not be shown in inventories.

### Analysis Pane

The following information is shown in the Analysis pane for Monitored LSP inventory:

- **Monitored LSP Summary**
  - Id - The unique identifier for the selected Monitored LSP
  - Update Time
  - Tunnel name

**Note:** The fields Update Time and Tunnel name will be displayed only when a TE Tunnel is part of the selected LSP.

- Status - Shows the status of the LSP
- Management Mode
- Source Node - Name of the source node for the selected LSP
- Destination Node - Name of the destination node for the selected LSP
- **Outer Label** - This is the label on the source LER<sup>1</sup> that gets swapped as the top label, through which the MPLS traffic is sent to the next router.
- **Inner Label** - This is the label on the destination LER that is sent by a Service destination during the LSP setup.

<sup>1</sup>Only out segment is present for a source LER

- Source service - Name of the source service for the selected LSP
- Destination service - Name of the destination service for the selected LSP
- **LSP Information** tab shows information about the LSP in a tabular format.
  - Out node
    - **Node** - Name of the node from where the segment originates. Click the node name to open the node form.
    - **Interface** - The associated interface on out node that carries the LSP traffic. Click the interface name to open the interface form.
  - In node
    - **Node** - Name of the node at which the segment ends. Click the node name to open the node form.
    - **Interface** - Interface that resides on the node where the segment ends. Click interface name to open the interface form.
  - Segment Type/(Label | Tunnel name): Shows the OutSegment or Tunnel. The label name is displayed for an OutSegment or the Tunnel name is displayed for a Tunnel that is associated with the corresponding LSP.
  - Segment Status: Shows the current status of the segment.
  - Out segment
    - **Node** - Name of the source node. Click to open the node form
    - **Interface** - Interface that resides on the source node. Click to open interface form.
  - In segment
    - **Node** - Name of the destination node. Click to open the node form.
    - **Interface** - Name of the destination node. Click to open the interface form.
  - **Label** - Label associated with the corresponding nodes.
- **Performance** Tab - The Performance Tab enables you to analyze the performance metrics for the selected object in the inventory with the help of graphs. The graph shows the following information:
  - AvailabilityPct - The availability for which the status of the selected Monitored LSP is up and active, represented in percentage.
  - Hop count - A gauge type counter to show number the of active hops for the selected Monitored LSP.
  - Avg weighted status - A gauge type counter to find the average change in status of the selected Monitored LSP by considering the number of samples in that polling interval.
  - With Hop count and Average - A combination of Hop count and Avg weighted status.

To enable monitoring, see one of the following :

[Monitoring LSP for VRF](#)

[Monitoring LSP for PseudoWire](#)



# SDP Inventory









The SDP Inventory provides a list of available Service Distribution Points (SDPs) on the network. The SDP logically directs the traffic from one source to destination through a unidirectional service tunnel.

**Note:** The Service Distribution Point (SDP) is discovered only on Alcatel device. For more information on supported combinations of devices for the NNM iSPI for MPLS objects and services, see *NNM iSPI for MPLS 10.00 Support Matrix* document.



Use the SDP Inventory for the following tasks:

- Monitor the SDPs on the network.
- View the number of SDPBinds associated with the SDP. Check the status of the SDPs on the network.

## Basic Attributes

Attribute	Description
Status	<p>The status of the SDP is derived and calculated based on SDP polling. Possible values are:</p> <ul style="list-style-type: none"> <li> <b>No Status:</b> A SDP is newly formed and not polled, status of the SDP is No Status.</li> <li> <b>Normal</b> - If the status of the SDP is Up, the status of the SDP is Normal.</li> <li> <b>Unknown</b> - If there is no SNMP response for the selected node and the selected SDP is configured on this node, the status of the SDP is Unknown.</li> <li> <b>Warning</b> - The status of one or more VFIs participating to form a VPLS VPN is Unknown but, none of them is Critical.</li> <li> <b>Minor</b> - The status of one or more VFIs participating to form a VPLS VPN is Critical.</li> <li> <b>Critical</b> - If the status of the SDP is Down, the status of the SDP is Critical.</li> </ul>
SDP ID	The unique identifier of the selected SDP.
Source Node	The selected SDP starts from this node. Click  (the <b>Lookup</b> icon) to view more information about the source node.
Destination Node	Name of the destination node of the selected SDP. Click  (the <b>Lookup</b> icon) to view more information about the Destination Node.
Number of Services	The number of services associated with the SDP.
Status Last Modified	The status of the SDP is calculated whenever there is a change in topology. The status Last Modified shows date and time on which the status was last set.

### Basic Attributes, continued

Attribute	Description
Management Mode	Management mode of the selected SDP. Possible values are:  <b>Managed</b> - The selected SDP is managed.  <b>Not Managed</b> - The selected SDP is not managed.

### Filter by Attribute Value

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

- Status
- SDP ID
- Management Mode

You can create, change, or remove a filter at any time. The NNM 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 SDP inventory:

- Status
- SDP ID

- Management Mode

**Analysis Pane:**

Analysis Pane displays a quick summary of a particular object without opening a form view. The **Analysis Pane** remains blank until an object is selected in the inventory.

The following information is shown in the **Analysis Pane** of SDP Inventory:

- Status
- SDP Id
- Source
- Destination
- Delivery Type
- **SDPBinds Status Pie Chart** Tab- Shows Pie Chart that represents the status of all the SDPBinds.

For more information on how to access Analysis Pane, see *About Analysis Pane* in *NNMi Online Help*.

## Monitoring your network with MPLS Forms

You can use the MPLS forms to view the details associated with the NNM 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.

The following MPLS forms are available from the MPLS workspace:

Form Name	Description
L3 VPN Form	Provides details about the selected L3 VPN. For more information, see <a href="#">L3 VPN Form</a> .
VRF Form	Provides details about the selected VRF that participates in a L3 VPN. For more information, see <a href="#">VRF Form</a> .
TE Tunnel Form	Provides details about the selected TE tunnel. For more information, see <a href="#">TE Tunnel Form</a> .
PseudoWire VC Form	Provides details about the selected PseudoWire VCs. For more information, see <a href="#">PseudoWire VC Form</a> .
VC LSP Form	Provides details about the selected VC LSP. For more information, see <a href="#">VC LSP Form</a> .
VPLS-VPN Form	Provides details about the selected VPLS VPN. For more information, see <a href="#">VPLS VPN Form</a> .
VPWS-VPN Form	Provides details about the selected VPWS VPN. For more information, see <a href="#">VPWS VPN Form</a> .

Form Name	Description
MVPN Form	Provides details about the selected MVPN. For more information, see <a href="#">MVPN Form</a> .
MDT Form	Provides details about the selected MDT. For more information, see <a href="#">MDT Form</a> .
Monitored LSP Form	Provides details about the selected LSP and the service to which it is mapped, see <a href="#">Monitored LSP Form</a> .
VFI Form	Provides details about the selected VFI participating to form a VPLS VPN. For more information, see <a href="#">VFI Form</a> .
SDP Form	Provides details of the SDP that logically directs the traffic from one source to destination through a unidirectional service tunnel. For more information, see <a href="#">SDP Form</a> .
SDPBind Form	Provides details of the service binded to the SDP. For more information, see <a href="#">SDPBind Form</a> .

**To view the MPLS forms:**

1. From the left navigation panel, select the MPLS workspace and click <MPLS> Inventory (for example, **MPLS- > MPLS L3 VPN inventory**).
2. Select a specific object and click  (the **Open** icon) to view the detailed information about that specific object. The form shows the information specific to the MPLS object.

## L3 VPN Form

The L3 VPN form provides details of the VRFs participating to form an L3 VPN. All PE routers containing VRFs relevant to the named L3 VPN are grouped in one VPN and displayed in the inventory.


Use the L3 VPN Form to perform 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, Number of VRFs, Multicast Enabled , IPv6 Enabled	These attributes listed in the L3 VPN form are same as available in the L3 VPN Inventory view. For more information, see <a href="#">L3 VPN Inventory</a> .
Management Mode	The NNM iSPI for MPLS supports management of VPNs. Possible values are:

### Basic Attributes, continued

Attribute	Description
	<p><b>Managed</b> – The selected VPN is managed.</p> <p><b>Not Managed</b> – The selected VPN is not managed.</p> <p><b>Note:</b> To modify the Management Mode, select "Managed" or "Not Managed" respectively from the Management Mode list of the VPN form.</p>
Management Type	<p>Inheritance type for the selected VPN. An MPLS object inherits management mode of its container object. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Node Inherited</b></li> <li>• <b>Self</b></li> </ul>
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. Status Last Modified shows the date and time on which the status of the selected L3 VPN was last set.
Hub VRF	The name of the VRF participating to form a Hub - Spoke VPN. To open the hub VRF, click  (the <b>Lookup</b> icon). This column is blank if the corresponding VRF is not a Hub VRF.

**Related Topics:** [VRFs Tab](#), [Status Tab](#), [Conclusions Tab](#), [Incidents Tab](#), [RAMS Traps Tab](#), [Custom Attributes Tab](#), [QA Probes Tab](#), and [Registration Tab](#).

### Analysis Pane

Information shown for L3 VPN form is same as that in the L3 VPN Inventory. For more information, see [L3 VPN Inventory](#).

## 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.

### Basic Attributes

Attribute	Description
VRF Attributes	The attributes listed in the VRF tab are same as available in VRF form. For more information, see <a href="#">VRF Form</a> .

## Monitoring LSPs

In addition to monitoring VRFs, NNM iSPI for MPLS monitors LSPs. To enable monitoring LSPs:

1. [Open VRFs in a new window](#)
  - a. From the **MPLS** workspace, click **L3 VPN Inventory**.
  - b. Select a VPN to open the **L3 VPN** form.
  - c. In the **VRFs** tab, click  to open the VRFs in a new window.
2. Select two VRFs for which you want to monitor the LSP.
3. Click **Actions**.
4. Click **Monitor LSP**.

The "LSP set for monitoring." message is shown in a new window.

The monitored LSP can be viewed in the [Monitored LSP Inventory](#).

**You may encounter the following messages:**

- "No LSP Path defined for monitoring" - displayed if no LSP path exists between the selected VRFs.
- "LSP path not available, because there is no neighboring relation between two VRFs" - displayed if there is no neighboring relation between the select VRFs.






**Analysis Pane**

Information shown in the Analysis Pane of VRF tab is same as available in the VRF form. For more information, see [VRF Form](#).


## 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	<p>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:</p> <ul style="list-style-type: none"> <li> <b>No Status</b> - The status of an L3 VPN is 'No Status' when:                             <ul style="list-style-type: none"> <li>• An L3 VPN is newly formed and not polled.</li> <li>• If all the VRFs participating to form an L3 VPN are in 'Not Managed' mode.</li> <li>• When VRFs participating in the L3 VPN are not mapped to any interfaces and hence, not polled.</li> </ul> </li> <li> <b>Normal</b> - The status of all the VRFs participating in the L3 VPN is Normal.</li> <li> <b>Unknown</b> - The status of all the VRFs participating in the L3 VPN is Unknown.</li> <li> <b>Warning</b> - The status of one or more the VRFs participating in the L3 VPN is Unknown, however none of them is Critical.</li> <li> <b>Minor</b> - The status of the L3 VPN is Minor if the status of one or more, but not all, of the VRFs participating in the L3 VPN is Critical.</li> </ul>

### Overall Status, continued

Attribute	Description
	 <b>Critical</b> - The status of the L3 VPN is Critical if the status of all the VRFs participating in the L3 VPN is Critical. It is also critical when the HUB VRF is critical.
Status Last Modified	Status Last Modified shows the date and time on which the status of the selected L3 VPN was last set.

### Status History

Attribute	Description
Status History	List of the last thirty status updates for the selected L3 VPN.
Time Stamp	Time when the selected L3 VPN was last modified.

### Analysis Pane

Analysis Pane is not implemented for the Status tab.

## L3 VPN Form: Conclusions Tab

The L3 VPN Form contains details about the all the VRFs participating in the VPN. The Conclusions tab shows the result 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 <a href="#">VPN Form: Status tab</a> .
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: <ul style="list-style-type: none"> <li>• VPNCritical</li> <li>• VPNNormal</li> <li>• VPNUnknown</li> <li>• VPNMinor</li> <li>• VPNWarning</li> <li>• VPNHubVRFUp</li> </ul>

### Analysis Pane

Analysis Pane is not implemented for the Conclusions tab.

## 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 NNM iSPI for MPLS receives the notification and generates an incident that provides details of the affected L3 VPNs on the network. The NNM 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	<p>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 <i>NNMi Incidents Form</i>.</p> <p>You can cross launch the VPN or the source node from the service impact incident such as MplsL3VPNImpacted.</p>

### Analysis Pane

Information shown in the Analysis Pane of Incidents tab is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## L3 VPN Form: RAMS Traps Tab

The VPN form provides details about the selected VPN. The RAMS<sup>1</sup> Traps tab provides details of all the traps generated by a RAMS appliance for the selected L3 VPN.

After the integration with RAMS, the NNM iSPI for MPLS receives the status traps. These traps are sent by a RAMS appliance for the L3 VPNs within the managed network. The NNM iSPI for MPLS monitors the L3 VPNs by listing the RAMS traps in the L3 VPN view. The trap list shows the current 100 traps.

**Note:** A "Unable to retrieve data from server for extension "iSPI for MPLS". Please contact your system administrator" message is displayed if you access RAMS Traps Tab when iSPI for MPLS is not integrated with Route Analytics Management Software (RAMS).

### Basic Attributes

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

### Analysis Pane

<sup>1</sup>Route Analytics Management System



Analysis Pane is not implemented for the RAMS Traps tab.

## L3 VPN Form: Custom Attributes

The L3 VPN form provides details about the selected L3 VPN. Custom Attributes tab displays the set of name-value pairs of custom attributes associated with L3 VPNs. You can set Custom Attributes using the webservice calls.

### Custom Attributes

Attribute	Description
Name Attributes	Name of the Custom Attribute defined in the web services.
Value	Value assigned to the Custom Attribute in the web services.

### Analysis Pane









Analysis Pane is not implemented for the Custom Attributes tab.

## L3 VPN Form: QA Probes Tab

The L3 VPN form provides details about the selected L3 VPN. The QA Probes tab provides details of the tests configured for the selected VRFs participating to form the VPN. VRF-enabled QA Probes listed in this tab are only for the VRFs that participate in the iSPI for MPLS network.

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

### Basic Attributes

Attribute	Description
Status	Status of the node participating in the L3 VPN. Possible values are: <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul>
Test Name	Name of the selected probe.
Service Type	The type of the discovered QA probe. The NNM iSPI for MPLS recognizes the following QA probe types: <ul style="list-style-type: none"> <li>• UDP Echo</li> </ul>

### Basic Attributes, continued

Attribute	Description
	<ul style="list-style-type: none"><li>• ICMP Echo</li><li>• UDP</li><li>• TCP Connect</li><li>• Voice over Internet Protocol (VoIP)</li></ul>
Source	Name of the source node.
Destination	Name of the destination node.
RTT (ms)	The round-trip time used by QA probe for the selected node.
Packet Loss	The delay variance for a data packet to reach the destination node.
Jitter	The percentage of packets that failed to arrive at the destination node.
Polled Time	Last recorded time when a QA probe was polled.
Category	Type of probe selected. Possible values are: <ul style="list-style-type: none"><li>• PE-PE (VRF-VRF, where both the VRFs belong to the same VPN)</li><li>• CE-CE</li><li>• PE-CE</li><li>• CE-PE</li><li>• CE-Unknown</li></ul>

### Analysis Pane

For the QA Probes Tab, the Analysis Pane shows information about Quality Analysis (QA) probes. You can *maintain* (start or stop) a probe by using the Analysis Pane.

- Name
- Status

In addition, you can launch QA graphs by using **QA Probe Actions** tab. Following are the QA graphs that can be launched from iSPI for MPLS:

- Round Trip time
- Ping Average RTT
- Two Way Jitter
- 2-Way % Packet Loss

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

## L3 VPN Form: Registration Tab

The L3 VPN Form provides details about the selected VPN.

## Registration Table

Attribute	Description
Create Time	Date and time on which the selected L3 VPN was created.
Status Last Modified	Status Last Modified shows the date and time on which the status of the selected L3 VPN was last modified.

## Analysis Pane

Analysis Pane is not implemented for the Registration tab.






# VRF Form

The VRF form provides details about the selected VRF, and VRF Lite participating to form an L3 VPN.

Use the VRF form for the following tasks:

- Monitor the VRFs, MVRFs, or VRF Lites participating in the selected L3 VPN or MVPN. The **MVRF** and **MVRF Status** tabs 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 or VRF Lite 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. PE node on VRF lite shows the VRF Lite router though it is named PE router. Click  (the <b>Lookup</b> icon) to access the node details. For more information for the node, see <i>NNMi Help</i> .
Status	Overall status for the current VRF. Possible values are: <ul style="list-style-type: none"> <li> <b>No Status</b>- The VRF is Not Managed.</li> <li> <b>Normal</b> - The operstatus of the VRF is Up, status is Normal.</li> <li> <b>Unknown</b> - The VRF is not reachable or not responding.</li> <li> <b>Critical</b> - The operstatus of the VRF is Down when the status of all the interfaces on the VRF is Down.</li> </ul>
Management Mode	The NNM iSPI for MPLS supports management of VRFs. Possible values are:



### Basic Attributes, continued

Attribute	Description
	<ul style="list-style-type: none"> <li>• <b>Managed</b> – The selected VRF is managed.</li> <li>• <b>Not Managed</b> – The selected VRF is not managed.</li> </ul> <p><b>Note:</b> To modify the Management Mode, select "Managed" or "Not Managed" respectively from the <b>Management Mode</b> list of the VRF form.</p> <ul style="list-style-type: none"> <li>• <b>Out of Service</b> – 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 is temporarily out of service.</li> </ul> <p><b>Note:</b> Out of Service is an NNMi supported mode. The NNM iSPI for MPLS does not allow users to store 'Out of Service' value from the Management Mode list.</p> <p>For more information, see the <i>Help for NNMi; View the Management Mode for an Object in Your Network</i>.</p>
Management Type	<p>Inheritance type for the selected VRF. An MPLS object inherits management mode of its container object. Management Type displays the type of container object from which the selected VRF has inherited the Management Mode. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Node Inherited</b> - The selected VRF inherits management mode from a node.</li> <li>• <b>VPN Inherited</b> - The selected VRF inherits management mode from a node.</li> <li>• <b>Self</b> - The selected VRF is <b>Not Managed</b> but it belongs to a <b>Managed</b> node, participating in a <b>Managed</b> VPN.</li> </ul> <p><b>Note:</b> You cannot change Management Type of an <b>Not Managed</b> VRF to <b>Self</b> if it is <b>VPN Inherited</b>.</p> <ul style="list-style-type: none"> <li>• <b>Regional Inherited</b>- One of the VRF belonging to a VPN at Regional level is <b>Not Managed</b>. In addition, these VRFs are not affected by management changes made at the Global level.</li> </ul> <p><b>Note:</b> '<b>Regional Inherited</b>' type is only applicable for a <b>Global Manager</b>. This is because a VRF <b>Not Managed</b> in a regional manager has a direct effect on the Global Manager. However, any VPN managed/not managed at Global level will not affect a VRF that is '<b>Regional Inherited</b>' .</p>

### Basic Attributes, continued

Attribute	Description
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	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 <input checked="" type="checkbox"/> .
VRF Lite Enabled	The selected VRF supports VRF Lite and Shadow routing. True is represented by <input checked="" type="checkbox"/> .
IPv6 Enabled	The selected VRF supports IPv6. True is represented by <input checked="" type="checkbox"/> .
Hub VRF	The selected VRF is a Hub VRF. True is represented by <input checked="" type="checkbox"/> .
QA Probes	The selected VRF is configured to run tests from the iSPI Performance for Quality Assurance (QA). True is represented by <input checked="" type="checkbox"/> .
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 NNM 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. Status Last Modified shows the date and time on which the status of the selected VRF was last set.
Mean Time Between Failure	<p>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.</p> <p>For example, if the status of the selected VRF is Up at 10:00 AM and the status changes to Down at 10:20 AM. Again, the status of the VRF changes from Down to Up at 10:30 AM and is again Down at 10:40 AM. The status is changed from Down to UP at 10:50 AM. Therefore, the Time Between Failures is the total time when the selected VRF was available ( 50 minutes) by the total number of occurrences when the status was down (2) (MTBF = .50 minutes/ 2).</p> <p>When the iSPI Performance for Metrics is not installed, value is <b>Not Computed</b>.</p>

### Basic Attributes, continued

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 <b>Not Computed</b> .
L3 VPN	The selected VRF belongs to the specified L3 VPN. Access the L3 VPN form from  (the <b>Lookup</b> icon).
VRF Peer	<p>The VRF- VRF Lite relationship. When a PE VRF and a VRF Lite participating in the same VPN are discovered, they are termed as peers. For a VRF Lite object, when the VRF form is opened its corresponding PE VRF is shown as its peer. Similarly, when PE VRF is opened, the corresponding VRF Lite is shown as its peer. You can open a VRF peer by clicking on the VRF peer object. The VRF peer field remains blank if no VRF- VRF Lite relationship exists. You can open a VRF Peer by using  (the <b>Lookup</b> icon).</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p><b>Note:</b> Look up shows a "Cannot perform operation" pop-up if you do not have access to the VRF peer.</p> </div>

**Related Topics:** [PE Interfaces Tab](#), [CE Interfaces Tab](#), [Neighbors VRFs Tab](#), [MVRF Tab](#), [Upstream MDTs](#), [Downstream MDTs](#), [MVRF Status](#), [Status Tab](#), [Conclusions Tab](#), [Incidents Tab](#), [Custom Attributes Tab](#), and [Registration Tab](#)

### Analysis Pane

For the VRF form, an Analysis Pane with VRF Summary and **QA Probe Actions** tab are displayed.

#### VRF Summary:

VRF Summary provides the following information:

- **Name:** Name of the selected VRF.
- **Create time:** Time when the associated VPN was created.
- **Status:** Status of the VRF.
- **VPN Name:** Name of the VPN associated with the VRF.
- **Exported RT List:** List of Route Targets exported from this VRF to other VRFs.
- **Imported RT List:** List of Route Targets imported other VRFs.
- **Management Type:** Current management type of the VRF.
- **Management Mode:** Current management mode of the VRF.

#### QA Probe Actions

You can *setup* a new probe or *maintain* (start or stop) a probe by using the Analysis Pane. From **QA Probe Actions** tab, you can also launch QA graphs.

- Probe Setup
- Probe Maintenance
- Round Trip time
- Ping Average RTT
- Two Way Jitter
- Percentage Packet Loss Two Way

You can click 'Click here' to launch each of these graphs.

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

## VRF Form: PE Interfaces Tab

The VRF form provides details about the selected VRF and VRF Lite.

The PE Interfaces tab provides details of the Provider Edge interfaces associated with the current VRF. Similarly, it provides details of the Provider Edge interfaces associated with the current VRF Lite. 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
Status, IfName, IfAlias, IfType	The attributes listed in the PE interfaces tab are same as available in NNMi Interface form. For more information, see the Help for <i>NNMi Interface Form</i> .
Next hop IP	The IP address of the interface of the third-party service provider that is immediate next to the PE node.
Next hop AS	The name or AS number of the first service provider network encountered by the PE node.
PE-CE Protocol	The protocol followed for data transmission between the PE node and the CE node. If the PE interface has a corresponding VRF Lite peer, then PE-Vrf Lite router link is displayed here. This is because the VRF Lite router is also considered as a CE for that PE interface.

Values under Next hop IP, Next hop AS, and PE-CE Protocol will be visible only when the Inter-Provider VPN feature is on for the iSPI for MPLS. For more information, see *Troubleshooting the iSPI for MPLS*.

### Analysis Pane

Information shown in the Analysis Pane of PE Interface tab is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in NNMi Online Help.

## VRF Form: CE Interfaces Tab

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

### 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 <i>NNMi Interface Form</i> .
CE Node	The name of the CE node where the CE interface is configured.
Next hop IP	The IP address of the interface of the third-party service provider that is immediate next to the CE node.
AS Path	The associated path which connects the CE node with the PE node. AS Path is a comma separated string of AS Names or AS Numbers of the service providers encountered between the CE node and PE node.
PE IfName	The name of the associated PE interface.
PE Node	The name of the PE node where the PE interface is configured. PE node on VRF Lite shows the VRF Lite router though it is named PE router

Values under Next hop IP and As Path will be visible only when the Inter-Provider VPN feature is on for iSPI for MPLS VPN. For more information, see *Troubleshooting the iSPI for MPLS*.

#### PE IfName and PE Node columns display incorrect information for the Inter-Provider feature.

In this case, Next Hop IP column displays IP address of the PE interface of the third-party service provider that is immediate next to the CE node. Whereas, PE IfName and PE Node columns display information of only those PE interfaces that participate in the NNM iSPI for MPLS VPN and not of those participating in the third-party VPN network cloud.

#### Analysis Pane

Information shown in the Analysis Pane of CE Interfaces tab is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see About the Analysis Pane in NNMi Online Help.

## 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 <a href="#">VRF Form</a> .

#### Analysis Pane

Information shown in the Analysis Pane of Neighbor VRFs tab is same as available in the VRF form. For more information, see [VRF form](#).



## VRF Form: Route Targets Tab

The VRF Form provides details about the selected VRF. The Route Targets (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 on the network. The NNM 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 NNM 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 NNM 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
Imported	The selected RT that is imported for the selected VRF. True is represented by <input checked="" type="checkbox"/> .
Exported	The selected RT that is exported for the selected VRF. True is represented by <input checked="" type="checkbox"/> .
Excluded	The selected RT that is ignored for the selected VRF.

### Analysis Pane









Analysis Pane is not implemented for the Route Targets tab.

## 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. VRF-enabled QA Probes listed in this tab are only for the VRFs that participate in the iSPI for MPLS network. For more information, see *NNM iSPI Performance for QA*.

**Note:** The QA Probes tab will not be displayed if the NNM iSPI for MPLS is not integrated with the NNM iSPI Performance for QA.

### General Attributes

Attribute	Description
Status	Status of the VRF. Possible values are: <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul>
Test Name	Name of the selected probe.
Service Type	The type of the discovered QA probe. The NNM iSPI for MPLS recognizes the following QA probe types: <ul style="list-style-type: none"> <li>• UDP Echo</li> <li>• ICMP Echo</li> <li>• UDP</li> <li>• TCP Connect</li> <li>• Voice over Internet Protocol (VoIP)</li> </ul>
Source	Name of the source VRF.
Destination	Name of the destination VRF.
RTT (ms)	The round-trip time used by QA probe for the selected VRF.
Packet Loss	The delay variance for a data packet to reach the destination node.
Jitter	The percentage of packets that failed to arrive at the destination node.
Polled Time	Last recorded time when a QA probe was polled.
Category	Type of probe selected. Possible values are: <ul style="list-style-type: none"> <li>• PE-PE (VRF-VRF, where both the VRFs belong to the same VPN)</li> <li>• CE-CE</li> <li>• PE-CE</li> <li>• CE-PE</li> <li>• CE-Unknown</li> </ul>

### Analysis Pane

For the QA Probes Tab, the Analysis Pane shows information about Quality Analysis (QA) probes. You can *maintain* (start or stop) a probe by using the Analysis Pane. In addition, you can launch QA graphs by using **QA Probe Actions** tab. Following are the QA graphs that can be launched from iSPI for MPLS:

- Probe Setup
- Probe Maintenance
- Round Trip time
- Ping Average RTT
- Two Way Jitter
- Percentage Packet Loss Two Way

You can click 'Click here' to launch each of these graphs.

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

## 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 <a href="#">MVPN Form: MVRF Tab</a> .
MVPN	The selected MVRF participates in the named MVPN.

### Analysis Pane

Information shows in the Analysis Pane of MVRF is same as available in the VRF form. For more information, see [VRF Form](#).

## VRF Form: Upstream MDTs Tab

The VRF form provides details about the selected VRF and 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 <a href="#">MVPN form: MDT Tab</a> .

### Analysis Pane

Analysis Pane is not implemented for the Upstream MDTs 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 <a href="#">MVPN form: MDT Tab</a> .

The list of senders is displayed in the Analysis Pane. Click a sender from the table, to draw a path from the receiver to the selected router.

### Analysis Pane

Analysis Pane is not implemented for Downstream MDTs tab.

You can use the Analysis pane to launch a reverse path from the receiver to a provider source. The following tabular information is displayed in Analysis Pane:

- **Provider Source**- The IP address of the provider source.
- **Provider Group** - The group IP address of the provider source.
- **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.
- **Multicast Reverse Path View** - URL to launch the Reverse Path View.

For more information, see [Multicast Reverse Path View](#).

## 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: <ul style="list-style-type: none"> <li>🟡 <b>No Status</b> - The status of a VRF is 'No Status' when:               <ul style="list-style-type: none"> <li>• The VRF is newly created and not polled.</li> <li>• When a VRF is not mapped to any interface and hence, not polled.</li> </ul> </li> <li>🟢 <b>Normal</b> - The operstatus of the VRF is Up.</li> <li>🟡 <b>Unknown</b> - The VRF is not reachable or not responding.</li> <li>🔴 <b>Critical</b> - The operstatus of the VRF is Down.</li> </ul>
Last Modified	Date and time on which 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 <i>NNMi Status tab</i> .
Time Stamp	Time when the selected VRF was last modified.




### Analysis Pane

Analysis Pane is not implemented for the 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	<p>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:</p> <ul style="list-style-type: none"><li> <b>Normal</b> - The status of the VRF is Normal and MTI is Up, status of the MVRF is Normal.</li><li> <b>Unknown</b> - The status of the VRF is Unknown and MTI is Up, status of the MVRF is Unknown.</li><li> <b>Critical</b> - The status of the VRF is Unknown, the status of MTI is Down, or both, status of the MVRF is Critical.</li></ul>
Last Modified	Date and time on which 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 <i>NNMi Status tab</i> .

### Analysis Pane

Analysis Pane is not implemented for the MVRF 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 <a href="#">VRF Form: Status tab</a> .
Time Stamp	The Time Stamp data is the time when the status of the VRF is last set.
Conclusion	<p>The conclusion is set by the Causal Engine after the status calculation. Possible conclusions are:</p> <ul style="list-style-type: none"> <li>• <b>MplsVRFDown</b></li> <li>• <b>MplsVRFUp</b></li> <li>• <b>MplsVRFUnknown</b></li> </ul> <p>Example: The conclusion MplsVRFDown sends an MplsVRFDown incident.</p>

### Analysis Pane

Analysis Pane is not implemented for the Conclusions tab.

## 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	<p>The attributes listed in the incidents tab are same as available in NNMI Incidents form.</p> <p>For more information for the attributes, see the Help for <i>NNMi Incidents Form</i>.</p>

### Analysis Pane

Information shown in the Analysis Pane of Incidents tab is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## VRF Form: Custom Attributes

The VRF form provides details about the selected VRF. Custom Attributes tab displays the set of name-value pairs of custom attributes associated with VRFs. You can set Custom Attributes using the webservice calls.

### Custom Attributes

Attribute	Description
Name Attributes	Name of the Custom Attribute defined in the web services.
Value	Value assigned to the Custom Attribute in the web services.

### Analysis Pane

Analysis Pane is not implemented for the Custom Attributes tab.

## VRF Form: Registration Tab

The VRF form provides details about the selected VRF. Registration tab shows details about when a selected VRF was created and when the status was last modified.

### Registration Table

Attribute	Description
Create Time	Date and time on which the selected VRF was created.
Status Last Modified	Status Last Modified shows the date and time on which the status of the selected VRF was last modified.

### Analysis Pane

Analysis Pane is not implemented for the Registration tab.

## MVPN Form

The MVPN inventory view provides a list of layer 3 Virtual Private Network (VPNs) with multicast services on the network. The MVPN form provides details about the selected Multicast VPN (MVPN).


Before you perform any tasks, ensure that:

- Multicast nodes on the network are discovered.
- All the flows are active.
- Group discovery is successful.

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 <b>Lookup</b> icon) to access the node. For more information about MVPN attributes, see <a href="#">MVPN Inventory</a> .
Create Time	The time when the selected MVPN was formed and created.
Status Last Modified	Shows date and time on which the status was last set.

**Related Topics:** [MVRFs Tab](#) , [MDTs Tab](#), [Status Tab](#) , [Conclusions Tab](#), [Custom Attributes Tab](#), and [Registration Tab](#).




### Analysis Pane

Information shown for MVPN form is same as that in MVPN Inventory. For more information, see [MVPN Inventory](#).

## 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:   <b>Normal</b> - The status of the VRF is Normal and MTI is Up, status of the MVRF is Normal.   <b>Unknown</b> - The status of the VRF is Unknown and MTI is Up, status of the MVRF is Unknown.   <b>Critical</b> - 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.
Multicast Tunnel IF	The name of the Multicast tunnel interface.
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.

### Analysis Pane

The Analysis Pane for MVRFs Tab is same as that in the VRF form. See ["Analysis Pane" on page 62](#)



## 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 Type 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.






### Analysis Pane

Analysis Pane is not implemented.

## MVPN Form: StatusTab

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

### Overall Status Table

Attribute	Description
Status	<p>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:</p> <ul style="list-style-type: none"> <li> <b>Normal</b> - The status of the MVPN is Normal if the status of all the MVRFs participating in the MVPN is Normal.</li> <li> <b>Unknown</b> - The status of the MVPN is Unknown if the status of all the MVRFs participating in the MVPN is Unknown.</li> <li> <b>Warning</b> - 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.</li> <li> <b>Minor</b> - The status of the MVPN is Minor if one or more MVRFs participating in the MVPN is Critical.</li> <li> <b>Critical</b> - The status of the MVPN is Critical if the status of all the MVRFs participating in the MVPN is Critical.</li> </ul>
Last Modified	Date and time on which status was last set.

## Status History

Attribute	Description
Status History	List of last thirty status updates for the selected MVPN.
Time Stamp	Time at which the selected MVPN was last modified.

## Analysis Pane

Analysis Pane is not implemented for the Status tab.

## 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 <a href="#">MVPN Form: Status tab</a> .
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 conclusion is set by the Causal Engine after the status calculation. Possible conclusions are: <ul style="list-style-type: none"><li>• <b>MVPNNormal</b></li><li>• <b>MVPNCritical</b></li><li>• <b>MVPNUnknown</b></li><li>• <b>MVPNMinor</b></li><li>• <b>MVPNWarning</b></li></ul>

## Analysis Pane

Analysis Pane is not implemented for the Conclusions Tab.

## MVPN Form: Custom Attributes

The MVPN form provides details about the selected MVPN. Custom Attributes tab displays the set of name-value pairs of custom attributes associated with MVPNs. You can set Custom Attributes using the webservice calls.

### Custom Attributes

Attribute	Description
Name Attributes	Name of the Custom Attribute defined in the web services.
Value	Value assigned to the Custom Attribute in the web services.

#### Analysis Pane

Analysis Pane is not implemented for the Custom Attributes Tab.

## MVPN Form: Registration Tab

The MVPN form provides details about the selected MVPN.

### Registration Table

Attribute	Description
Create Time	Date and time on which the selected MPLS object instance was created.
Status Last Modified	Status Last Modified shows the date and time on which the status of the selected MVPN was last modified.

#### Analysis Pane

Analysis Pane is not implemented for the Registration Tab.



## 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 <a href="#">PseudoWire VC Inventory</a> .
Management Mode	The NNM iSPI for MPLS supports management of Pseudowire VCs. Possible values are: <ul style="list-style-type: none"> <li>• <b>Managed</b> – The selected Pseudowire VC is managed.</li> <li>• <b>Not Managed</b> – The selected Pseudowire VC is not managed.</li> </ul> <b>Note:</b> To modify the Management Mode, select "Managed" or "Not Managed" respectively from the <b>Management Mode</b> list of the Pseudowire VC form.
Management Type	Inheritance type for the selected Pseudowire VC. An MPLS object inherits management mode of its container object. Possible values are:

### Basic Attributes, continued

Attribute	Description
	<ul style="list-style-type: none"> <li>• <b>Node Inherited</b> - Inherits management mode of the corresponding node.</li> <li>• <b>VPLS Inherited</b> - Inherits management mode on the corresponding VPLS VPN.</li> <li>• <b>VPWS Inherited</b> - Inherits management mode of the corresponding VPWS VPN.</li> <li>• <b>Self</b></li> </ul> <p><b>Note:</b> You cannot change Management Type of an <b>Not Managed</b> PseudoWire VC to <b>Self</b> if it is <b>VPWS Inherited</b> or <b>VPLS Inherited</b>.</p>
VPLS Name	The name of the VPLS VPN. Click  (the <b>Lookup</b> icon) to show more information about the VPLS VPN.
VPWS Name	The name of the VPWS VPN. Click  (the <b>Lookup</b> icon) to view more information about the VPWS VPN.
Discovery State	<p>The state of the PseudoWire VCs. Possible values are:</p> <p><b>Fully Discovered</b> - Both the endpoints (PE1 and PE2) are discovered and the status of both the LSPs is normal.</p> <p><b>Partially Discovered</b> - One of the endpoint is discovered and other endpoint is unknown, not managed, or not discovered. For example, if PE1 is discovered and PE2 is unknown, not managed, or not discovered. You can only get PE1 information and PE2 IP Address. This state is partially discovered.</p>
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. Status Last Modified shows date and time on which the status was last set.

**Related Topics:** [VC LSPs Tab](#), [Status Tab](#), [Conclusions Tab](#), [Incidents Tab](#), [Custom Attributes](#), and [Registration Tab](#).

## LSP-PseudoWire Mapping

You can launch MPLS LSP view by selecting PseudoWire VCs. To launch an MPLS LSP path view:

1. Click **PseudoWire VC Inventory** from the **MPLS** workspace.
2. Select a PseudoWire VC for which you want to launch LSP.
3. Click **Actions** and select **MPLS Lsp Path View**. This will launch the LSP path view between these VC LSPs in a different browser window.

### Analysis Pane

Information shown for PseudoWire VC form is same as that in PseudoWire VC Inventory. For more information, see [PseudoWire VC Inventory](#).

## PseudoWire VC Form: VC LSPs Tab

The PseudoWire VC Form provides details about the selected PseudoWire VC. The VC LSPs 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 LSPs tab are available in the VC LSP form. For more information, see <a href="#">VC LSP Form</a> .

### Analysis Pane

Analysis Pane displays a quick summary of a particular object without opening a form view. The **Analysis Pane** remains blank until an object is selected in the inventory.

The following information is shown in the **Analysis Pane** of VC LSPs tab:




#### VC LSP Summary:

- Create Time
- Status
- Source
- Source Address
- Destination
- Destination Address
- Management Mode

## 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 :   <b>Normal</b> - The status of both the LSPs is Normal.   <b>Critical</b> - The status of any one or both the LSPs is Critical.   <b>Unknown</b> - The status of any one or both the LSPs is Unknown.
Last Modified	Date and time on which status was last set.

## Status History

Attribute	Description
Status	List of last thirty status updates for the selected PseudoWire VC.
Time Stamp	Date and time when the status of the PseudoWire VC is last set.

### Analysis Pane

Analysis Pane is not implemented for the Status tab.

## 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 <a href="#">PseudoWire VC Form: Status Tab</a> .
Time Stamp	Date and time on which the status of the PseudoWire VC is last set.
Conclusions	<p>The conclusions are set by the Causal Engine after the status calculation. Possible conclusions are:</p> <ul style="list-style-type: none"> <li>• <b>MplsPseudoWireVCDown</b></li> <li>• <b>MplsPseudoWireVCNormal</b></li> <li>• <b>MplsPseudoWireVCUnknown</b></li> </ul> <p>The PseudoWire VC down conclusion generates the incident to send the alert for the status attribute. For example, MplsPseudoWireVCDown generates MplsPseudoWireVCDown incident</p>

### Analysis Pane

Analysis Pane is not implemented for the Conclusions tab.


## 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.

### Incidents Table , continued

Attribute	Description
	<p>Click  (the <b>Open</b> 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.</p> <p>For more information, see the Help for <i>NNMi Incidents Form</i>.</p>

#### Analysis Pane

Information shown in the Analysis Pane of Incidents tab is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## PseudoWire VC Form: Custom Attributes

The Pseudowire VC form provides details about the selected Pseudowire VC. Custom Attributes tab displays the set of name-value pairs of custom attributes associated with PseudoWire VCs. You can set Custom Attributes using the webservice calls.

#### Custom Attributes

Attribute	Description
Name Attributes	Name of the Custom Attribute defined by using the web services.
Value	Value assigned to the Custom Attribute in the web services.

#### Analysis Pane

Analysis Pane is not implemented for Custom Attributes tab.

## 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 on which the selected PseudoWire VC was created.
Last Modified	Date and time of when the selected PseudoWire VC was last modified.

#### Analysis Pane

Analysis Pane is not implemented for the Registration tab.

## VPLS VPN Form

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

Use the VPLS VPN form for the following tasks:

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

### Basic Attributes

Attribute	Description
Name, VPN ID, Number of VFIs, Status	<p>The attributes listed in the VPLS VPN form are available in the VPLS VPN inventory view. For more information, see <a href="#">VPLS VPN Inventory</a>.</p> <p><b>Note:</b> VPN ID is set to Not Applicable for a BGP-based VPLS.</p>
Management Mode	<p>The NNM iSPI for MPLS supports management of VPLS VPNs. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Managed</b> – The selected VPLS VPN is managed.</li> <li>• <b>Not Managed</b> – The selected VPLS VPN is not managed.</li> </ul> <p><b>Note:</b> To modify the Management Mode, select "Managed" or "Not Managed" respectively from the <b>Management Mode</b> list of the VPLS VPN form.</p>
Management Type	<p>Inheritance type for the selected VPLS VPN. An MPLS object inherits management mode of its container object. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Node Inherited</b></li> <li>• <b>Self.</b></li> </ul>
Create Time	The time when the VPLS was discovered.
Status Last Modified	Status Last Modified shows date and time on which the status was last set.

**Related Topics:** [VFIs Tab](#), [PseudoWire VCs Tab](#), [Status Tab](#), [Conclusions Tab](#), [Custom Attributes Tab](#), and [Registration Tab](#).

### Analysis Pane

Information shown for VPLS VPN form is same as that in VPLS VPN Inventory. For more information, see [VPLS VPN Inventory](#).

## VPLS VPN Form: VFIs Tab









The VPLS VPN form provides details about the selected VPLS VPN. In the VFIs Tab, you can view the VFIs participating to form a VPLS VPN.

### Basic Attributes

Attribute	Description
VFI Name	The name of the selected VFI .
Source Node	The selected VFI starts from this node.
Status	The status of the VPLS VPN is derived and calculated based on the status of all the VFIs participating in the VPLS VPN. Possible values of VFI are:



### Basic Attributes, continued

Attribute	Description
	<p> <b>No Status</b> - A VPLS VPN is newly formed and not polled, status of the L2 VPN is No Status. When all the VFIs participating to form an L2VPN are in a 'Not Managed' mode, the derived status of the VPN is No Status.</p> <p> <b>Normal</b> - The status of all the VFIs participating to form a VPLS VPN is Normal.</p> <p> <b>Unknown</b> - The status of all the VFIs participating to form a VPLS VPN is Unknown.</p> <p> <b>Warning</b> - The status of one or more VFIs participating to form a VPLS VPN is Unknown. However, the status of none of the VFI is Critical.</p> <p> <b>Minor</b> - The status of one or more VFIs participating to form a VPLS VPN is Critical.</p> <p> <b>Critical</b> - The status of all the VFIs participating in a VPLS VPN is Critical.</p>
RD	<p>The Route Distinguisher of the selected VFI.</p> <p>This value appears only if the VFI is associated with a BGP-based VPLS.</p>
VPN ID	<p>The unique identifier of the selected VPLS VPN.</p> <p><b>Note:</b> VPN ID is set to Not Applicable for a BGP-based VPLS.</p>
Management Mode	<p>Management mode of the selected VFI. Possible values are:</p> <p> <b>Managed</b> - The selected VFI is managed.</p> <p> <b>Not Managed</b> - The selected VFI is not managed.</p>

#### Analysis Pane:

The Analysis pane for VFIs tab is same as that in the VFI form. For more information, see [VFI Form](#).

## VPLS VPN Form: PseudoWire VCs Tab

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

### Basic Attributes

Attribute	Description
Status, Id, Encapsulation Type, PE 1, PE 1 Address, PE 2, PE 2 Address, Status Last Modified, Management Mode	The attributes listed in the PseudoWire VCs tab are same as available in PseudoWire VC inventory. For more information, see <a href="#">PseudoWire VC inventory</a> .









#### Analysis Pane

The Analysis pane for PseudoWire VCs tab is same as that in the PseudoWire VC inventory. For more information, see ["Analysis Pane" on page 42](#)

## 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: <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul>
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 is displayed as a single string value. For more information, see <i>NNMi Help for Operator, Device Profile Form</i> .


### Analysis Pane

Information shown in the Analysis Pane of PE Routers is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.






## VPLS VPN Form: Status Tab

The VPLS VPN form provides details 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 VFIs participating in the VPLS VPN. Possible values are: <ul style="list-style-type: none"> <li> <b>No Status</b> - A VPLS VPN is newly formed and not polled, status of the L2 VPN is No Status. When all the VFIs participating to form an L2VPN are in a 'Not Managed' mode, the derived status of the VPN is No Status.</li> </ul>

### Overall Status Table, continued

Attribute	Description
	<p> <b>Normal</b> - The status of all the VFIs participating to form a VPLS VPN is Normal.</p> <p> <b>Unknown</b> - The status of all the VFIs participating to form a VPLS VPN is Unknown.</p> <p> <b>Warning</b> - The status of one or more VFIs participating to form a VPLS VPN is Unknown. However, the status of none of the VFI is Critical.</p> <p> <b>Minor</b> - The status of one or more VFIs participating to form a VPLS VPN is Critical.</p> <p> <b>Critical</b> - The status of all the VFIs participating in a VPLS VPN is Critical.</p>
Status Last Modified	Status Last Modified shows the date and time on which the status of the selected VPLS VPN was last set.

### Status History

Attribute	Description
Status	List of the last thirty status updates for the selected MPLS object. For more information, see <i>NNMi Status tab</i> .
Time Stamp	The time when the status of the VPLS VPN was last modified.

## VPLS VPN Form: Conclusions Tab

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

### Conclusions Table

Attribute	Description
Status	The derived status of the selected VPLS VPN. For more information, see <a href="#">VPLS VPN Form: Status tab</a> .
Time Stamp	The time when the status of the PseudoWires VC was last set.
Conclusions	<p>The conclusions are set by the Causal Engine after the status calculation. Possible conclusions are:</p> <ul style="list-style-type: none"> <li>• <b>VPLSCritical</b></li> <li>• <b>VPLSNormal</b></li> <li>• <b>VPLSUnknown</b></li> <li>• <b>VPLSMinor</b></li> <li>• <b>VPLSWarning</b></li> </ul>

## VPLS VPN Form: Custom Attributes

The VPLS VPN form provides details about the selected VPLS VPN. Custom Attributes tab displays the set of name-value pairs of custom attributes associated with VPLS VPNs. You can set Custom Attributes using the Web Service calls.

### Custom Attributes

Attribute	Description
Name Attributes	Name of the Custom Attribute defined by using the web services.
Value	Value assigned to the Custom Attribute by using the web services.

## 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 on which the selected VPLS VPN was created.
Status Last Modified	Status Last Modified shows the date and time on which the status of the selected VPLS VPN was last modified.

## VFI Form

The VFI form provides details about the selected VFI participating to form a VPLS VPN.


### Basic Attributes

Attribute	Description
Name	The name of the selected VFI.
Source Node	The selected VFI starts from this node. Click  (the <b>Lookup</b> icon) to view more information about the source node.
Status	Displays the status of the selected VFI.
Description	Provides relevant information about the VFI.
VPN ID	The unique identifier of the selected VPLS VPN.  <b>Note:</b> VPN ID is set to Not Applicable for a BGP-based VPLS.
Management Mode	The NNM iSPI for MPLS supports management of VFIs.

### Basic Attributes, continued

Attribute	Description
	<p>Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Managed</b> – The selected VFI is managed.</li> <li>• <b>Not Managed</b> – The selected VFI is not managed.</li> </ul> <p><b>Note:</b> To modify the Management Mode, select "Managed" or "Not Managed" respectively from the <b>Management Mode</b> list of the VFI form.</p> <ul style="list-style-type: none"> <li>• <b>Out of Service</b> – 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 is temporarily out of service.</li> </ul> <p><b>Note:</b> <i>Out of Service</i> is an NNMi supported mode. The NNM iSPI for MPLS does not allow users to store 'Out of Service' value from the Management Mode list</p> <p>For more information, see the <i>Help for NNMi; View the Management Mode for an Object in Your Network</i>.</p>
Management Type	<p>Inheritance type for the selected VFI. An MPLS object inherits management mode of its container object. Management Type displays the type of container object from which the selected VFI has inherited the Management Mode. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Node Inherited</b> - The selected VFI inherits management mode from a node.</li> <li>• <b>VPLS Inherited</b> - The selected VFI inherits management mode from a VPLS.</li> <li>• <b>Self</b> - The selected VFI is <b>Not Managed</b> but it belongs to a <b>Managed</b> node, participating in a <b>Managed</b> VPLS.</li> </ul> <p><b>Note:</b> You cannot change Management Type of an <b>Not Managed</b> VFI to <b>Self</b> if it is <b>VPLS Inherited</b>.</p> <ul style="list-style-type: none"> <li>• <b>Regional Inherited</b>- One of the VFI belonging to a VPLS at Regional level is <b>Not Managed</b>. In addition, these VFIs are not affected by management changes made at the Global level.</li> </ul> <p><b>Note:</b> '<b>Regional Inherited</b>' type is only applicable for a <b>Global Manager</b>. This is because a VFI <b>Not Managed</b> in a regional manager has a direct effect on the Global Manager. However, any VPLS managed/not managed at Global level</p>

### Basic Attributes, continued

Attribute	Description
	will not affect a VFI that is <b>'Regional Inherited'</b> .
Create Time	Date and time on which the selected VFI was created.
Status Last Modified	Status Last Modified shows the date and time on which the status for the selected VFI was last set.
ACType	This shows the type of Attachment Circuit.
hasPseudoWires	The selected VFI has PseudoWires.
hasSDPBinds	The selected VFI has SDPBinds.
VPLS	The selected VFI belongs to the specified VPLS. Access the VPLS VPN form from  (the <b>Lookup</b> icon).

**Related topics:** [ACs Tab](#), [Neighbor VFIs Tab](#), [SDPBinds Tab](#), [Status Tab](#), [Conclusions Tab](#), [Incidents Tab](#), [Registration Tab](#)

#### Analysis Pane:

The following information is shown in the **Analysis Pane** of VFI form:

- Status
- VPLS Name
- Hosted on Node
- **PseudoWire VC Status Pie Chart** Tab- Shows Pie Chart that represents the status of all the PseudoWire VCs participating to form the selected VPLS VPN
- **SDPBinds Status Pie Chart** Tab- Shows Pie Chart that represents the status of all the SDPBinds participating to form the selected VPLS VPN
- **VFI Neighbor** Tab- Shows the status of all the VFI Neighbors participating to form the selected VPLS VPN
- **PseudoWires** Tab- Shows the status of all the PseudoWires participating to form the selected VPLS VPN
- **Performance** Tab- The Performance Tab enables you to analyze the performance metrics for the selected object in the inventory with the help of graphs. The graph shows the following information:
  - AvailabilityPct - Total duration for which the status of the selected VFI is up and active.

For more information on how to access Analysis Pane, see *About Analysis Pane* in *NNMi Online Help*.

## VFI Form: ACs tab

The VFI form provides details about the selected VFI participating to form a VPLS VPN. You can use the ACs tab to view the attachment circuit of the selected VFI participating to form a VPLS VPN.

#### ACs Table:

Attribute	Description
Status	This attribute listed in the ACs tab is same as available in the NNMi Interface form. For more information, see <i>Help for NNMi Interface form</i> .
AC Interface	The attachment circuit or the data link of the selected VFI. For more information, see the <i>Help for NNMi, Interface Form</i> and <i>Help for NNMi, Port Form</i> .
ACType	This shows the type of Attachment Circuit.
PE Node	The name of the PE node where the PE interface is configured.

**Analysis Pane:**

Information shown in the Analysis Pane is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## VFI Form: Neighbor VFIs tab

The VFI form provides details about the selected VFI participating to form a VPLS VPN. You can use the Neighbor VFIs tab to view the selected VFI participating to form a VPLS VPN.

**Neighbor VFI table**

Attribute	Description
Status, VFI Name, Source Node, Management Mode	These attributes listed in the Neighbor VFIs tab are same as available in the VPLS VPN: VFIs Tab. For more indformation, see <a href="#">VFIs Tab</a> .

**Analysis Pane:**

The Analysis Pane for Neighbor VFIs is same as that in the VFI form. For more information, see [VFI Form](#).

## VFI Form: PseudoWire VCs tab

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

**Basic Attributes**

Attribute	Description
Attributes	The attributes listed in the PseudoWire VCs tab are same as available in PseudoWire VC Form. For more information, see <a href="#">PseudoWire VC Form</a> .

**Analysis Pane**

- Information shown for **VcLspStatusPieChart** tab is same as that in VPLS VPN Inventory. For more information, see [VPLS VPN Inventory](#).
- LSP Path View**- Click Launch LSP Path view to navigate to [MPLS LSP Path View](#).

## VPLS VPN Form: Route Targets Tab

The Route Target tab appears only for VFIs associated with a BGP-based VPLS

### Route Targets Table

Attribute	Description
Route Target	Route target summary
Imported	
Exported	
Excluded	

## VFI Form: SDPBinds tab

The VFI form provides details about the selected VFI participating to form a VPLS VPN. You can use the SDPBinds tab to view the SDP details.

### SDPBinds table:

Attribute	Description
Status, Service Id, Service Type, Bind Type, Delivery Type, Service Name, Destination Node, SDP ID, Management Mode	These attributes listed in the SDP Binds Tab are same as available in the <a href="#">SDP Form: SDPBinds Tab</a>


### Analysis Pane:

The Analysis Pane for SDPBinds Tab is same as available in the SDPBind form. For more information, see [SDPBind Form](#).

## VFI Form: Status tab




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

### Overall Status Table

Attribute	Description
Status	Overall status for the current VFI. Possible values are:  <b>No Status</b> - The status of a VFI is 'No Status' when: <ul style="list-style-type: none"><li>• The VFI is newly created and not polled.</li><li>• When a VFI is not mapped to any interface and hence, not polled.</li></ul>



### Overall Status Table, continued

Attribute	Description
	<p> <b>Normal</b> - The operstatus of the VFI is Up.</p> <p> <b>Unknown</b> - The VFI is not reachable or not responding.</p> <p> <b>Critical</b> - The operstatus of the VFI is Down.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> For Cisco/Juniper device the overall status is derived and calculated based on the status of the PseudoWire VCs belonging to the current VFI.</p> </div>
Last Modified	Date and time on which the status was last set.

### Status History

Attribute	Description
Status	List of last thirty status updates for the selected VFI. For more information, see <i>NNMi Status tab</i> .
Time Stamp	Time when the selected VFI was last modified.

### Analysis Pane

Analysis Pane is not implemented for the Status tab.

## VFI Form: Conclusions tab

The VFI form provides details about the selected VFI. 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 VFI.

### Conclusions Table

Attributes	Description
Status	The status of the selected VFI is dependent on the status of the interface on the selected VFI. For more information, see <a href="#">VFI Form: Status tab</a> .
Time Stamp	The Time Stamp data is the time when the status of the VFI is last set.
Conclusion	<p>The conclusion is set by the Causal Engine after the status calculation. Possible conclusions are:</p> <ul style="list-style-type: none"> <li>• <b>MplsVFIDown</b></li> <li>• <b>MplsVFIUp</b></li> <li>• <b>MplsVFIUnknown</b></li> <li>• <b>MPLSVFINoStatus</b></li> </ul> <p>Example: The conclusion MplsVFIDown sends an MplsVFIDown incident.</p>


### Analysis Pane

Analysis Pane is not implemented for the Conclusions tab.

## VFI Form: Incidents tab

The VFI form provides details about the selected VFI participating to form a VPLS VPN. The Incidents tab is useful for obtaining a quick summary of the incident and problem description for the VFI.

### Incidents Table:

Attribute	Description
Incidents Attributes	The attributes listed in the incidents tab are same as available in NNMi Incidents form. Click  (the <b>Open</b> 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 <i>Help for NNMi Incidents Form</i> .

### Analysis Pane:

Information shown in the Analysis Pane of Incidents tab is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## VFI form: Custom Attributes Tab

The VFI form provides details about the selected VFI. Custom Attributes tab displays the set of name-value pairs of custom attributes associated with VFIs. You can set Custom Attributes using the webservice calls.

### Custom Attributes

Attribute	Description
Name Attributes	Name of the Custom Attribute defined by using the web services.
Value	Value assigned to the Custom Attribute by using the web services.

### Analysis Pane

Analysis Pane is not implemented for the Custom Attributes tab.

## VFI Form: Registration tab

The VFI form provides details about the selected VFI. Registration tab shows details about when a selected VFI was created and when the status was last modified.

### Registration Table

Attribute	Description
Create Time	Date and time on which the selected VFI was created.

### Registration Table, continued

Attribute	Description
Status Last Modified	Status Last Modified shows the date and time on which the status of the selected VFI was last modified.



### Analysis Pane

Analysis Pane is not implemented for the Registration tab.

## SDP Form

The SDP form provides details of the SDP that logically directs the traffic from one source to destination through a unidirectional service tunnel.

### Basic Attributes

Attribute	Description
SDP ID	The unique identifier of the selected SDP.
Source Node	The selected SDP starts from this node. Click  (the <b>Lookup</b> icon) to view more information about the Source Node.
Destination Node	Name of the destination node of the selected SDP. Click  (the <b>Lookup</b> icon) to view more information about the Destination Node.
Status	Displays the status of the selected SDP.
Management Mode	<p>The NNM iSPI for MPLS supports management of SDPs. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Managed</b> – The selected SDP is managed.</li> <li>• <b>Not Managed</b> – The selected SDP is not managed.</li> <li>• <b>Out of Service</b> – 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 is temporarily out of service.</li> </ul> <p><b>Note:</b> <i>Out of Service</i> is an NNMi supported mode. The NNM iSPI for MPLS does not allow users to store 'Out of Service' value from the Management Mode list</p> <p>For more information, see the <i>Help for NNMi; View the Management Mode for an Object in Your Network</i>.</p>
Management Type	Inheritance type for the selected SDP. An MPLS object inherits management mode of its container object. Management Type displays the type of container object from which the selected

### Basic Attributes, continued

Attribute	Description
	<p>SDP has inherited the Management Mode. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Node Inherited</b> - The selected SDP inherits management mode from a node.</li> <li>• <b>Self</b> - The selected SDP is <b>Not Managed</b> but it belongs to a <b>Managed</b> node, participating in a <b>Managed</b> VPLS.</li> </ul> <p><b>Note:</b> You cannot change Management Type of an <b>Not Managed</b> SDP to <b>Self</b> if it is <b>VPLS Inherited</b>.</p> <ul style="list-style-type: none"> <li>• <b>Regional Inherited</b>- One of the SDP belonging to a VPLS at Regional level is <b>Not Managed</b>. In addition, these SDPs are not affected by management changes made at the Global level.</li> </ul> <p><b>Note:</b> '<b>Regional Inherited</b>' type is only applicable for a <b>Global Manager</b>. This is because a SDP <b>Not Managed</b> in a regional manager has a direct effect on the Global Manager. However, any VPLS managed/not managed at Global level will not affect a SDP that is '<b>Regional Inherited</b>' .</p>
Delivery Type	Name of the delivery type for the selected SDP.
Number of Services	The number of services associated with the SDP.
Create Time	Date and time on which the selected SDP was created.
Status Last Modified	Status Last Modified shows the date and time on which the status for the selected SDP was last set.

**Related Topics:** [SDPBinds Tab](#), [Status Tab](#), [Conclusions Tab](#), [Incidents Tab](#), [Registration Tab](#)

#### Analysis Pane:







Information shown for SDP form is same as that in SDP Inventory. For more information, see [SDP Inventory](#).

## SDP Form: SDPBinds Tab

The SDP form provides details of the SDP that logically directs the traffic from one source to destination through a unidirectional service tunnel. You can use the SDPBinds tab to view the SDP details.

#### SDPBinds table

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

Attribute	Description
	<p> <b>No Status</b> - The status of a SDPBind is 'No Status' when:</p> <ul style="list-style-type: none"> <li>• The SDPBind is newly created and not polled.</li> <li>• When a SDPBind is not mapped to any interface and hence, not polled.</li> </ul> <p> <b>Normal</b> - The status of the SDPBind is Up.</p> <p> <b>Unknown</b> - The SDPBind is not reachable or not responding.</p> <p> <b>Critical</b> - The status of the SDPBind is Down.</p>
Service Id	The Service Id number for the selected SDPBind.
Service Type	The Service Type for the selected SDPBind.
Bind Type	The Bind type for the selected SDPBind.
Delivery Type	The delivery type for the selected SDPBind
Service Name	Name of the service.
Destination Node	Name of the destination node for the selected SDP.
SDP ID	The unique identifier for the selected SDP.
Management Mode	<p>Management mode of the selected SDPBind. Possible values are:</p> <p> <b>Managed</b> - The selected SDPBind is managed.</p> <p> <b>Not Managed</b> - The selected SDPBind is not managed.</p>



**Analysis Pane:**

The Analysis Pane for SDPBind Tab is same as available in the SDPBind form. For more information, see [SDPBind Form](#).



## SDP Form: Status Tab

The SDP form provides details of the SDP that logically directs the traffic from one source to destination through a unidirectional service tunnel. You can use the Status tab to view the status summary of the selected SDP.

**Overall Status Table**

Attribute	Description
Status	<p>Overall status for the current SDP. Possible values are:</p> <p> <b>No Status</b> - The status of a SDP is 'No Status' when:</p> <ul style="list-style-type: none"> <li>• The SDP is newly created and not polled.</li> <li>• When a SDP is not mapped to any interface and hence, not polled.</li> </ul> <p> <b>Normal</b> - The status of the SDP is Up.</p>

### Overall Status Table, continued

Attribute	Description
	 <b>Unknown</b> - The SDP is not reachable or not responding.  <b>Critical</b> - The status of the SDP is Down.
Last Modified	Date and time on which the status was last set.

### Status History

Attribute	Description
Status	List of last thirty status updates for the selected SDP. For more information, see <i>NNMi Status tab</i> .
Time Stamp	Time when the selected SDP was last modified.

#### Analysis Pane:

Analysis Pane is not implemented for the Status tab.

## SDP Form: Conclusions Tab

The SDP form provides details of the SDP that logically directs the traffic from one source to destination through a unidirectional service 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 SDP.

### Conclusions Table

Attribute	Description
Status	The status of the selected SDP is dependent on the status of the interface on the selected SDP. For more information, see <a href="#">SDP Form: Status Tab</a> .
Time Stamp	The Time Stamp data is the time when the status of the SDP is last set.
Conclusions	<p>The conclusion is set by the Causal Engine after the status calculation. Possible conclusions are:</p> <ul style="list-style-type: none"> <li>• <b>MplsSdpNoStatus</b></li> <li>• <b>MplsSdpDown</b></li> <li>• <b>MplsSdpUp</b></li> <li>• <b>MPLSSdpUnkown</b></li> </ul> <p>Example: The conclusion MplsSdpDown sends an MplsSdpDown incident</p>


#### Analysis Pane:

Analysis Pane is not implemented for the Conclusions tab.

## SDP Form: Incidents Tab

The SDP form provides details of the SDP that logically directs the traffic from one source to destination through a unidirectional service tunnel. The Incidents tab is useful for obtaining a quick summary of the incident and problem description for the SDP.

### Incidents table:

Attribute	Description
Incidents Attributes	The attributes listed in the incidents tab are same as available in NNMi Incidents form. Click  (the <b>Open</b> 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 <i>Help for NNMi Incidents Form</i> .

### Analysis Pane:

Information shown in the Analysis Pane of Incidents tab is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## SDP Form: Registration Tab

The SDP form provides details of the SDP that logically directs the traffic from onsource to destination through a unidirectional service tunnel. Registration tab shows details about when a selected SDP was created and when the status was last modified.

### Registration Table

Attribute	Description
Create Time	Date and time on which the selected SDP was created.
Status Last Modified	Status Last Modified shows the date and time on which the status of the selected SDP was last modified.

### Analysis Pane

Analysis Pane is not implemented for the Registration tab.

## SDPBind Form

The SDPBind form provides details of the service binded to the SDP.

### Basic Attributes





Attribute	Description
Destination IP Address	The destination IP address for the selected SDP.

### Basic Attributes, continued

Attribute	Description
Status	Displays the status of the selected SDPBind.
Management Mode	<p>The NNM iSPI for MPLS supports management of SDPBinds. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Managed</b> – The selected SDPBind is managed.</li> <li>• <b>Not Managed</b> – The selected SDPBind is not managed.</li> <li>• <b>Out of Service</b> – 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 is temporarily out of service.</li> </ul> <div style="background-color: #e0e0e0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> <i>Out of Service</i> is an NNMi supported mode. The NNM iSPI for MPLS does not allow users to store 'Out of Service' value from the Management Mode list</p> </div> <p>For more information, see the <i>Help for NNMi; View the Management Mode for an Object in Your Network</i>.</p>
Management Type	<p>Inheritance type for the selected SDPBind. An MPLS object inherits management mode of its container object. Management Type displays the type of container object from which the selected SDPBind has inherited the Management Mode. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Node Inherited</b> - The selected SDPBind inherits management mode from a node.</li> <li>• <b>Self</b> - The selected SDPBind is <b>Not Managed</b> but it belongs to a <b>Managed</b> node, participating in a <b>Managed</b> VPLS.</li> </ul> <div style="background-color: #e0e0e0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> You cannot change Management Type of an <b>Not Managed</b> SDPBind to <b>Self</b> if it is <b>VPLS Inherited</b>.</p> </div> <ul style="list-style-type: none"> <li>• <b>Regional Inherited</b>- One of the SDPBind belonging to a VPLS at Regional level is <b>Not Managed</b>. In addition, these SDPBinds are not affected by management changes made at the Global level.</li> </ul> <div style="background-color: #e0e0e0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> '<b>Regional Inherited</b>' type is only applicable for a <b>Global Manager</b>. This is because a SDPBind <b>Not Managed</b> in a regional manager has a direct effect on the Global Manager. However, any VPLS managed/not managed at Global level will not affect a SDPBind that is '<b>Regional Inherited</b>' .</p> </div>



### Basic Attributes, continued

Attribute	Description
Bind Type	Name of the Bind type for the selected SDPBind.
Service ID	The Service Id number for the selected SDPBind.
Create Time	Date and time on which the selected SDPBind was created.
Status Last Modified	The status of the SDPBind is calculated whenever there is a change in topology. The status Last Modified shows date and time on which the status was last set.
SDP	The selected SDPBind belong to the specified SDP. Access the SDP form from the <b>Lookup</b> icon (  ).
VFI	The selected SDPBind belong to the specified VFI. Access the VFI form from the <b>Lookup</b> icon (  ).
VRF	The selected SDPBind belong to the specified VRF. Access the VRF form from the <b>Lookup</b> icon (  ).
VC LSP	The selected SDPBind belong to the specified VC LSP. Access the VC LSP form from the <b>Lookup</b> icon (  ).

**Related Topics:** [Status Tab](#), [Conclusions Tab](#), [Incidents Tab](#), [Registration Tab](#)

#### Analysis Pane:

For the SDPBind form, an Analysis Pane with SDPBind Summary, SDPBind Service data tab and SDP tab are displayed.

#### SDPBind Summary:

The SDPBind Summary provides the following information:

- Bind Type
- Service Id
- Status
- Source
- Description

#### SDPBind Service data:

The SDPBind Sample data provides the following information:

- Service Type
- VRF Status
- VRF Name
- VPN Name

OR

- Service Type
- VPLS Name
- VPLS Status
- L2VPN Name

**SDP tab**





The SDP tab provides the following information:

- Delivery Type
- Description
- Destination Node
- SDP ID
- Source Node
- Status

## SDPBind Form: Status Tab

The SDPBind form provides details of the service bound to the SDP. You can use the Status tab to view the status summary of the selected SDPBind.

**Overall Status Table**

Attribute	Description
Status	Overall status for the current SDPBind. Possible values are: <ul style="list-style-type: none"> <li> <b>No Status</b> - The status of a SDPBind is 'No Status' when:                             <ul style="list-style-type: none"> <li>• The SDPBind is newly created and not polled.</li> <li>• When a SDPBind is not mapped to any interface and hence, not polled.</li> </ul> </li> <li> <b>Normal</b> - The status of the SDPBind is Up.</li> <li> <b>Unknown</b> - The SDPBind is not reachable or not responding.</li> <li> <b>Critical</b> - The status of the SDPBind is Down.</li> </ul>
Last Modified	Date and time on which the status was last set.

**Status History**

Attribute	Description
Status	List of last thirty status updates for the selected SDPBind. For more information, see <i>NNMi Status tab</i> .
Time Stamp	Time when the selected SDPBind was last modified.

**Analysis Pane**

Analysis Pane is not implemented for the Status tab.

## SDPBind Form: Conclusions Tab

The SDPBind form provides details of the service bound to the SDP. 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 SDPBind.

### Conclusions Table

Attribute	Description
Status	The status of the selected SDPBind is dependent on the status of the interface on the selected SDPBind. For more information, see <i>SDPBind Form: Status Tab</i> .
Time Stamp	The Time Stamp data is the time when the status of the SDPBind is last set.
Conclusions	<p>The conclusion is set by the Causal Engine after the status calculation. Possible conclusions are:</p> <ul style="list-style-type: none"><li>• <b>MplsSdpBindNoStatus</b></li><li>• <b>MplsSdpBindDown</b></li><li>• <b>MplsSdpBindUp</b></li><li>• <b>MPLSSdpBindUnkown</b></li></ul> <p>Example: The conclusion MplsSdpBindDown sends an MplsSdpBindDown incident</p>


### Analysis Pane:

Analysis Pane is not implemented for the Conclusions tab.

## SDPBind Form: Incidents Tab

The SDPBind form provides details of the service bound to the SDP. The Incidents tab is useful for obtaining a quick summary of the incident and problem description for the SDPBind.

### Incidents table:

Attribute	Description
Incidents Attributes	<p>The attributes listed in the incidents tab are same as available in NNMI Incidents form. Click  (the <b>Open</b> 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.</p> <p>For more information, see the <i>Help for NNMI Incidents Form</i>.</p>

### Analysis Pane:

Information shown in the Analysis Pane of Incidents tab is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## SDPBind Form: Registration Tab

The SDPBind form provides details of the service bound to the SDP. Registration tab shows details about when a selected SDPBind was created and when the status was last modified.

### Registration Table

Attribute	Description
Create Time	Date and time on which the selected SDPBind was created.
Status Last Modified	Status Last Modified shows the date and time on which the status of the selected SDPBind was last modified.

### Analysis Pane

Analysis Pane is not implemented for the Registration tab.

## VPWS VPN Form

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

Use the VPWS VPN form to complete 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
Name, Number of PseudoWireVCs, Status, Status Last Modified	These attributes listed in the VPWS VPN form are same and available in the VPWS VPN inventory view. For more information, see <a href="#">VPWS VPN Inventory</a> .
Management Mode	The NNM iSPI for MPLS supports management of VPWS VPNs. Possible values are: <ul style="list-style-type: none"><li>• <b>Managed</b> – The selected VPWS VPN is managed.</li><li>• <b>Not Managed</b> – The selected VPWS VPN is not managed.</li></ul> <b>Note:</b> To modify the Management Mode, select "Managed" or "Not Managed" respectively from the <b>Management Mode</b> list of the VPWS VPN form.
Management Type	Inheritance type for the selected VPWS VPN. An MPLS object inherits management mode of its container object. Possible values are: <ul style="list-style-type: none"><li>• <b>Node Inherited</b></li><li>• <b>Self</b></li></ul>
Create Time	Date and time on which the selected VPWS VPN was created.

**Related Topics:** [PseudoWire VCs Tab](#), [VC IDs Tab](#), [PE Routers Tab](#), [Status Tab](#), [Conclusions Tab](#), [Custom Attributes Tab](#), [Registration Tab](#)

### Analysis Pane

Information shown for VPWS VPN form is same as that in VPWS VPN Inventory. 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 VCs 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 <a href="#">PseudoWire VC Form</a> .

### Analysis Pane

Information shown for PseudoWire VC tab is same as that in PseudoWire VC Inventory. For more information, see [PseudoWire VC Inventory](#).

## 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.



### Analysis Pane

Analysis Pane is not implemented for the VC ID tab.







## 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  Normal

### Basic Attributes, continued

Attribute	Description
	<ul style="list-style-type: none"> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul>
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 is displayed as a single string value. For more information, see <i>NNMi Help for Operator, Device Profile Form</i> .






### Analysis Pane

Information shown in the Analysis Pane of PE Routers is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.


## 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	<p>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:</p> <ul style="list-style-type: none"> <li> <b>No Status</b> - 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 'Not Managed mode, the derived status of the VPWS VPN is No Status.</li> <li> <b>Normal</b> - The status of all the PseudoWires VCs participating to form a VPWS VPN is Normal.</li> <li> <b>Unknown</b> - The status of all the PseudoWires VCs participating to form a VPWS VPN is Unknown.</li> <li> <b>Warning</b> - 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.</li> <li> <b>Minor</b> - The status of one or more PseudoWires VCs participating to form a</li> </ul>

### Overall Status Table, continued

Attribute	Description
	VPWS VPN is Critical.  <b>Critical</b> - The status of all the PseudoWires VCs participating to form a VPWS VPN is Critical.
Last Modified	Date and time on which the status was last set.

### Status History

Attribute	Description
Status	List of last thirty status updates for the selected MPLS object. For more information, see <i>NNMi Status tab</i> .
Time Stamp	Time when the status of the selected VPWS VPN was last modified.

### Analysis Pane

Analysis Pane is not implemented for the Status tab.

## VPWS VPN Form: Conclusions Tab

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

### Conclusions Table

Attribute	Description
Status	The derived status of the selected VPWS VPN. For more information, see <a href="#">VPWS-VPN Form: Status tab</a> .
Time Stamp	The time when the status of the VPLS VPN is last set.
Conclusions	The conclusions are set by the Causal Engine after the status calculation. Possible conclusions are: <ul style="list-style-type: none"> <li>• <b>VPWSCritical</b></li> <li>• <b>VPWSNormal</b></li> <li>• <b>VPWSUnknown</b></li> <li>• <b>VPWSMinor</b></li> <li>• <b>VPWSWarning</b></li> </ul>

### Analysis Pane

Analysis Pane is not implemented for the Conclusions tab.

## VPWS VPN Form: Custom Attributes

The VPWS VPN form provides details about the selected VPWS VPN. Custom Attributes tab displays the set of name-value pairs of custom attributes associated with VPWS VPNs. You can set Custom Attributes using the webservice calls.

### Custom Attributes

Attribute	Description
Name Attributes	Name of the Custom Attribute defined in the web services.
Value	Value assigned to the Custom Attribute in the web services.

### Analysis Pane

Analysis Pane is not implemented for the Custom Attributes tab.

## VPWS VPN Form: Registration Tab

The VPWS VPN provides details about the selected VPWS VPN.

### Registration Table

Attribute	Description
Create Time	Date and time on which the selected VPWS VPN was created.
Status Last Modified	Status Last Modified shows the date and time on which the status of the selected VPWS VPN was last modified.

### Analysis Pane

Analysis Pane is not implemented for the Registration tab.

## 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 on 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,	The attributes listed in the TE Form are same as available in the TE Tunnel Inventory.



### Basic Attributes, continued

Attribute	Description
Tail, Tail IP Address, Description, Status, and Bandwidth	For more information, see <a href="#">TE Tunnel Inventory</a> .
Management Mode	<p>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 NNM iSPI for MPLS shows the same values for TE Tunnels as that of the corresponding nodes. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Managed</b> – The node, interface, or address is managed by NNMi.</li> <li>• <b>Not Managed</b> – 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</li> <li>• <b>Out of Service</b> – 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.</li> </ul> <p><b>Note:</b> The NNM iSPI for MPLS does not support modification of Management Mode for TE Tunnel</p>
Management Type	Management type for TE Tunnel will always be <b>Node Inherited</b> .
Head Interface	The interface of the head node where the selected TE Tunnel is configured. To view the Head interface details, click  (the <b>Lookup</b> icon).
Setup Priority	<p>The priority used to determine if the selected TE Tunnel is eligible to be preempted.</p> <p>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.</p>
Hold Priority	<p>The holding priority value specifies the priority used when protecting the tunnel from preemption by other tunnels.</p> <p>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.</p>
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. Status Last Modified shows the date and time on which the status was last set.

For more information, see [Attributes Tab](#) , [Hops Tab](#) , [Status Tab](#) , [Conclusions Tab](#) , [Incidents Tab](#) , [Custom Attributes Tab](#) , and [Registration Tab](#).

## Analysis Pane

Information shown for TE Tunnel form is same as that in TE Tunnel Inventory. For more information, see [TE Tunnel Inventory](#).

## 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 of the head node device type for Cisco, Juniper, and Alcatel routers. The listed attributes are available from the Cisco, Juniper, and Alcatel MIBs.

### Supported Attributes for Cisco Nodes

Attribute	Description
fastReroute	If the tunnel is configured with the fastReroute attribute, the value is true. True is represented by <input checked="" type="checkbox"/> .
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 <input checked="" type="checkbox"/> .
isPersistent	If the tunnel is configured with the isPersistent attribute, the value is true. True is represented by <input checked="" type="checkbox"/> .
isPinned	If the tunnel is configured with the isPinned attribute, the value is true. True is represented by <input checked="" type="checkbox"/> .
mergingPermitted	If the tunnel is configured with the MergingPermitted attribute, the value is true. True is represented by <input checked="" type="checkbox"/> .
record Route	If the tunnel is configured with the recordRoute attribute, the value is true. True is represented by <input checked="" type="checkbox"/> .

### Supported Attributes for Juniper Nodes

Attribute	Description
adaptive	If the tunnel is configured with the adaptive attribute, the value is true. True is represented by <input checked="" type="checkbox"/> .
cspf	If the tunnel is configured with the cspf attribute, the value is true. True is represented by <input checked="" type="checkbox"/> .
fast-reroute	If the tunnel is configured with the fast-reroute attribute, the value is true. True is represented by <input checked="" type="checkbox"/> .
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 <input checked="" type="checkbox"/> .
preemptable	If the tunnel is configured with the preemptable attribute, the value is true.

### Supported Attributes for Juniper Nodes, continued

Attribute	Description
	The status of the flag is either true or false. True is represented by <input checked="" type="checkbox"/> .
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 <input checked="" type="checkbox"/> .
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 <input checked="" type="checkbox"/> .

### Supported Attributes for Alcatel Nodes

Attribute	Description
record-route	If the tunnel is configured with the record-route , the value is true. The status of the flag is either true or false. True is represented by <input checked="" type="checkbox"/> .
fast-reroute	If the tunnel is configured with the fast-reroute attribute, the value is true otherwise it is false. True is represented by <input checked="" type="checkbox"/> .
decrementTtl	If the tunnel is configured with the decrementTtl attribute, the value is true. True is represented by <input checked="" type="checkbox"/> . When the value is set to 'true', the ingress ESR <sup>1</sup> includes the TTL <sup>1</sup> of the IP packet into the label and each transit ESR decrements the TTL in the label. If the value is set to 'false', the ESR ignores the IP packet TTL and writes value '225' into the label.
bwProtect	If the tunnel is configured with the bwProtect attribute, the value is true. True is represented by <input checked="" type="checkbox"/> . If the value is set to 'true', bandwidth protection is enabled on an LSP. Enabling bandwidth protection ensures that an LSP is allocated fixed bandwidth. Each time this LSP is used for any service, the bandwidth allocated to that service is deducted from bandwidth reserved for the LSP. After the bandwidth is exhausted on the LSP, the ESR will indicate that the LSP has exhausted its resources. Default value for bwProtect is 'false'.
fRNodeProtect	If the tunnel is configured with the fRNodeProtect attribute, the value is true. True is represented by <input checked="" type="checkbox"/> . Setting value of fRNodeProtect to 'true' enables protection against the failure of a node on the LSP. Default value for fRNodeProtect is 'true'.
cspf	If the tunnel is configured with the cspf attribute, the value is true. True is represented by <input checked="" type="checkbox"/> .

<sup>1</sup>Edge Service Router  
<sup>1</sup>Time To Live

### Supported Attributes for Alcatel Nodes, continued

Attribute	Description
adaptive	If the tunnel is configured with the adaptive attribute, the value is true. True is represented by <input checked="" type="checkbox"/> . When the value is set to 'true', adaptive enables make-before-break functionality <sup>1</sup> for the P2MP <sup>1</sup> LSP.
operFastReroute	If the tunnel is configured with the operFastReroute attribute, the value is true. True is represented by <input checked="" type="checkbox"/> . The value of operFastReroute specifies whether the fast-reroute is enabled or disabled for any operational LSP.
fRObject	If the tunnel is configured with the fRObject attribute, the value is true. True is represented by <input checked="" type="checkbox"/> . Value of fRObject specifies whether fast -reroute for LSPs using ' Facility Backup <sup>1</sup> ' is signaled with or without the fast reroute object. The value of fRObject is ignored if fast-reroute is disabled for the LSP or if the LSP is using ' One-to-One Backup <sup>1</sup> '.

#### Analysis Pane

Analysis Pane is not implemented for the Attributes tab.

## 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 intermediate router in the tunnel path.

#### Basic Attributes

Attribute	Description
Hop #	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:


<sup>1</sup>It is a configuration in which a new connection path is established before the previous connection is opened to prevent an open circuit.

<sup>1</sup>Point to Multipoint is a communications network commonly used for wireless and telephony networks. Point to Multipoint provides a path from a single location to multiple locations.

<sup>1</sup>This is a backup approach where a single backup is maintained for a set of LSPs.

<sup>1</sup>This is a backup approach where a separate backup path is maintained for each LSP passing through a facility.

### Basic Attributes, continued

Attribute	Description
	<ul style="list-style-type: none"> <li>• <b>No Data Available</b> - 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.</li> <li>• <b>Virtual Interface</b> - Whenever an interface on the head node is not discovered, the value is Virtual Interface. This value is applicable only for the Cisco devices.</li> </ul> <p>Click  (the <b>Open</b> icon) to view details about the selected Outgoing-IfName.</p>
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 <b>Unknown</b> .
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 <b>Unknown</b> .
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 <b>Unknown</b> .




### Analysis Pane

Analysis Pane is not implemented for the Hops tab.

## 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	<p>Overall status of the TE Tunnel. Possible values are :</p> <ul style="list-style-type: none"> <li> <b>Normal</b> - If the status of the TE Tunnel is Up, the status of the TE Tunnel is Normal.</li> <li> <b>Critical</b> - If the status of the TE Tunnel is Down, the status of the TE Tunnel is Critical.</li> <li> <b>Unknown</b> - 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.</li> </ul>
Status Last Modified	Status Last Modified shows the date and time on which the status of the selected TE Tunnel was last set.

### Status History

Attribute	Description
Status	List of the last thirty status updates for the selected MPLS object. For more information, see <i>NNMi Status tab</i> .
Time Stamp	Time when the status of the selected TE tunnel was last modified.

### Analysis Pane

Analysis Pane is not implemented for the 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 <a href="#">TE Tunnel: Status Tab</a> .
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: <ul style="list-style-type: none"> <li>• <b>MplsTunnelDown</b></li> <li>• <b>MplsTunnelUp</b></li> <li>• <b>MplsTunnelUnknown</b></li> <li>• <b>MPLSTETunnelReroute</b></li> </ul>


### Analysis Pane

Analysis Pane is not implemented for the Conclusions tab.

## 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 <b>Open</b> 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.

### Incidents Table , continued

Attributes	Description
	For more information, see <a href="#">Viewing MPLS Incidents</a> .

A node or an interface down in NNMi is correlated to Tunnel Down or Tunnel Reroute. If a node or an interface is down, the corresponding TE Tunnel will also generate a 'Reroute' or 'Down incidents '

To view the correlation, follow these steps:

1. Go to **TE tunnel inventory**.
2. Select the TE Tunnel for which you want to view the correlation, and then click  (the **Open** icon). The TE Tunnel form opens.
3. Select the **Incidents** tab.
4. Open the 'down' or 'Reroute' incident.
5. Click the **Correlated Children** tab.

For more information on Correlated Children see, *Incident Form:Correlated Children Tab* and *Correlation Rule Example* in the *NNMi Online Help for Operators*.

### Analysis Pane

Information shown in the Analysis Pane of Incidents is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## TE Tunnel Form: Custom Attributes

The TE Tunnel form provides details about the selected TE Tunnel. Custom Attributes tab displays the set of name-value pairs of custom attributes associated with TE Tunnels. You can set Custom Attributes using the webservice calls.

### Custom Attributes

Attribute	Description
Name Attributes	Name of the Custom Attribute defined in the web services.
Value	Value assigned to the Custom Attribute in the web services.

### Analysis Pane

Analysis Pane is not implemented for the Customs Attribute tab.

## 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 on which the selected TE Tunnel was created.
Last Modified	Date and time of when the selected TE Tunnel was last modified.






## Analysis Pane

Analysis Pane is not implemented for the Registration tab.

# VC LSPs Form

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

## Basic Attributes

Attribute	Description
VC ID	<p>The unique index identifier for each virtual circuit.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note:</b> VC ID is set to Not Applicable for a BGP-based VPLS.</p> </div>
PSN Type	The kind of Packet Switched Network (PSN) for the selected VC LSP.
Source	<p>The name of a node. The selected PseudoWire VC starts from this node. Click  (the <b>Lookup</b> icon) to view more information about the source node.</p>
Source Address	The IP Address of the source node. The source node is one of the endpoints of the PseudoWire VC.
Destination	<p>The name of a node. The selected PseudoWire VC terminates at this node. Click  (the <b>Lookup</b> icon) to view more information about the node.</p>
Destination Address	The IP Address of the destination node.
Status	<p>The status of the PseudoWire VC. Possible values are:</p> <ul style="list-style-type: none"> <li> <b>Normal</b> - The status of both the LSPs is Normal.</li> <li> <b>Critical</b> - The status of any one or both the LSPs is Critical.</li> <li> <b>Unknown</b> - The status of any one or both the LSPs is Unknown.</li> </ul>
ACType	This shows the type of Attachment Circuit.
VFI	This shows the name of the associated VFI.
AC Interface	The attachment circuit or the data link of the selected VC LSP. For more information, see the <i>Help for NNMi, Interface Form</i> .
AC Name	The name of the attachment circuit or the data link of the selected VC LSP.



### Basic Attributes, continued

Attribute	Description
Encapsulation Type	<p>The kind of service carried in the selected PseudoWire VC. For example, the services are ATM, Frame Relay, or Ethernet.</p> <p>If both the endpoints (PE1 and PE2) are discovered but the status of the LSPs is not Normal, the value of Encapsulation Type is <b>Others</b>.</p>
Management Mode	<p>The NNM iSPI for MPLS supports management of VC LSPs. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Managed</b> – The selected VC LSP is managed.</li> <li>• <b>Not Managed</b> – The selected VC LSP is not managed.</li> </ul> <div style="background-color: #e0e0e0; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> To modify the Management Mode, select "Managed" or "Not Managed" respectively from the <b>Management Mode</b> list of the VC LSP form.</p> </div> <p><b>Out of Service</b> –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 is temporarily out of service.</p> <div style="background-color: #e0e0e0; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> <i>Out of Service</i> is an NNMi supported mode. The NNM iSPI for MPLS does not allow users to select 'Out of Service' value from the Management Mode list.</p> </div> <p>For more information, see <i>Help for NNMi; View the Management Mode for an Object in Your Network</i>.</p>
Management Type	<p>Inheritance type for the selected VC LSP. An MPLS object inherits management mode of its container object. Management Type displays the type of container object from which the selected VC LSP has inherited the Management Mode. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Node Inherited</b> - The selected VC LSP belongs to an <b>Not Managed</b> node.</li> <li>• <b>PseudoWire VC Inherited</b> - The selected VC LSP belongs to a <b>Managed</b> node participating in an <b>Not Managed</b> VPN.</li> <li>• <b>Self</b></li> </ul> <div style="background-color: #e0e0e0; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> You cannot change Management Type of an <b>Not Managed</b> VC LSP to <b>Self</b> if it is <b>PseudoWire Inherited</b></p> </div> <ul style="list-style-type: none"> <li>• <b>Regional Inherited</b>- One of the VC LSP belonging to a</li> </ul>

### Basic Attributes, continued

Attribute	Description
	<p>Pseudowire VC at Regional level is <b>Not Managed</b>. In addition, these VC LSPs are not affected by management changes made at the Global level.</p> <p><b>Note: 'Regional Inherited'</b> type is only applicable for a <b>Global Manager</b>. This is because a VC LSP <b>Not Managed</b> in a regional manager has a direct effect on the Global Manager. However, any Pseudowire VC managed/not managed at Global level will not affect a VC LSP that is <b>'Regional Inherited'</b></p>
Create Time	Date and time on which the selected VC LSP was created.
Status Last Modified	Status Last Modified shows the date and time on which the status for the selected VC LSP was last set.

#### Analysis Pane

Information shown for VC LSP form is same as that in PseudoWire VC Form: VC LSPs Tab. For more information, see [PseudoWire VC form: VC LSPs Tab](#).

## VC LSP Form: ACs Tab

The VC LSPs form provides details about the selected VC LSP. You can use the ACs tab to view the attachment circuit of the selected VC LSP.

#### ACs Table:

Attribute	Description
Status	This attribute listed in the ACs tab is same as available in the NNMi Interface form. For more information, see <i>Help for NNMi Interface form</i> .
AC Interface	The attachment circuit or the data link of the selected VC LSP. For more information, see the <i>Help for NNMi, Interface Form</i> .
ACType	This shows the type of attachment circuit.
PE Node	The name of the PE node where the PE interface is configured.




#### Analysis Pane:

Information shown in the Analysis Pane is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## 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:  <b>Normal</b>  <b>Critical</b>  <b>Unknown</b>
Last Modified	Date and time on which 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 <i>NNMi Status tab</i> .
Time Stamp	Time at which the selected VC LSP was last modified.

### Analysis Pane

Analysis Pane is not implemented for the 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 <a href="#">VC LSP Form: Status Tab</a> .
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: <ul style="list-style-type: none"> <li>• <b>MplsVCLSPUp</b></li> <li>• <b>MplsVCLSPDown</b></li> <li>• <b>MplsVCLSPUnknown</b></li> </ul> The VC LSP down conclusion generates the PseudoWire VC incident to send the alert for the status. For example, MplsVCLSPDown generates the MplsPseudoWireVCDown incident.

### Analysis Pane

Analysis Pane is not implemented for the Conclusions tab.

## 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 on which the selected MPLS object instance was created.
Last Modified	Date when the selected VC LSP was last modified.

### Analysis Pane

Analysis Pane is not implemented for the Registration tab.


## Monitored LSP Form

The monitored LSP form provides details about selected LSP .






Use the LSP form for the following tasks:

- Monitor the status of the LSPs.
- View the service type associated with the LSPs.
- View the node and the services to which an LSP is mapped.

### Basic Attributes

Attributes	Description
Status	Each row in the Monitored LSP Inventory represents a service being monitored. This column shows direct impact of status of an LSP on the selected service.
Management Mode	Management mode of the selected LSP
Service Type	Type of service, to which the LSP is mapped. Services available are: <ul style="list-style-type: none"><li>• VRF</li><li>• Pseudowire VC</li></ul>
LSP Name	Name of the selected LSP.
Source VRF	Source VRF from where the LSP originates. Click  (the <b>Lookup</b> icon) to view the Analysis Pane of the VRF or to open the <a href="#">VRF form</a> . This field is blank if the Service Type of the LSP is Pseudowire VC.

### Basic Attributes, continued

Attributes	Description
Source VC	Source VC from where the LSP originates. Click  (the <b>Lookup</b> icon) to view the Analysis Pane of the VC LSP or to open the <a href="#">VC LSP form</a> . This field is blank if the Service Type of the LSP is VRF.
Source Node	Source node from where the LSP originates. Click  (the <b>Lookup</b> icon) to view the Analysis Pane of the node or to open the <a href="#">Node form</a> .
Destination VRF	Destination VRF where the LSP ends. Click  (the <b>Lookup</b> icon) to view the Analysis Pane of the VRF or to open the <a href="#">VRF form</a> . This field is blank if the Service Type of the LSP is VC.
Destination VC	Destination VC where the LSP ends. Click  (the <b>Lookup</b> icon) to view the Analysis Pane of the VC LSP or to open the <a href="#">VC LSP form</a> . This field is blank if the Service Type of the LSP is VRF.
Destination Node	Destination node where the LSP ends. Click  (the <b>Lookup</b> icon) to view the Analysis Pane of the node or to open the <a href="#">Node form</a> .

For more information see, [Status tab](#), [Conclusion tab](#), and [Incidents tab](#) .

#### Analysis Pane

Analysis Pane is same for Monitored LSP form is same as available in the [Monitored LSP Inventory](#) .

## Monitored LSP Form: Status Tab

You can use the Status tab to view the status summary of the monitored LSP.

#### Overall Status History

Attribute	Description
Status	Status of the Monitored LSP.
Time Stamp	Date and time when the LSP went up, down, or was re-routed.

#### Analysis Pane

Analysis Pane is not implemented for the Status tab.

## Monitored LSP Form: Conclusions Tab

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 monitored LSP.

### Conclusions Table

Attribute	Description
Status	Status of the Monitored LSP.
Time Stamp	Date and time when the LSP went up, down, or was re-routed.
Conclusion	Shows if an LSP is one of the following: <ul style="list-style-type: none"><li>• LSPUp</li><li>• LSPDown</li><li>• LSP Rerouted</li></ul>

### Analysis Pane

Analysis Pane is not implemented for the Conclusions tab.

## Monitored LSP Form: Incident Tab

The Incidents tab is useful for obtaining a quick summary of the incident and problem description for Monitored LSP. You can click on the incidents to open the **Incident Form**. For more information see, *Incident Form* in *NNMi Online Help*.

### Incident Table

Attribute	Description
Severity	Severity of the incident. An incident is <b>Critical</b> if an LSP is Down or is a <b>Warning</b> if the LSP is Re-routed.
Lifecycle State	Identifies where the incident is in the incident lifecycle. For more information see, <i>Incident Form</i> in <i>NNMi Online Help</i> .
Last Occurrence Time	Time and date when the incident last occurred.
Correlation Nature	The incident's contribution to a root-cause calculation, if any. For more information see, <i>Incident Form: General Tab</i> in <i>NNMi Online Help</i> .
Source Node	Indicated the node on which the incident was generated.

### Incident Table, continued

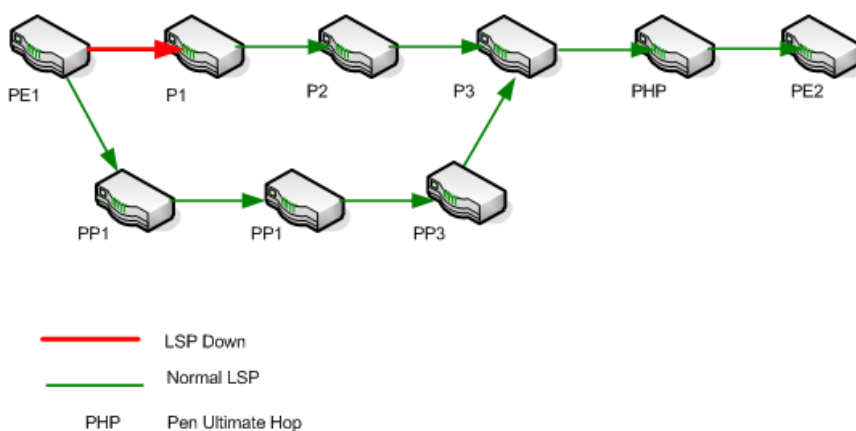
Attribute	Description
Messages	Relevant message that provides information about the incident.

Click the incident to open the Incident Form. For more information see, *Incident Form* in the *NNMi Online Help*.

### LSP Re-route Scenarios

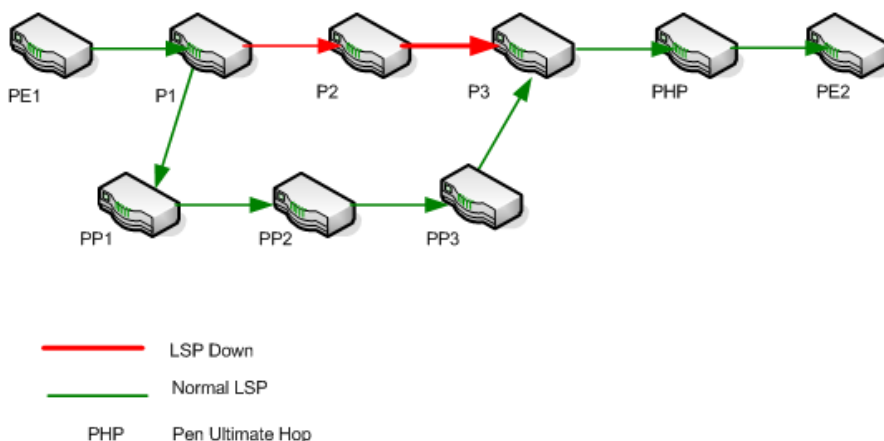
To understand the cases in which an LSP re-route incident will be generated, see the following examples:

- LSP Re-routed at the PE



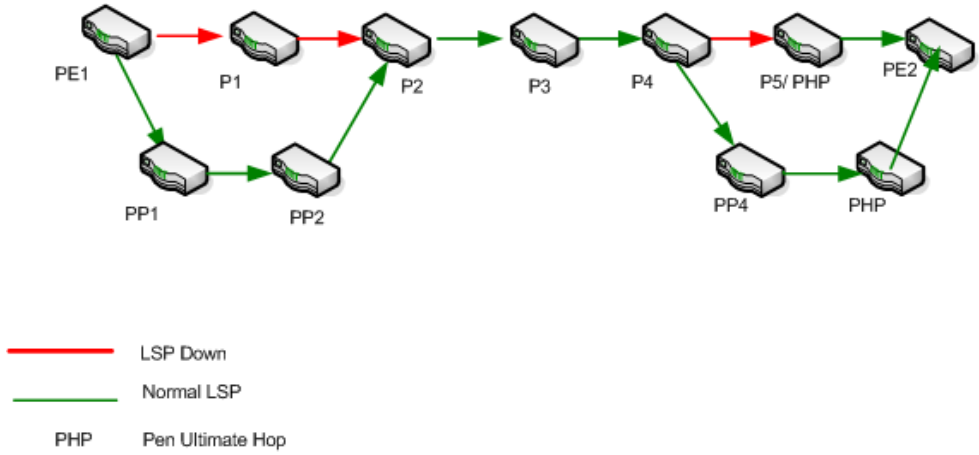
In the example, the fault occurred at Provider Edge router (PE1) and the LSP got re-routed to alternate Provider routers ( PP1-PP2-PP3). In this case, a **Re-route** incident is generated for the LSP originating from PE1.

- LSP Re-routed at a Provider router (P router)



In the example, the fault occurred at Provider router (P1) and the LSP got re-routed to alternate Provider routers ( PP1-PP2-PP3). In this case, a Re-route incident is generated for the LSP originating from P1.

- LSP Re-routed at PE and again at a P router



The re-route incident is generated only the first time, in this case the LSP is first Re-routed at PE1 and then again at P4. The re-route incident is generated at PE1.

**Analysis Pane**

Information shown in the Analysis Pane is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## Interface Form

The Interface form provides details about the selected interface. For more information, see *NNMi Interface Form*.

**Basic Attributes**

Attribute	Description
Interface attributes	The attributes listed in the Interface form are available from NNMi Interface form. For more information, see the Help for <i>NNMi Interface Form</i> .

**Analysis Pane**

Information shown in the Analysis Pane of Interface form is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## MDT Form

The MDT form provides details about the selected Multicast Distribution Tree (MDT). The MDT form provides the complete data flow from one CE node to another CE node. The data flows from the CE - PE node to PE-CE node. The PE routers are configured with multicast-enabled VRFs (MVRF) and use the multicast services to transmit data. You can view the multicast traffic by starting the iSPI for IP Multicast.



### MDTs Attributes

Attribute	Description
Customer Source	The IP address of the source that 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 type 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.

#### Analysis Pane

Information shown for MDTs form is same as that in MVPN Inventory. For more information, see [MVPN Inventory](#).

## Node Form: VRF Tab

The NNMi Node form provides details about the selected node. The **VRF** tab 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 <a href="#">VRF Form</a> .

#### Related Topic:

[LSR Inventory](#)

#### Analysis Pane

Information shown in the Analysis Pane for VRF Tab is same as available in the VRF form. For more information, see [VRF Form](#).

## Node Form: TE Tunnel Tab

The NNMi Node form provides details about the selected node. The **TE Tunnel** tab 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

### Basic Attributes, continued

Attribute	Description
	to determine all TE tunnels in which this node participates. For more details, see <a href="#">TE Tunnel Form</a> .

#### Related Topic:

[LSR Inventory](#)

#### Analysis Pane

Information shown for the TE Tunnel tab is same as that in TE Tunnel Inventory. For more information, see [TE Tunnel Inventory](#).

## Node Form: PseudoWire VC LSP Tab

The Node form provides details about the selected node. The **VC LSP** tab 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 <a href="#">PseudoWire VC Form</a> .

#### Related Topic:

[LSR Inventory](#)

#### Analysis Pane

Information shown in the Analysis Pane of PseudoWire VC LSP Tab is same as available in "[PseudoWire VC Form: VC LSPs Tab](#)" on page 77.

## Node Form: VPLS VPNs Tab

The Node form provides details about the selected node. In addition, the **VPLS VPNs** tab 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 <a href="#">VPLS VPN view</a> .

#### Related Topic:

[LSR Inventory](#)

#### Analysis Pane

Information shown for VPLS VPN tab is same as that in VPLS VPN Inventory. For more information, see [VPLS VPN Inventory](#).

## Node Form: VPWS VPNs Tab

The NNMi Node form provides details about the selected node. The **VPWS VPN** tab 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 <a href="#">VPWS VPN view</a> .

### Related Topic:

[LSR Inventory](#)

### Analysis Pane

Information shown for VPWS VPN tab is same as that in VPWS VPN Inventory. For more information, see [VPWS VPN Inventory](#).


## 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
Status, IfName, IfAlias, IfType	The attributes listed in the PE Interface tab are same as available in NNMi Interface form. For more information for the attributes, see the Help for <i>NNMi Interface Form</i> .
VRF Name	The name is obtained from the PE router during the NNM iSPI for MPLS discovery.
VPN Name	Name of the VPN. You can update the system generated VPN Name from the forms. For more details, see <a href="#">L3 VPN Form</a> .

### To view the L3 VPN PE Interface tab, follow the steps:

1. From NNMi Workspace, click **Inventory-> Nodes view**.  
**OR**  
From iSPI for MPLS workspace, click **LSR Inventory**.
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.

### Related Topic:

[LSR Inventory](#)

### Analysis Pane

Information shown in the Analysis Pane of L3 VPN PE Interface tab is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## Node Form: LDP Attributes Tab

The NNMi Node form provides details about the selected node. The LDP Attributes tab provides LDP details of the selected node. Click on each Attribute to open the **LDP Attribute Form**. This form provides details about the selected attribute along with its description. The following table provides the possible values for each attribute

### Basic Attributes

Attribute Name	Attribute Value
Label Retention Mode	The possible Label Retention Mode values are : <ul style="list-style-type: none"> <li>• Conservative</li> <li>• Liberal</li> </ul>
Entity Operational Status	The possible Entity Operational Status values are: <ul style="list-style-type: none"> <li>• 0: When the status is unknown.</li> <li>• 1: When the status is enabled.</li> <li>• 2: When the status is disabled.</li> </ul>
LDP Port	There are no fixed set of Values for LDP port.
Label Distribution Method	The possible values for Label Distribution Method are: <ul style="list-style-type: none"> <li>• 1: downstreamOnDemand</li> <li>• 2: downstreamUnsolicited</li> </ul>
Max Pdu Length	The possible range is between 0-65535.
Hop Count	The possible range is between 0-255.
Path Vector Limit	The possible range is between 0-255.

### Analysis Pane

Analysis Pane is not implemented for LDP Attributes tab.

## PE Interface Form: L3 VPN Tab

The NNMi PE Interface form provides details about the selected 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 L3 VPN.

### L3 VPN Attributes

Attribute	Description
L3 VPN Name	The L3 VPN name. You can update the system generated VPN Name from the forms.



### L3 VPN Attributes, continued

Attribute	Description
	For more details, see <a href="#">VPN Form</a> .
VRF Name	The name of a VRF.

### L3 VPN 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 <i>NNMi Interface Form</i> .
CE Node	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- > L3 VPN Inventory**.
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.

#### Analysis Pane

Information shown in the Analysis Pane of L3 VPN Tab is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*

## CE Interface Form: L3 VPN Tab

The NNMi CE Interface form contains details about the selected node. 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 <a href="#">L3 VPN Form</a> .
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 <i>NNMi Interface Form</i> .
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:

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

### Analysis Pane



Information shown in the Analysis Pane of L3 VPN Tab is inherited from the HPE Network Node Manager i-Software (NNMi). For more information, see *About the Analysis Pane* in *NNMi Online Help*.

## Viewing the NNM iSPI for MPLS Incidents

(See, *Monitoring Incidents for Problems*, in *NNM Online Help: Help for Operators* before you begin this topic)

The NNM iSPI for MPLS generates the incidents if any fault or change is detected on 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 Inventory**).
  2. Select an L3 VPN and click  (the **Open** icon).
  3. Select an Incident from the incident tab and click  (the **Open** icon) 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 NNM 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

## Incidents Generated for MPLS-enabled Nodes and Objects

### MPLS Incidents

Incident Name	Description
MplsVFIDown	This incident is generated when the VFI belonging to the specified VPLS goes down.
MplsSdpDown	This incident is generated when a SDP between the specified source node and destination ip address is down.
MplsSdpBindDown	This incident is generated when the SDPBind between the specified SDP and its service is down.
MplsTETunnelDown	This incident is generated when TE Tunnel between the source and destination of the selected node is down. When generated, this incident displays "TE Tunnel <i>\$TunnelName</i> is Down between <i>\$TunnelSrcName</i> and <i>\$TunnelDestName \$RCA</i> ". In this case, <i>\$TunnelName</i> is the name of the TE Tunnel and <i>\$RCA</i> is the node and interface name where the TE Tunnel went down.
MplsTETunnelUp	This incident is generated when a TE Tunnel is up. This incident is a part of the MPLS Traffic Engineering family.
MplsTETunnelReroute	This incident is generated when TE Tunnel between the two end points is rerouted. When generated, this incident displays the "TE Tunnel <i>\$TunnelName</i> is Rerouted <i>\$RCA</i> " message. In this case, <i>\$TunnelName</i> is the name of the TE Tunnel and <i>\$RCA</i> is the node and interface name where the reroute occurred in the path.
MplsVRFDOWN	The VRF incident is generated when the status of the selected VRF is down. It 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. This incident is also generated for VRF Lite when the status of the selected VRF Lite is down. Although, in case of a VRF Lite down the corresponding message displayed for the incident mentions that a VRF Lite is down.

### MPLS Incidents, continued

Incident Name	Description
MplsVRFUp	The VRF incident is generated when the status of the selected VRF is up. It 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 up. This incident is also generated for VRF Lite when the status of the selected VRF Lite is up. Although, in case of a VRF Lite up the corresponding message displayed for the incident mentions that a VRF Lite is up.
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.
LSPReRoute	Generated when an LSP is re-routed.
LSPCritical	Generated when an LSP is down.

**Note:** The LSP service impact incidents pick up the custom attributes of the corresponding source and destination services. For more information, see *Incident Form: Custom Attribute Tab* in *NNMi Online Help for Operators*.

## Service Impact Incidents

The NNM iSPI for MPLS lists the Service Impact incidents for the selected L3 VPNs or L2 VPNs. The service impact incidents do not change the status of the L3 VPNs or L2 VPNs. You can view the Service Impact incidents from the **NNMi Workspaces-> Incident Browsing -> Service Impact incidents**.

The root-cause incident generated by NNMi generates a service impact incident. This incident provides details of the affected L3 VPN or L2 VPN on the network. For example, an Interface Down incident can change the status of a CE node participating in an L3 VPN. 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

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, Connection Down or



### MPLS Service incidents, continued

Incident Name	Description
	VRF Lite Down) is detected on a CE node or a shadow router. This is a service impact incident.
MplsServiceImpacted	Generated when the LSP belonging to a service is down or re-routed.

## 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 L3 VPN from the same node and VPN.

## Viewing the MPLS SNMP Traps

After NNMi discovered devices are configured, they generate SNMP traps that are received by NNMi. The NNM iSPI for MPLS supports the trap driven polling. When the traps are received, the State Poller starts polling the device, updates the status, and generates the incidents, if required. The SNMP traps are correlated under the MPLS incidents, if required. 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	MplsTETunnelDown	Generated when the status of the configured tunnel is

### SNMP Traps , continued

Name	Family	Correlation Type	Description
	Engineering		Down. This trap is generated by a Cisco node.
CiscoMplsTETunnelRerouted	MPLS Traffic Engineering	-	Generated when a tunnel originating from the router/device is rerouted because of some change in network or policy. 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	MplsVRFDnwn	Generated when the status of the VRF interface is Down. This trap is generated by a Cisco node.
CiscoMplsL3VPNvrfUp	MPLS L3 VPN	-	Generated when the status of the VRF associated with an L3 VPN returns from Down to Up. This trap is generated by a Cisco node.
CiscoMplsL3VPNvrfDown	MPLS L3 VPN	-	Generated when the status of the VRF associated with an L3 VPN goes Down. 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	-	Generated when the status of the configured tunnel is

### SNMP Traps , continued

Name	Family	Correlation Type	Description
	Engineering		Up. This trap is generated by a Juniper node.
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.
JnxMplsVrflfDown	MPLS Interface	MplsVRFDwn	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 down. This trap is generated by a Juniper node.
JnxMplsPseudoWireVCUp	MPLS PseudoWire VC	-	Generated when the status of the configured PseudoWire VC is up. This trap is generated by a Juniper node.
AlcatelMplsLspDown	MPLS Traffic Engineering	MplsTETunnelDown	Generated when the status of the configured TE Tunnel is down. This trap is generated by an Alcatel node.
AlcatelMplsLspUp	MPLS Traffic Engineering	-	Generated when the status of the configured TE Tunnel returns from Down to Up. This trap is generated by an Alcatel node.
AlcatelMplsStateChange	MPLS Interface	-	Generated when the MPLS module state is changed. This trap is generated by an Alcatel node.
AlcatelMplsIfStateChange	MPLS Interface	-	Generated when the MPLS interface State is changed.

### SNMP Traps , continued

Name	Family	Correlation Type	Description
			This trap is generated by an Alcatel 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.

## Viewing the MPLS Topology Maps

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

The NNM iSPI for MPLS presents map views that help you visualize your topology to view the network connectivity.

The NNM iSPI for MPLS presents map views—**MPLS Path view**, **MPLS is VPN Topology view**, **L3 VPN Topology View**, **L2 VPN Topology View**, **LSP Path View** and **MPLS TE Tunnel Path view**. With the NNM iSPI for MPLS, you can view the graphical representation of your network connectivity by using the following actions:

The NNM iSPI for MPLS presents map views—**MPLS Path view**, **MPLS is VPN Topology view**, **L3 VPN Topology View**, **L2 VPN Topology View**, **LSP Path View**, **MPLS TE Tunnel Path view** and **MPLS LDP Neighbors View**—that help you construct, visualize, and troubleshoot the network. With the NNM iSPI for MPLS, you can view the graphical representation of your network connectivity by using the following actions:

- [MPLS Path View](#)
- [MPLS L3 VPN Topology View](#)
- [MPLS LSP View](#)
- [MPLS TE Tunnel Path View](#)
- [MPLS LDP Neighbors](#)
- [MPLS L2 VPN Topology View](#)

#### Use the map views for the following:

- **MPLS Path view** to monitor the MPLS-enabled nodes and MPLS objects . MPLS Path view shows an MPLS path map view from source to destination on the network. This action is available from the MPLS LSR view.
- **MPLS L3 VPN Topology** to monitor the PE-CE nodes and interfaces participating to form an L3 VPN. MPLS L3 VPN Topology 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 L2 VPN Topology to monitor PseudoWires or VFI's participating to form an L2 VPN. The MPLS L2 VPN Topology View shows an MPLS L2 VPN map. The MPLS L2 VPN Topology Map view shows the PseudoWires or VFI's participating to form an L2 VPN. This action is available from the VPLS/VPWS VPN view
- MPLS LSP View to monitor the Label Switched Path (LSP) path between the two VRFs or PseudoWire VC. MPLS LSP view shows one endpoint connected to another endpoint through an LSP. In this case, an endpoint can be an MPLS object like a VRF or a service like an Attachment Circuit (AC). This action is available from L3 VPN inventory, VPLS inventory, VPWS inventory, and PseudoWire VC inventory.
- MPLS TE Tunnel Path View to monitor the path of TE tunnels. 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.
- MPLS LDP Neighbors map helps you to view the LDP neighbors for the selected source node. The Label Distribution Protocol (LDP) also enables the MPLS nodes to exchange label information. The MPLS LDP neighbor map displays the immediate LDP neighbors of a selected node.

**In addition, you can perform the following tasks:**

- Troubleshoot and investigate the status change and loss of connectivity of the MPLS nodes or interfaces.
- Navigate to the node and interface inventory from the map views
- Show Multicast Data Flow. This action displays a Multicast forwarding tree for the selected MDT. This action is available from the MDT form.
- Show Multicast Reverse Path. This action displays the path that a packet takes from a receiver or the selected router to reach the source. The action is available from the MDT form.
- Maintain QA probes for VRFs and displays QA probes graphs. This action is available from QA Probes tab and Analysis Pane of VRF Form.

You can access the map views from the **Actions** menu. Also, see [MPLS Map Symbols](#) to understand the topology views better.

## TE Tunnel Path View

The MPLS TE Tunnel Path View shows a 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 all the Cisco, Juniper, and Alcatel routers configured with TE Tunnel. The TE Tunnel path is the dynamic traffic flow path where the hops are updated periodically.


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 TE Tunnel path view to perform the following tasks:


- Find and view the nodes and interfaces participating to form a TE tunnel path.
- Determine the head, tail and intermediate routers of the TE Tunnel.

**To launch a TE Tunnel Path view:**

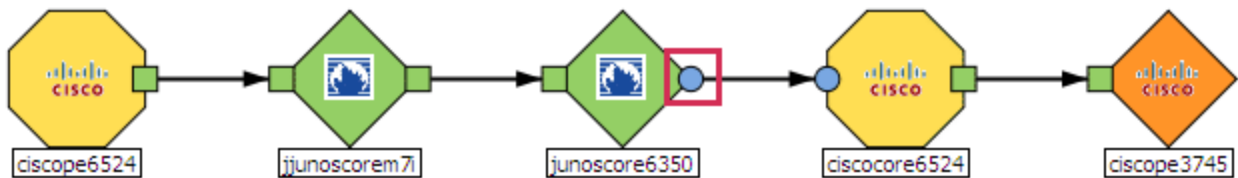
1. From the **Workspaces** navigation pane, click **MPLS-> TE Tunnel Inventory**. The MPLS TE Tunnel view opens in the right pane.
2. In the **TE Tunnel Inventory**, select a TE Tunnel.

3. From the menu bar, select **Actions-> MPLS TE Tunnel Path view**. The TE Tunnel path 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 path opens in a new window.

**Example of the TE Tunnel Path View:**




In this example, the TE Tunnel starts from the head node *cisco6524* to the tail node *cisco3745*. The intermediate routers are Juniper and Cisco routers. Double-click the node to open the node form. Double-click the square boxes attached to the node to open the interface form. The marked outgoing interface of the *junoscore6350* is Unknown. For more information about the node symbols, icons, and status color, see [MPLS Map Symbols](#).

The path between the selected source and destination node may go down or reroute. If you want to view the earlier path between the selected node, the map provides a **Show previous path** option. To view the previous path, follow these steps:

1. Launch the [TE Tunnel path view](#).
2. Select 'Yes' from the **Show previous path** drop-down in the upper right corner of the window.

**Note:** The NNM iSPI for MPLS only maintains the current and its previous path between the selected node.

**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.
  - Select the node, click  (the **Open** icon).
3. From the TE Tunnel form, click the **Incidents** tab to view the incident.

**Related Topic:**

[MPLS Map Symbols](#).

## MPLS L3 VPN Topology View




You can troubleshoot the faults associated in your L3 VPN 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.
- View Inter-Provider VPNs with AS#s of other ISPs .

### To launch an MPLS L3 VPN view:

1. From the **Workspaces** navigation pane, click **MPLS-> L3 VPN Inventory**. The MPLS L3 VPN view opens in the right pane.
2. In the **MPLS L3 VPN** view, select a row representing the required L3 VPN.
3. Click **Actions-> MPLS L3 VPN Topology View** The L3 VPN graph opens in a new window.
4. Click  (the **Compute Map** icon) to display the updated map, Click  (the **Refresh Status** 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 VRF icon to open the 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 L3 VPN.
- 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 on the network.


**Examples of the MPLS L3 VPN map view**

	<p>This is an example of a Full Mesh L3 VPN.</p> <p>Double-click the VRF icon to open the VRF form.</p>
	<p>This is an example of a Hub and Spoke L3 VPN. All the VRFs are communicating with the Hub VRF.</p> <p>Double-click the Hub VRF icon to open the Hub VRF form.</p>

This is an example of a Full Mesh L3 VPN.



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

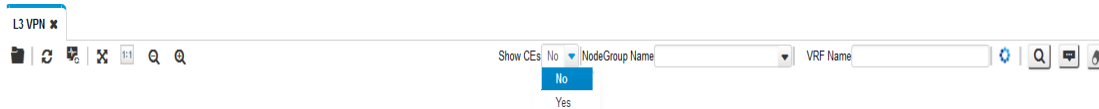
1. Navigate to the **MPLS L3 VPN view**.
2. To open the node or interface, use any *one* of the following:
  - Double-click the VRF or CE node.
  - Select the VRF and click  (the **Open** icon).
3. From the VRF or L3 VPN form, click the **Incidents** tab to view the incident.

**Related Topics:**

- [MPLS Map Symbols](#)
- [MPLS L3 VPN toolbar](#)

## Using the L3 VPN Map View Toolbar

The NNM 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 and VRF Lites participating in the L3 VPN. The map view toolbar contains the NNMi icons such as Open, Refresh, Refresh, and Status. The following table lists the MPLS icons.

### MPLS L3 VPN Map Toolbar Icons

Icon	Description
Show CEs	Select the option <b>Yes</b> or <b>No</b> 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 NNM 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. This field is applicable only if you have selected 'Yes' for show CEs.
VRF Name	Type the <b>VRF Name</b> . The CE nodes associated with the selected VRF name appears in the map view. This field is applicable only if you have selected 'Yes' for show CEs.

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

1. Select the option **Yes** from the Show CEs list. This will display all the CEs participating to form the selected L3 VPN. You can filter these CEs based the host node.
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 Node Group or VRF or both. If the conditions such as VRF Name and Node Name do not match the requirement, the map view shows the appropriate messages.

**Note:** Type a VRF Name in the filter as following: *VRFName@nodename*. For example, if you are searching for a VRF named test on a Cisco device, then you will search it as '**test@cisco**'.

## MPLS Inter-Provider VPN Topology Map View

Inter-Provider VPN is an extended feature for L3 VPN. You can view and troubleshoot the faults associated to your MPLS Inter-Provider VPN 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, PE nodes, PE-CE connectivity, and AS names or numbers of the third-party carrier service provider network participating to form an Inter-Provider VPN.

Use the Inter-Provider VPN Topology Map view to perform the following tasks:

- Find the VRFs participating to form an Inter-Provider VPN.
- Find the CE nodes and interfaces participating in the Inter-Provider VPN. For more information, see [L3 VPN Map Toolbar](#).
- Discover the CE nodes residing in the remote client site.
- The third-party VPN clouds participating in the Inter-Provider VPN.
- As path followed by the PE-CE connectivity.

You can perform tasks such as launching and troubleshooting for MPLS objects participating in an Inter-Provider VPN. For more details, see *To launch an MPLS L3 VPN view* and *Troubleshooting the network connectivity from the MPLS L3 VPN View* in the [MPLS L3 VPN Topology Map View](#).

**Note:** PE-CE connectivity may show incorrect information if the CE is not configured properly. For example, a CE may be shown connected to a Cisco router instead of a Juniper router. In such cases, reconfiguring the CE will solve the problem.

## MPLS L2 VPN Topology View

You can troubleshoot the faults associated in L2 VPN topology by using the MPLS L2 VPN map view. This map view is a service-centric map view. You can monitor the Attachment Circuits (ACs), status of service-centric objects associated with a VPLS or a VPWS, and status of Pseudo Wires participating to form an L2 VPN.

In an MPLS L2 VPN topology map view, ACs, service-centric objects, and Pseudo Wires are represented as symbols on the map. Status of each service-centric object is represented by a color, for more information on each status color, see [MPLS Map Symbols](#) and NNMi Help, *Maps Symbols*.

Use this view to perform the following tasks:




- Monitor status of service-centric objects associated with a VPLS/ VPWS. Status of service-centric objects is calculated based on most critical status of the ACs
- Monitor status of PseudoWires associated with a VPLS/ VPWS
- Launch LSP path view by selecting service centric object or PseudoWire in VPLS/VPWS map
- Monitor group of PseudoWires. This group is represented by a thick line. This group of PseudoWires is formed in the following two scenarios:

- Full-mesh VPLS topology, where all participant service centric objects are connected with each other.
- For a VPWS, where there are multiple PseudoWire connections between two service centric objects

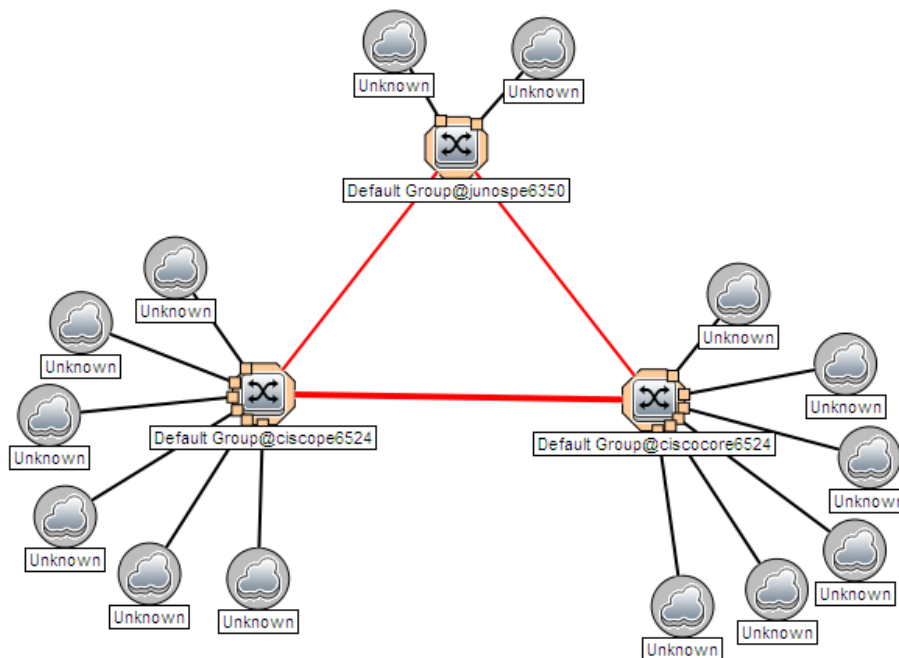
Status of this thick line is calculated based on most critical status of PseudoWires<sup>1</sup> participating to form the group. In addition, you can click the group of PseudoWires to get detailed information about each PseudoWire. This information is shown in the [Analysis Pane](#)

#### To launch an MPLS L2 VPN view:

These are steps to launch VPLS VPN topology view. You can follow the same steps to launch VPWS VPN topology view.

1. From the **Workspaces** navigation pane, click **MPLS-> VPLS VPN Inventory**.
2. Click and select a row representing the required L2 VPN.
3. Click **Actions-> MPLS L2 VPN Topology View** The L2 VPN topology view opens in a new window.
4. Click  (the **Compute Map** icon) to display the updated map, Click  (the **Refresh Status** icon) to update the status of MPLS objects. Click  (the **Refresh** icon) to update the map topology and status.

#### Example of an L2 VPN Map



This is an example of VPWS topology.

#### Analysis Pane

Analysis Pane for L2 VPN topology view shows details about the objects participating in a VPLS or VPWS topology respectively.

#### For service-centric object:

<sup>1</sup>For example, in a group of five pseudowires, even if one is critical, the entire group will have status as critical.

When you click on a service centric object in a VPLS or VPWS map, you will see the name of the object and of the node it is hosted to the left, under *Summary*.

To the right the following information is shown:

- **PseudowireVCStatusPie chart** - Shows Pie Chart that represents the status of all thePseudoWires
- **SDPBindsStatusPie Chart** - Shows Pie Chart that represents the status of all the SDPBinds.
- **VFI Neighbours** - Shows the status of all the VFI Neighbors participating to form the selected VPLS VPN

Under **PseudoWires**, following information is shown:

- **PseudoWire Id** : This is the ID of the corresponding PseudoWire. Click on this ID to open the PseudoWire VC form. In case of group of PseudoWires, a list of all the PseudoWires that are a part of the group is shown.
- **Status**: Status of the selected PseudoWire. In case of a group of PseudoWires, this status will correspond to the most critical status of PseudoWires.
- **AC1**: Attachment Circuit corresponding to PE1
- **PE1**: Source Provider Edge corresponding to the selected PseudoWire
- **AC2**: Attachment Circuit corresponding to PE2
- **PE2**: Destination Provider Edge corresponding to the selected PseudoWire
- **LSP Path View** - Shows a link to **Launch** LSP Path View. Click the link to launch a LSP path.

#### **For PseudoWire:**

When you click on a single PseudoWire corresponding to a VPLS or VPWS, you will see the following information:

- **PseudoWire VC Summary**. Shows the following details:
  - Create Time
  - Status
  - Custom Attributes
  - Management Type
  - Management Mode
  - PE1 - Source provider edge.
  - PE2 - Destination provider edge devices
- **VCLspStatusPieChart** Tab- Shows Pie Chart that represents the status of all the VC LSPs participating to form the PsuedoWire
- **LSP Path View** Tab - Shows a link to **Launch LSP Path View**. You can click on this link to launch an LSP path.

In addition, if you click on a group of PseudoWires, you will see the following information:

- **PseudoWires Summary** : Name of the Source and destination sites corresponding the selected PseudoWire.
- **Grouped PseudoWire details**: Shows a table that lists all the individual PseudoWires that form the selected group. You can see the following information in the table:

- **PseudoWire Id** - This is the Id number of the selected PseudoWire. Click on it to open the PseudoWire VC form.
- **Status** - Status of the selected individual PseudoWire status.
- **PE1** - Source Provider Edge corresponding to the selected PseudoWire
- **AC1** - Attachment Circuit associated with PE1.
- **PE2** - Destination Provider Edge corresponding to the selected PseudoWire.
- **AC2** - Attachment Circuit associated with PE2.
- **URL for LSP Path View** - Shows a link to **Launch LSP Path View**. You can click on this link to launch an LSP path

To the right, for *PseudoWire to AC Mapping* the following information is shown:

- **PseudoWire Id** : This is the ID of the corresponding PseudoWire. Click on this ID to open the PseudoWire VC form. In case of group of PseudoWires, a list of all the PseudoWires that are a part of the group is shown.
- **Status**: Status of the selected PseudoWire. In case of a group of PseudoWires, this status will correspond to the most critical status of PseudoWires.
- **AC1**: Attachment Circuit corresponding to PE1
- **AC2**: Attachment Circuit corresponding to PE2

## MPLS Path View

The MPLS Path view shows the Label Switched Path (LSP) between two 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 NNM iSPI for MPLS supports only OSPF<sup>1</sup> protocols for the path calculation. When the NNM 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:

1. From the **Workspaces** navigation pane, click **MPLS-> LSR Inventory**. The **MPLS LSR View** opens in the right pane.
2. In the **MPLS LSR** view, select a LSR node
3. From the menu bar, select **Actions-> MPLS Path View**. The **MPLS Path View** opens.

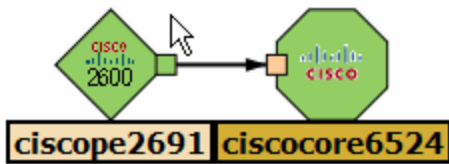
<sup>1</sup>Open Shortest Path First

4. Click  (the **Refresh Status** icon) to update the status of the MPLS objects. Click  (the **Refresh** icon) to update the map view.

The MPLS path view contains the following information:

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


#### Example of the MPLS Path View:




The MPLS Path view shows the path from the node *cisco2691* to the node *ciscocore6524*. Double-click the square boxes attached to the MPLS node or switch to open the interface form. Alternatively, you can view the details from the Quick View window.

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

#### Troubleshoot the network connectivity from the MPLS Path View, follow the 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 displayed in the Inventory view on the right panel.
  - Select the node, click  (the **Open** icon).
3. Navigate to the **Incidents** tab to view the incident and troubleshoot the cause of loss of network connectivity.

#### To find details of the TE tunnels, VRFs or PseudoWires VCs configured on the selected node from the MPLS Path view, follow these steps:

1. Navigate to the **MPLS Path view**.
2. To open the node form, use any *one* of the following:
  - Double-click the node to view the node details such as VRF Tab, TE Tunnel Tab, and so on.
  - Select the node, click  (the **Open** icon).
3. Click the *<MPLS object>* Tab from the selected Node form to view details of the MPLS objects such as TE Tunnel or VRF.

#### Related Topic:

[MPLS Map Symbols](#)


# LSP Path View

LSP Path View shows the Label Switched Path (LSP) between two service centric objects.

## To Launch LSP Path View:

- [From L3 VPN Inventory](#)

You can launch an LSP path view between any two devices from the LSR inventory. To launch an LSP path view:

- a. Click **L3 VPN Inventory** from the **MPLS** workspace .
- b. Select an L3 VPN and open the **L3 VPN** form
- c. Click , available under the **VRF** tab, to open all the VRFs of the L3 VPN in a new window.
- d. Select two VRFs to determine which LSP you want to monitor
- e. Click **Actions**
- f. Click **Monitor LSP**

Similarly, from the L3 VPN topology view you can monitor LSP:

- a. Launch L3 VPN topology view
- b. Select two VRFs to determine which LSP you want to monitor
- c. Click **Actions**
- d. Click **Monitor LSP**

- [From VPLS Inventory](#)

- a. [Launch VPLS map](#)
- b. Select a PseudoWire
- c. Select **LSP Path View** tab from the Analysis Pane
- d. Click **Launch LSP Path View**. The LSP Path View shows a one-way path between the source and the destination.  
**Note:** For a full-mesh VPLS, you have to select a PseudoWire from the Analysis Pane and then launch LSP Path View from the same table.

- [From VPWS Inventory](#)

- a. [Launch VPWS map](#)
- b. Select a PseudoWire

For a group of PseudoWires,select a PseudoWire from the Analysis Pane by clicking the PseudoWire Id. This action opens the [PseudoWire VC form](#) for the selected PseudoWire



- c. Select **LSP Path View** tab from the Analysis Pane
- d. Click **Launch LSP Path View**. The LSP Path View shows a one-way path between the source and the destination.

- [From PseudoWire VC Inventory](#)

- a. From the **Workspaces** navigation pane, click **MPLS->PseudoWire VC Inventory**.

- b. Select a PseudoWire from the PseudoWire VC Inventory view for which you want to launch a path view.
- c. Select **LSP Path View** tab from the Analysis Pane.

In addition, from the MPLS LSP Path View window, you can reverse the direction of the LSP path. Follow these steps to reverse the LSP path:

1. [Launch LSP path view](#)
2. To reverse the path select any service centric object or PseudoWire.
3. Select 'Yes' from the **Show Reverse LSP** drop-down in the upper right corner of the window.
4. Click  (the **Compute Path** icon) to get the reversed path.
5. To see the original direction of the path, click  (the **Compute Path** icon) again.

LSPs are unidirectional, hence you must reverse path to see bi-directional LSP. Reversing LSP path is mandatory for PseudoWire VCs.


## VRF-LSP Service Mapping


You can launch MPLS LSP path view by selecting two neighboring VRFs participating to form the selected L3 VPN. Follow these steps to launch an MPLS LSP path view:

1. Launch an L3 VPN map view from the L3 VPN Inventory.
2. Select two neighboring VRFs participating in that L3 VPN by clicking on the VRF icons  
**Note:** The first VRF selected represents the source LSR and the second VRF represents the destination LSR. You can reverse source and destination by reversing the order of selection
3. Click **Actions** and select **MPLS Lsp Path View**. This will launch the LSP path view between these VRFs in a different browser window.

MPLS LSP Path View shows the source LSR and destination LSR connected by a cloud when:

- Source and destination LSRs are not mapped to the services
- No Path exists between the source and destination

A path between two selected VRFs can pass through an LSP or a TE tunnel. TE tunnels are represented by the TE Tunnel icon. In addition, the map provides a **Show Nodes for Tunnel** option that expands the tunnel icon to display the Tunnel path. To expand, select 'Yes' from the **Show Nodes for Tunnel** list. Click  (the **Compute Path** icon) to get the Tunnel path. For more information, see [Map Symbols](#).

Also, the map provides a **Show previous path** option that displays the previous path between the selected source and destination node. To view the previous path, select **Yes** from the **Show previous path** list. Click  (the **Compute Path** icon) and then, you can view the previous LSP between the selected source and destination node for the VRF service.

## MPLS LDP Neighbors

With the MPLS LDP Neighbors map, you can view the LDP Neighbors within an MPLS network. Label Distribution Protocol (LDP) enables MPLS nodes to exchange label information. Any two routers that have an active LDP session between them are called peers or neighbors.

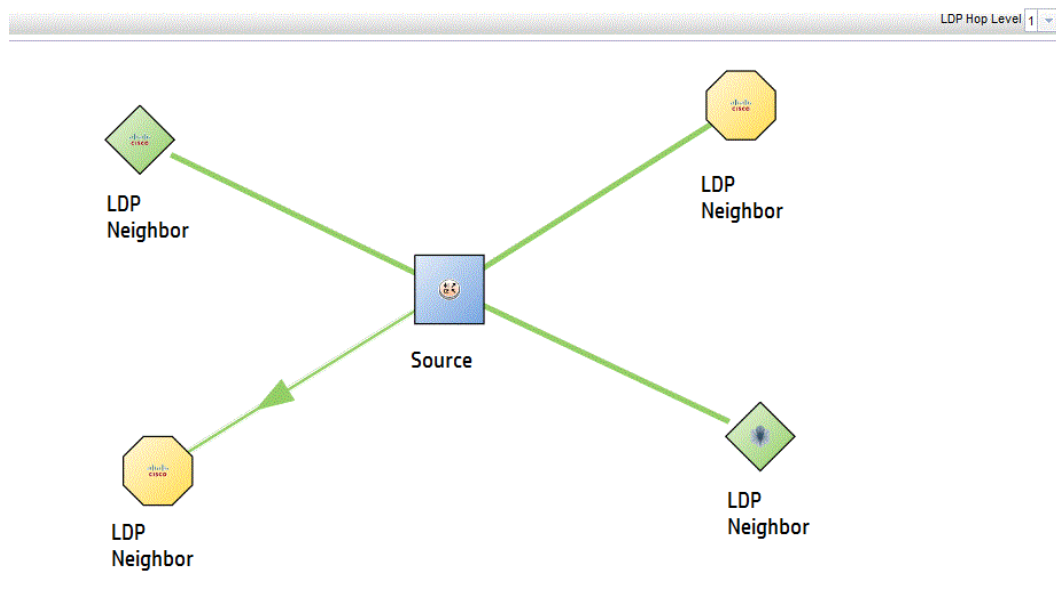
**To Launch MPLS LDP Neighbors:**



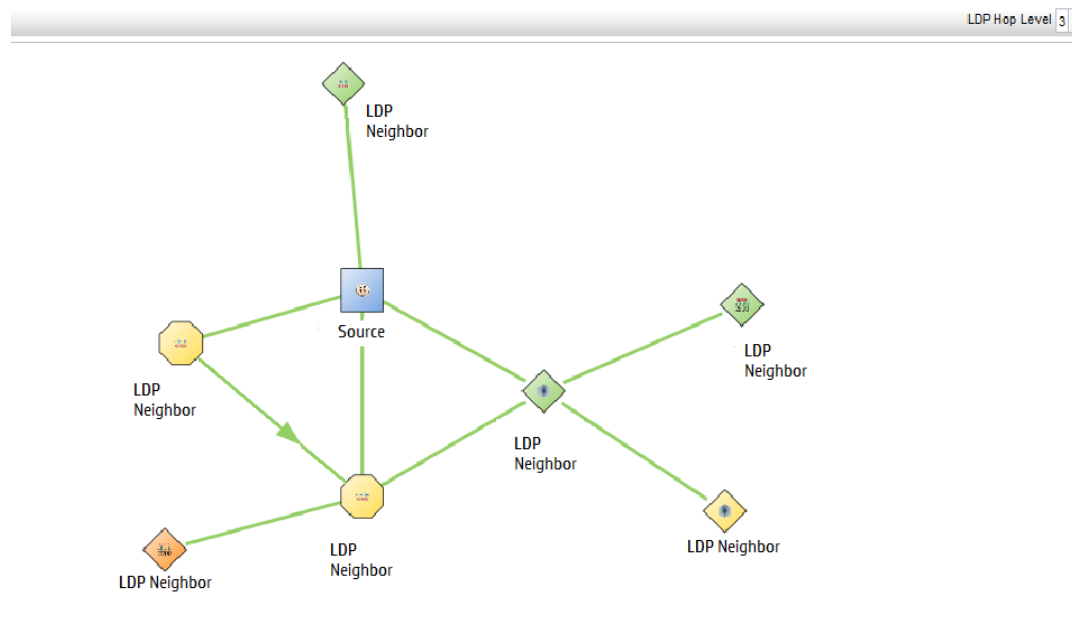
1. Open LSR Inventory
  - a. Click the **MPLS** workspace
  - b. Click **LSR Inventory**
2. Select the LSR for which you want to launch the map.
3. Click **Actions**
4. Click **MPLS LDP Neighbors**.

The MPLS LDP Neighbors map shows the LDP neighbors of a selected source node. Proximity of an LDP neighbor is based on the number of hops between the LDP neighbor and the source node and is indicated by the **Hop Level**. By default, the map displays the immediate LDP neighbors of a selected node that is **Hop Level 1**. You can change the hop level by using the **LDP Hop Level** list on the top right of the screen.

### Example of MPLS LDP Neighbors map with LDP Hop Level 1



### Example of MPLS LDP Neighbors map with LDP Hop Level 3



## 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:

1. Navigate to the MVPN form
  - a. From the **Workspaces** navigation pane, click **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 **Refresh Status** 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
  - a. From the **Workspaces** navigation pane, click **MPLS-> MPLS L3 VPN Inventory**. The L3 VPN 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. *Do not 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.

## IP Multicast Reverse Path View

The reverse path view shows the multicast routing path from a receiver router to the source router.

The URL action to launch the IP Multicast Reverse Path 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 reverse path view:

1. Navigate to the MVRF Form
  - a. From the **Workspaces** navigation pane, click **MPLS-> MPLS L3 VPN Inventory**. Alternatively, from the **Workspaces** navigation pane, click **MPLS-> MVPN Inventory**. The L3 VPN 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. *Do not select the Default MDT.*
3. Click the URL for **Multicast Reverse Path View** from the Analysis Pane
4. Click  (the **Refresh** icon) to update the reverse path view.

### Example of a IP Multicast Reverse Path View










## MPLS Map Symbols

**(See, *About Map Symbols* and *About Status Colors* in *NNM Online Help: Console Help* before you begin with this topic)**







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

The NNM iSPI for MPLS uses NNMi shapes for the nodes and interfaces. The NNM iSPI for MPLS uses the same symbols to represent both, a VRF or a VRF-Lite on the map. The NNM 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.
	Used in maps to represent a Hub VRF.
	Used in maps to represent a VRF-Lite.
	Used in maps to represent an MVRF.
	Used in maps to represent a Hub MVRF.
	Used in map view to represent a CE node.
	<p>Used in L3 VPN to show:</p> <ul style="list-style-type: none"> <li>• A full mesh L3 VPN topology on the network.</li> <li>• A PE interface connected to an unknown CE interface. The CE interface on the node is indicated on the map by a cloud symbol.</li> <li>• 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.</li> <li>• 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.</li> </ul> <p>Used in Inter-provider VPN to show:</p> <ul style="list-style-type: none"> <li>• Third-party VPN clouds participating in the Inter-Provider VPN</li> </ul> <p>Used in L2 VPN to show:</p> <ul style="list-style-type: none"> <li>• A full mesh L2 VPN on the network</li> <li>• A service object connected to an unknown CE interface. The CE interface on the node is indicated on the map by a cloud symbol.</li> </ul>

### Icons Used By MPLS, continued

Icons	Meaning
	Represents the service centric object associated with a VPLS. For example, VPLS_<vc id>@hostname
	Represents the service centric object associated with a VPWS. <vpws_groupname>@<hostname>
	Connector that represents a CE-VRF-Lite or PE-VRF-Lite connection.
	Represents a Pseudo Wire. The color of the selected Pseudo Wire is the status color.
	Represents collective Pseudo Wires grouped as one. You can click this symbol to view individual Pseudo Wires in the <a href="#">Analysis Pane</a> . The color of the selected Pseudo Wire is the status color.
	Represents TE Tunnel.

### 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 represents the following: <ul style="list-style-type: none"> <li>• A PE interface connected to an unknown CE interface. The CE interface on the node is indicated on the map by a cloud symbol.</li> <li>• 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.</li> <li>• 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.</li> </ul>
	Used to represent a VRF. In a map view, this symbol is superimposed with the 'VRF' or 'VRF Lite' symbol. The color of the selected VRF is the status color.
	Used to represent a switch. The color of the selected switch is the status color.
	Used to represent third-party VPN provider in an Inter-Provider VPN network. This shape is superimposed with the cloud icon.

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

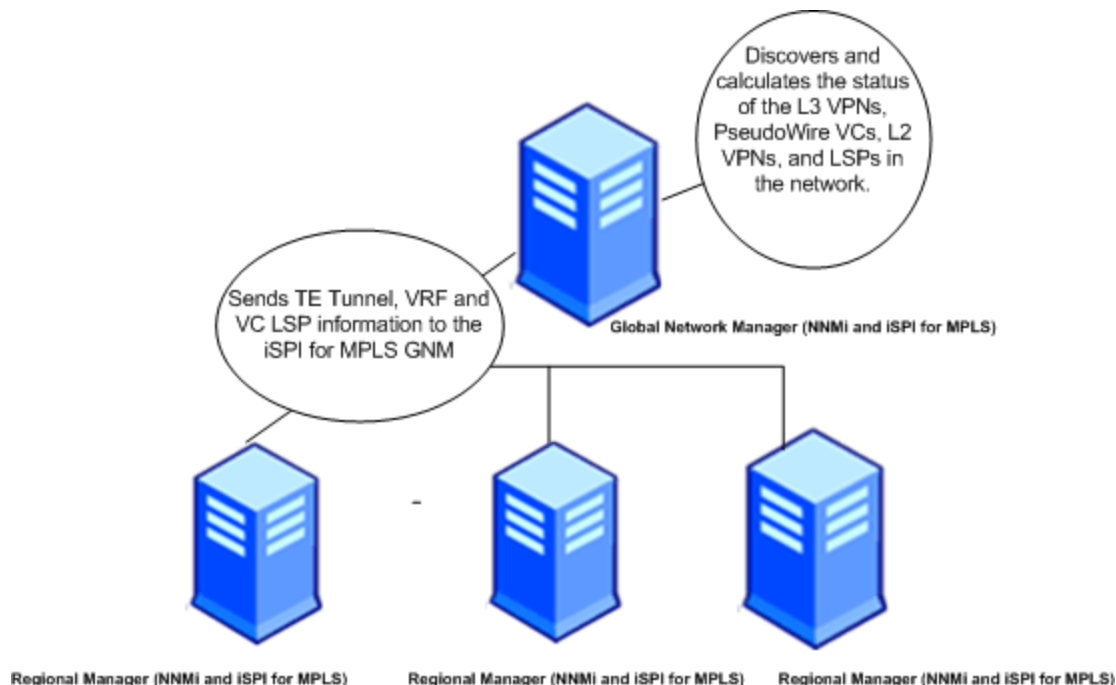
The NNM iSPI for MPLS uses the capabilities of NNMi Global Network Manager (GNM) and provides a centralized view to monitor multiple sites. You can configure the Regional Manager connections by using the **MPLS Configuration** workspace. After the connection is established, view and monitor the MPLS-enabled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

Use the NNM iSPI for MPLS view GNM for the following tasks:

- Monitor the MPLS-enabled routers on the network.
- View the MPLS objects such as VRFs, TE Tunnels, and VC LSP on the network and resolve problems, if any. 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 NNM 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 on the network to the NNM iSPI for MPLS GNM.

[About the NNM 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 NNM 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, L2 VPNs, and LSPs on the network.

Use the NNM 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 on 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 the same 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 on 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 on the network.
- Monitor the Pseudowire VCs on 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 on the network.
- Monitor LSPs on the network. LSP can be stitched at Global as it goes across more than one regional
- Monitor and generate the MPLS reports from the MPLS inventory (GNM). The MPLS LSR Node and Interface report is only available for the MPLS-enabled nodes that are seeded locally in the NNM iSPI for MPLS (GNM). The L3 VPN\_VRF report is available for the local nodes of the Regional Manager that appears in the NNM iSPI for MPLS inventory (GNM) and also for the nodes seeded locally in the NNM iSPI for MPLS (GNM).

The NNM 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 NNM 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 NNM iSPI for MPLS GNM. The configuration settings are limited to a local Regional Manager and do not get transferred to the NNM iSPI for MPLS GNM.

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

## Duplicate IP Address Support with the NNM iSPI for MPLS

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

The NNM 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 NNM 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 may 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 NNM iSPI for MPLS discovery process starts when ARP Cache is down, no information is found for the PE-CE communication. In this case, the NNM iSPI for MPLS does not resolve the duplicate IP address.



# Chapter 4: Help for NNM iSPI for MPLS Administrator

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

- You can modify the default polling intervals for all the MPLS objects. See, [Configure Polling Intervals](#)
- You can configure devices to support SSHv2 . See, [Non-SNMP Framework and Blacklisted Devices](#)
- You can configure device credentials and enable services such as LSP Service Mapping . See, [Configure Device Credentials](#)
- You can add or delete Route Targets (RTs) participating to form an L3 VPN. See, [Configure Exclude Route Targets](#)
- You can create VPWS VPNs with multiple encapsulations. See, [Configure VPWS VPN](#)
- You can configure Global Managers to communicate with Regional Managers. See, [Configure Regional Manager](#)
- [You can perform Backup and Restore Actions:](#)

You can perform the backup and restore actions for the NNM iSPI for MPLS by using NNMi Backup and Restore commands. 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`.

- [You can 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*

- [You can 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*.

- [You can log on to the MPLS Configuration Workspace:](#)

- a. Open the URL with Fully Qualified Name (FQDN), and log on as an admin user. You will be prompted to enter the login ID and password again.
- b. 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:
  - i. From the **User Configuration Interface**, click the **Enable URL Re-direct** checkbox and save the settings.
  - ii. 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.

In addition you can :

- [Manage and Unmanage Nodes](#)
- [Integrate the NNM iSPI for MPLS with Route Analytics Management Software \(RAMS\)](#)
- [Integrate the NNM iSPI for MPLS with NNM iSPI for IP Multicast](#)
- [Integrate the NNM iSPI for MPLS with NNM iSPI Performance for QA](#)

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

After you install NNMi and NNM iSPI for MPLS, seed the nodes from the NNMi console. The NNMi discovery process starts and discovers the nodes on the network. After every node is discovered, the NNM iSPI for MPLS discovery process starts automatically after the completion of NNMi discovery process .

When you add an MPLS node in the topology, NNMi discovery process detects the change in network and sends a notification to start the discovery process to the NNM iSPI for MPLS . 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 NNM iSPI for MPLS is set to 24 hours.

After installing the NNM 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.

To start the complete discovery for the NNM iSPI for MPLS, use `nmsmplsdisco.ovpl -a11`. For more information, see MPLS reference pages (*Help -> NNMi iSPI Documentation Library -> NNM iSPI for MPLS Reference Pages*).

In addition, you can also choose to not discover certain MPLS nodes. By doing so, you can handle the load of your MPLS network and also exclude the nodes that may cause issues during network discovery. To exclude:

1. Create a node group for MPLS-enabled devices with the name **MPLSNoDiscover**
2. Add the devices that you do not want to be discovered to this group.

If you have a node in the MPLSNoDiscover group for regional then that node from the NNM iSPI for MPLS GNM will be removed automatically .

Also, to exclude nodes from the NNM iSPI for MPLS GNM, you must create a **MPLSNoDiscover** node group on the NNM iSPI for MPLS GNM for regional nodes.

For more information, see *Create Node Groups* in *HPE NNMi Online Help for Administrators*.

## Configuring the NNM iSPI for MPLS

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

- Configure Polling Intervals
- Configure Device Authentication
- Configure Route Targets
- Configure VPWS VPN
- Configure Regional Manager

The MPLS Configuration workspace consists of the following tabs:

Configuration Tab	Description
Polling Frequencies	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.
Device Authentication	Used to add device credentials for non-SNMP framework
Exclude Route Targets	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.
MPLS 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 Device Credentials](#)
- [Configure Exclude Route Targets](#)
- [Configure VPWS VPN Configurations](#)
- [Configure MPLS Regional Manager Connections](#)

## Configure the Polling Frequency

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

The MPLS State Poller gathers information about nodes, interfaces, and MPLS objects from the discovered devices 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 State Poller identifies the topology changes and polls newly discovered devices and MPLS objects such as SDPs, VFIs, LDP peers, TE tunnels, VRFs, and VC LSPs. 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
- VPLS VPN status
- Monitored LSP status
- VFI Status
- SDP Status

After the NNM iSPI for MPLS discovers the available MPLS nodes and interfaces on 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:

1. Navigate to the MPLS Configuration form.
  - a. From the workspace navigation panel, select the **iSPI for MPLS Configuration** workspace.
  - b. Select the **Poller Frequencies** tab.
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 Polling Frequency:** Sets the interval (in minutes) between the two consecutive polls for PseudoWire VC. The default value is 5 minutes.
  - **LSP Polling Frequency:** Sets the interval (in minutes) between the two consecutive polls for LSPs. The default value is 5 minutes.
  - **VFI Polling Frequency:** Sets the time in minutes, seconds between the two consecutive polls for VFI. By default, the State Poller polls periodically every 5 minutes for the status of VFIs.
  - **SDP Polling Frequency:** The SDP polling frequency sets the time in minutes, seconds between the two consecutive polls for SDP. By default, the State Poller polls periodically every 5 minutes for the status of SDPs.
  - **VRF Performance Polling:** Sets the interval (in minutes) between the two consecutive polls for the selected VRF. The default value is 15 minutes. To enable Performance polling, check **Enable Polling**
  - **LSR Performance Polling:** Sets the interval (in minutes) between the two consecutive polls for the selected LSR node. The default value is 15 minutes. To enable Performance polling, check **Enable Polling**
  - **TE Tunnel Performance Polling:** Sets the interval (in minutes) between the two consecutive polls for the selected TE Tunnel. The default value is 15 minutes. To enable Performance polling, check **Enable Polling**
  - **VFI Performance Polling:** Sets the interval (in minutes) between the two consecutive polls for the selected VFI. The default value is 15 minutes. To enable Performance polling, check **Enable Polling**

- **PseudoWire Performance Polling:** Sets the interval (in minutes) between the two consecutive polls for the selected PseudoWire. The default value is 15 minutes. To enable Performance polling, check **Enable Polling**
- **LSP Performance Polling:** Sets the interval (in minutes) between the two consecutive polls for the selected LSP. The default value is 15 minutes. To enable Performance polling, check **Enable Polling**

3. Click  (the **Save** icon).

The default value of the State Poller is five minutes.

### 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 NNM 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 NNM iSPI for MPLS information explicitly but 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*.

## Configure the Exclude Route Targets

The Route Targets (RTs) that are responsible for the communication between two different VPNs are then identified and configured to exclude from the discovery of VPN. You can exclude RTs to terminate the communication between two or more VPNs. Whenever you update the list of RTs, the NNM 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.
  - a. From the workspace navigation panel, select the **MPLS Configuration** workspace.
  - b. Select the **Exclude Route Targets** tab.
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 save action starts the L3 VPN topology recalculation.
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).

You can use wildcard characters in the NNM iSPI for MPLS. A wildcard character such as an asterisk (\*) is used to exclude all the RTs.

For example, if you want to use a wildcard to exclude all the RTs from the RT list, you can specify an asterisk (\*) in the **Exclude Route Targets** tab. Moreover, if you want to include few RTs from the RT list, you can use the include RT feature. The include RT feature can be helpful if you want to exclude all RTs except few.

Choose \* Exclude to exclude all the RTs and then include the RTs you want to discover.

For example:

You have an RT list ranging from 100:1 - 100:98000. If you only want to include the following RTs:

- 100:2
- 100:49000
- 100:88000
- 100:90000
- 100:98000

First perform a \* Exclude that will exclude all the RTs and then, you can include the above RTs as:

- 100:2INCLUDE
- 100:49000INCLUDE
- 100:88000INCLUDE
- 100:90000INCLUDE
- 100:98000INCLUDE

**Note:** The NNM iSPI for MPLS does not support wildcards for the RT INCLUDE filter.

The NNM iSPI for MPLS then discovers and re-computes the L3 VPN. It will exclude the following list of RTs:

- 100:1
- 100:3, 100:4, 100:5, ....., 100:48998, 100:48999
- 100:49001, 100:49002, ....., 100:87998, 100:87999
- 100:88001, 100:88002, ....., 100:89998, 100:89999
- 100:90001, 100:90002, ....., 100:97998, 100:97999


## 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\_VCIId. 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, it appears as **Default Group**.

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

1. Navigate to the MPLS Configuration form.
  - a. From the workspace navigation panel, select the **MPLS Configuration** workspace.
  - b. Select the **VPWS VPN Configuration** tab.
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. *Do not* use special characters in the name. This field 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 list box. You can select multiple encapsulation types.
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.
  - a. From the workspace navigation panel, select the **MPLS Configuration** workspace.
  - b. Select the **VPWS VPN Configuration** tab.
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**.

## Non-SNMP Framework and Blacklisted Devices

The NNM iSPI for MPLS uses Simple Network Management Protocol (SNMP) for discovering and monitoring the health of MPLS-enabled nodes. However, for some of the MPLS features, management information is not available through SNMP interface. In such scenarios, the NNM iSPI for MPLS connects to Command Line Interface (CLI) of the supported devices participating in an MPLS network. Using the SSHv2<sup>1</sup> or Telnet, the NNM iSPI for MPLS gets information required to manage specific MPLS objects or services.

In order to use SSHv2 or Telnet, you have to get vendor specific installation support. For more information, see the vendor specific websites. The following is the list of conditions that should be met for non-SNMP framework support:

- The device should support SSHv2 or Telnet, and have appropriate credentials in MPLS iSPI configuration to connect to the device. For more information see, [Configure Device Credentials](#)
- Non-SNMP state should NOT be SESSION\_FAULT. For more information see, *Actions Available* below.
- You can connect through SSHv2 or Telnet only through standard ports. Make sure these ports are not blocked

**Note:** Though the NNM iSPI for MPLS supports both, SSHv2 and Telnet, it uses SSHv2 protocol as the first preference. NNM iSPI for MPLS uses Telnet if SSHv2 fails.

When SSHv2 is enabled on a device, the vendor specific commands clear the SSHv2 session after it ends. However, on some devices, these sessions may not get cleared due to vendor or operating system specific issues. Number of these sessions, if not cleared, would continue to increase. To avoid accumulation of the SSHv2 sessions the NNM iSPI for MPLS blacklists (SESSION\_FAULT) devices that have more than 4 such sessions accumulated for the same server. These devices are excluded from SSHv2 access in subsequent discoveries. Moreover, a device may get blacklisted if no session related data is available

The CLI commands for Cisco device are as follows:

<sup>1</sup>Secure Shell protocol version 2

- `show ip cef vrf <vrf_name> detail`
- `show mpls l2transport vc detail`
- `show mpls l2transport vc`
- `show vfi <VFI_NAME>`
- `show mpls forwarding-table <Destination prefix>`
- `show configuration`

For more information on these commands, see vendor specific guides.

The CLI commands for Juniper device are as follows:

- `show route table <route_table_name> detail`
- `show bgp neighbor`
- `route table bgp.l3vpn.0 next-hop <next_hop_ip_address> detail`
- `show route table l2circuit.0 protocol l2circuit active-path detail`
- `show route table <VRF_NAME> detail`
- `show route table l2circuit.0 protocol l2circuit active-path detail`
- `show route <destination> detail active-path`
- `show route <destination> detail table inet.3 active-path`

For more information on these commands, see vendor specific guides.

### Actions Available

- To get a list of blacklisted or SESSION\_FAULT devices, use the command script:  
`/opt/OV/support/nmsmplsDiagnostics.ovpl -printBlacklistedDevices`

In case of session faults, you can set time for automatic clearance of the SSHv2 sessions and reset the marking.

- To reset the blacklisted devices to normal, use:

```
/opt/OV/support/nmsmplsDiagnostics.ovpl -resetNonSnmpState <Device host name>
```

You can disable the session checks if you are sure that the SSHv2 session clearing is not required for the devices.

- To disable session checking, use:

```
/opt/OV/support/nmsmplsDiagnostics.ovpl -setNonSnmpStateOK <Device host name>
```

It is recommended that you keep maximum sessions open for SHH2 with minimum 8 sessions at all times to avoid blacklisting of the devices. Maximum sessions open ensure that even after a device is blacklisted, there is session available for an administrator to debug the machine remotely and terminate the sessions.

**Note:** The above rule is not applicable for Telnet.

## Configure Device Credentials



The NNM iSPI for MPLS can connect to Command Line Interface (CLI) the supported devices (for more information on supported devices, see *Non-SNMP Framework*) participating in an MPLS network, using the



or Telnet protocol to get information required to manage specific MPLS elements or services. This is required for some features such as LSP Service mapping, when information is not available through SNMP interface.

To use this function, users have to enter authentication information for these devices (device credentials). These credentials are encrypted and stored in the database

**To add a new device credential in the MPLS Inventory, follow the steps:**

1. Navigate to the MPLS Configuration form:
  - a. From the workspace navigation panel, select the **iSPI for MPLS Configuration** workspace.
  - b. Select the **Device Authentication** tab.
2. Click  (the **New** icon) and specify the following details:
  - Management IP address of the device
  
  - User name and password of the device
3. Click  (the **Save** icon).

Repeat these steps for each device you want to add.

**To Enable Telnet Access:**

The NNM iSPI for MPLS uses SSHv2 protocol as the first preference. You can enable or disable Telnet access. When enabled, NNM iSPI for MPLS uses Telnet if SSHv2 fails. To enable Telnet access, select the **Enable Telnet Access** check box. Similarly, to disable telnet access for the devices, you can clear the **Enable Telnet Access** check box.

**Note:** Enabling or disabling Telnet access is applicable for the entire list of configured devices. You can switch between SSHv2 and Telnet for individual devices by [switching Device Access Mode](#).

## Wildcard Support for Device Authentication

You can use wildcard characters; an asterisk (\*) and hyphen (-) in the NNM iSPI for MPLS. You can add authentication parameters to multiple devices by using wildcard characters in the IP addresses.

### Address Range Definition Attribute

Attribute	Description
IP Range	<p>To specify a range of IP addresses, use one of the following. Pick one address notation style, combinations of wildcards:</p> <ul style="list-style-type: none"><li>• <a href="#">IPv4 address wildcard notation</a></li></ul> <p>An IPv4 Address range is a modified dotted-notation where each octet is one of the following:</p> <ul style="list-style-type: none"><li>• A specific octet value between 0 and 255</li><li>• A low-high range specification for the octet value (for example, "112-119")</li></ul>

<sup>1</sup>Secure Shell protocol version 2

## Address Range Definition Attribute, continued

Attribute	Description
	<ul style="list-style-type: none"> <li>• An asterisk (*) wildcard character which is equivalent to the range expression "0-255"</li> </ul> <p>The following two IPv4 addresses are considered invalid:                      0.0.0.0 and 127.0.0.0.</p> <p>Examples of valid IPv4 address wildcards include:</p> <p>10.1.1.*                      10.*.*.*                      10.1.1.1-99                      10.10.50-55.*                      10.22.*.4                      10.1-9.1-9.1-9</p> <p>1.2*-3*.33.4. While (-) is used between octets, you can use (*) to specify a particular range. This example is a valid pattern for IP addresses with second octet ranging from 20-39</p> <ul style="list-style-type: none"> <li>• <b>IPv6 address wildcard notation</b></li> </ul> <p>Separate each 16-bit value of the IPv6 with a colon. The 16-bit value can be any of the following:</p> <ul style="list-style-type: none"> <li>• A specific hexadecimal value between 0 and FFFF (case insensitive)</li> <li>• A low-high range specification of the hexadecimal value (for example, 1-1fe)</li> <li>• An asterisk (*) wildcard character (equivalent to the range expression 0-ffff)</li> </ul> <p><b>Note:</b> The standard IPv6 short-hand notation (::) is allowed to express one or more 16-bit elements of zero (0) values. However, the mixed IPv6/IPv4 dot-notation (for example, 2001:d88::1.2.3.4) is not allowed as an IPv6 address range. Valid examples of ranges in modified IPv6 address notation include the following:</p> <p>2001:D88:0:A00-AFF:*:*:*                      2001:D88:1:*:*:*:*                      2001:D88:2:0:a07:ffff:0a01:3200-37ff</p> <p>Take a note that:</p> <ul style="list-style-type: none"> <li>• The NNM iSPI for MPLS does not support CIDR notations while configuring device authentication.</li> </ul>





### Address Range Definition Attribute, continued

Attribute	Description
	<ul style="list-style-type: none"><li>• If a configured device matches more than one wildcard pattern, the one that is first encountered will be used to get device credentials. For example, if you enter 1.22-25.33.4 and 1.*.33.4; then for a device with IP 1.23.33.4, credential for 1.22-25.33.4 is used.</li><li>• You have to use a specific IP address and its credentials. For example, if you configure 192.165-170.1.4 and 192.168.1.4, credentials for 192.168.1.4 is used. This way, you can have exception for specific devices in configuring credentials.</li><li>• In addition, if you enter 192.*.1.4 and 192.168.1.4, credentials for 192.168.1.4 is used.</li></ul>

## Configure an MPLS Regional Manager Connection

As an administrator, you can configure the NNM 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 NNM iSPI for MPLS Regional Manager connection, follow the steps:

1. Navigate to the Regional Manager form.<sup>1</sup>
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).
  - 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 NNM iSPI for MPLS Regional Manager](#).
5. Select the **Regional Manager Configuration** form, type the basic configuration settings. For more information, see [basic settings](#).
6. From the **Connections** tab, navigate to the **Regional Manager Connections** form. For more information, see [Configure the NNM iSPI for MPLS Regional Manager](#).
7. Click  (the **Save and Close** icon) to close the Regional Manager form.
8. Click  (**save and activate**). The NNM iSPI for MPLS Global Network Manager establishes communication with the specified Regional Manager.

1

- a. From the workspace navigation panel, select the **MPLS Configuration** workspace.
- b. Select the **MPLS Regional Manager Connections** tab.

## Basic Settings

Attributes	Description
Name	Type a name for this configuration record about the Regional MPLS management server.  The NNM 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 NNM iSPI for MPLS Regional Manager.](#)

## Configure the NNM iSPI for MPLS Regional Manager Connection

As an administrator, you can configure the NNM 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 NNM 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 Regional Manager should be same as the NNMi Regional Manager to establish the connection.

To configure the Regional Manager connection, follow the steps:

1. Navigate to the NNM iSPI for MPLS Regional Manager Connection form.<sup>1</sup>
2. Type the connection configuration settings for the NNM 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  (the **Save and Close** icon) to return to the Regional Manager form.
4. Click  (**save and activate**) to return to the MPLS Configuration form. The NNM iSPI for MPLS establishes communication with the Regional NNM 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 NNM iSPI for MPLS

Attribute	Description
Hostname	The fully-qualified hostname of the Regional NNM iSPI for MPLS management server. The NNM iSPI for MPLS uses this hostname for communication with the Regional NNM iSPI for

1

- a. From the workspace navigation panel, select the **MPLS Configuration** workspace.
- b. Select the **Regional Manager Connections** tab.

## Connection Configuration Settings for a Regional Manager of the NNM iSPI for MPLS, continued

Attribute	Description
	<p>MPLS management server and to construct URL Actions. See <i>NNMi Help, Authentication Requirements for launch URLs</i> .</p> <p><b>Note:</b> If you want NNM 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.</p>
Use Encryption	<p>If <input type="checkbox"/> disabled, the NNM iSPI for MPLS uses hypertext transfer protocol (HTTP) and plain sockets to access the NNM iSPI for MPLS Regional management server.</p> <p>If <input checked="" type="checkbox"/> enabled, the NNM iSPI for MPLS uses secure sockets layer encryption (HTTPS / SSL) to access the the NNM iSPI for MPLS Regional management server.</p>
HTTP(S) Port	<p>Default value for HTTP is 24040.</p> <p>Default value for HTTPS 24043.</p> <p>If <input type="checkbox"/> Use Encryption is disabled, enter the port number for HTTP access to the NNMi and MPLS console on the Regional NNMi management server.</p> <p>If <input checked="" type="checkbox"/> Use Encryption is enabled (previous attribute), enter the port number for HTTPS access to the NNMi console on the Regional NNMi management server.</p> <p>For MPLS ports, check the port numbers from the <code>nms-mp1s-ports.properties</code> file. Open the <code>nms-mp1s-ports.properties</code> file from the <code>%NnmDataDir%\shared\mp1s\conf</code> or <code>\$NnmDataDir/shared/mp1s/conf</code> directory on the management server, and then note down the NNM iSPI for MPLS HTTP and HTTPS values if you are not using the default values.</p>
User Name	<p>Type the user name required for the NNM iSPI for MPLS sign-in for the account on the NNM iSPI for MPLS Regional management server. The user name should be same as the name provided while installing the NNM iSPI for MPLS.</p>
User Password	<p>Type the password for the NNM iSPI for MPLS account on the NNM iSPI for MPLS Regional management server.</p> <p><b>Note:</b> The NNM 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.</p>
Ordering	<p>A numeric value. The NNM iSPI for MPLS checks for configuration settings in the order you define (lowest number first). The NNM iSPI for MPLS uses the first match found for each address. Provide a unique connection ordering number for each Regional Manager configuration.</p>

## Managing Nodes

The NNM 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 NNM iSPI for MPLS.

You can manage or stop managing all the MPLS objects such as VPNs, PseudoWires, and so on. However, if a node is not managed, all the MPLS objects on that node such as VRFs, VC LSPs, VFIs, SDPs and SDPBind are Not Managed .

In addition, The state of a 'Not Managed' MPLS object is set to Not Polled and the status is set to No Status if the corresponding Node is not managed. The state of the MPLS object is set to *Not Polled* and the status is set to *No Status*.

If a 'Not Managed' 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.

## NNM iSPI for MPLS System Health Report

You can check the health of the NNM iSPI for MPLS by viewing the MPLS Health Report.

### Launching the MPLS Health Report

Select **Help-> Help for NNM iSPIs -> iSPI for MPLS System Health**

The user interface displays six tabs; Memory Details, CPU Usage Details, System load Avg, Swap and other Details, Database Connection Details, State Poller Health and GNM Health.

The **Memory Details** tab contains the following information:

- Name
- Status
- Used(%)
- Max(MB)
- Committed(MB)

The **CPU Usage** tab contains the following information:

- CPU Usage Details
- Load Average

The **System load Avg, Swap and other details** tab contains the following information:

- Available Processors
- Free Physical Memory
- Physical Memory
- Committed Virtual Memory
- Free Swap Space
- Total Swap Space

The **Database Connection Details** tab contains the following information:

- Connections Available
- Total Connections
- Maximum Connections in Use
- Connection created

- Connection Destroyed
- Connections in Use

The **State Poller Health** tab contains the following information:

- Collections requested in last 5 minutes
- Collections completed in last 5 minutes
- Collections in process
- Time to execute skips in last 5 minutes
- Collector Collection State Count In Last 5 minutes
- Poller result queue length 5 min(avg)

The **GNM Health** tab contains the details of the Regional Managers configured.

## Using Single Sign-On with NNM iSPI for MPLS

By default Single Sign-On is disabled. To enable the Single Sign-On feature, follow these steps after installing the NNM iSPI for MPLS.

Edit `/var/opt/OV/shared/nnm/conf/props/nms-ui.properties`:

- Set `com.hp.nms.ui.sso.isEnabled = true`
- Run `nmssso.ovpl -reload`
- Run `mplssoreload.ovpl`

For more information, see *Using Single Sign-On with NNMi* in *NNMi 9.20 Deployment Reference*.

## Integrating the NNM iSPI for MPLS with Route Analytics Management Software (RAMS)

The HPE Route Analytics Management Software (RAMS) integrates with NNMi to provide the routing protocol path for the layer 3 topology. You can use the RAMS features to monitor the L3 VPNs that use 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.

**Note:** The NNM iSPI for MPLS 10.00 supports integration only with HPE RAMS 9.21.

To monitor the L3 VPNs in the NNM iSPI for MPLS using RAMS, follow these steps:

1. The NNM 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
```

To use the script, follow these steps:

- a. Click the Application button
- b. Click Accessories
- c. Open Terminal
- d. Type the script and hit Enter

With an administrative privilege to the NNMi console, send the L3 VPN name and RT list to the RAMS appliance.

2. After the integration with RAMS, you can monitor and view the SNMP traps from the RAMS appliance. To view the traps from the RAMS appliances navigate to the L3 VPN form and click the RAMS tab. The trap list shows the most recent 100 traps.
3. To monitor the L3 VPN inventory using RAMS, the L3 VPN names should be same as sent to the RAMS appliance.

**Note:** 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:**

[RAMS Traps Tab](#)

## Integrating the NNM iSPI for MPLS with the iSPI for IP Multicast

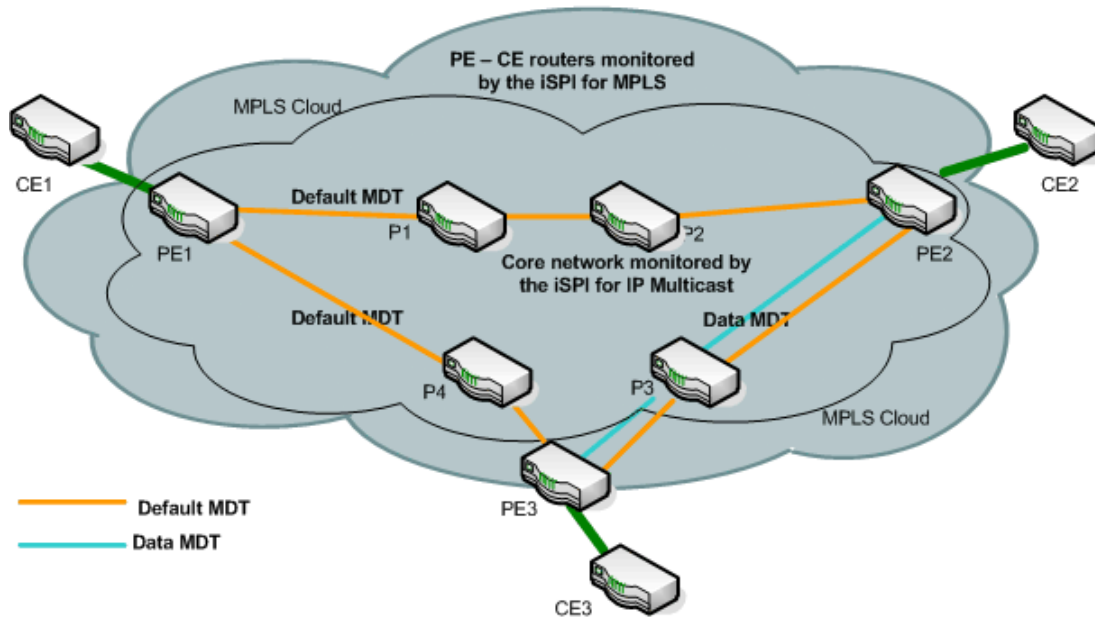
The NNM iSPI for MPLS helps you to monitor the Provider Edge (PE) routers discovered in an MVPN topology. The PE routers are configured with the multicast-enabled VRF (MVRF) capabilities and use the multicast services to transmit data. To view the list of MVPN inventory, see [MVPN Inventory](#). The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



In the example, the NNM 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 on the network.

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

The NNM iSPI for MPLS helps you to monitor the traffic passing through the VRFs on the network. The iSPI Performance for Quality Assurance measures the network traffic performance by configuring various tests on the VRFs. After installing the iSPI Performance for Quality Assurance, the NNM 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 NNM iSPI Performance for QA*.

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

### Related Topic:

[VRF: QA Probes Tab](#)

# Troubleshooting the NNM iSPI for MPLS

The following information can help you troubleshoot and resolve common problems in the NNM 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 > Polling > Configuration Poll**, or use the `nnmconfigpoll.ovpl` command. The NNM iSPI for MPLS uses the NNMi capability to poll the MPLS-enabled nodes. No NNM iSPI for MPLS specific information is displayed.
- **The NNM 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 > Polling > Status Poll**. No NNM 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 NNM iSPI for MPLS objects. Add the node 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 L3 VPN. 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 NNM iSPI for MPLS actions but does not display any message.
- **You performed various configuration actions on a node such as updated community strings. But, the NNM 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.**

By 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 NNM 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 NNM iSPI for MPLS inventory.**

The discovery of CE nodes participating in an L3 VPN 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 NNM iSPI for MPLS.

- **Some columns appear without values in the PE Interface tab and CE Interface tab of VRF Form**


Columns, namely, **Next hop IP**, **Next hop AS**, and **PE-CE protocol** in the **PE Interface** tab and **CE Node**, **Next hop IP**, **Next hop AS**, **PE IfName**, and **PE node** in the **CE interface** tab are visible only when the Inter-Provider VPN feature is turned on for NNM iSPI for MPLS. For more details, see *NNM iSPI for MPLS Deployment Guide*.

- **VRF is displayed as managed even when the VPN it participates in, is Not managed.**

A VRF participating in a VPN that is not managed is displayed as Managed in the following scenario:

- You have changed a 'Managed' VPN to 'Not Managed' hence, the corresponding VRF is not managed and its management mode is set to VPN inherited.
- If you stop managing the node on which this VRF resides and Manage it again, the VRF is reset to Managed state although, the VPN is still Not Managed.

- **Status of 'Not Managed' VPN/VPWS/VPLS has not changed to "No Status".**

Click  (the **Refresh** icon) to see the modified status.

- **Editing a VPWS group returns a 'Jasper Exception'.**

'Jasper Exception' occurs when you edit a VPWS group that contains some special characters ( \ " < > [ \ ] ^ { } % & = # + ) in the name. Do not create VPWS group names with special characters.

- **Exception occurred in L3 VPN Topology View and "Could not get form JSON" message is displayed.**

The exception occurs because VRF peer cannot be opened in the topology view if you do not have access to that VRF peer.

- **Error message: access denied or object does not exist for class com.hp.ov.nms.model.core.Node is displayed in the Analysis Pane**

This error occurs when you try to launch Analysis for a node or an interface for which you do not have access.

# Glossary

## A

---

### **AC**

An attachment circuit (AC) is a physical or virtual circuit (VC) that attaches a CE to a PE

### **ACs**

An attachment circuit (AC) is a physical or virtual circuit (VC) that attaches a CE to a PE

### **Attachment Circuits**

An attachment circuit (AC) is a physical or virtual circuit (VC) that attaches a CE to a PE

## L

---

### **L2 VPN**

L2 VPN or Layer 2 VPN is defined as a Virtual Private Network that is formed by network layer 2 services such as PseudoWire VCs, VPLS, VPWL, LSPs, and TE Tunnels.

### **L2 VPNs**

L2 VPNs or Layer 2 VPNs are defined as Virtual Private Networks that are formed by network layer 2 services such as PseudoWire VCs, VPLS, VPWL, LSPs, and TE Tunnels.

### **L3 VPN**

L3 VPN or Layer 3 VPN is defined as a Virtual Private Network that makes use of layer 3 Virtual Routing and Forwarding tables (VRFs) to form a peer-to-peer network model.

### **L3 VPNs**

L3 VPNs or Layer 3 VPNs are defined as Virtual Private Networks that makes use of

layer 3 Virtual Routing and Forwarding tables (VRFs) to form peer-to-peer network models.

### **Layer 2 VPN**

L2 VPN or Layer 2 VPN is defined as a Virtual Private Network that is formed by network layer 2 services such as PseudoWire VCs, VPLS, VPWL, LSPs, and TE Tunnels.

### **Layer 3 VPN**

L3 VPN or Layer 3 VPN is defined as a Virtual Private Network that makes use of layer 3 Virtual Routing and Forwarding tables (VRFs) to form a peer-to-peer network model.

### **LSPs**

Label Switch Path passing through an MPLS network and is set up by Label Distribution Protocol (LDP). LSP is set up to pass data packets based on Forwarding Equivalence Class. LSPs are unidirectional.

## M

---

### **MPLS network**

Multi Protocol Label Switching (MPLS) is a mechanism used to transfer data between networks based on short path labels. MPLS can encapsulate different network protocols. A network formed by MPLS-enabled devices is called an MPLS network.

### **MVPN**

A VPN that is formed by VRFs residing on Multi-cast enabled routers.

### **MVPNs**

VPNs that are formed by VRFs residing on Multi-cast enabled routers.

### **My Term**

My definition

## P

---

### **PseudoWire VC**

PseudoWire VC is a virtual 'wire' that transfers data from one endpoint to another in an MPLS network.

### **PseudoWire VCs**

PseudoWire VCs are virtual 'wires' that transfer data from one endpoint to another in an MPLS network.

### **PW**

PW or PseudoWire VC is a virtual 'wire' that transfers data from one endpoint to another in an MPLS network.

### **PWs**

PWs or PseudoWire VCs are virtual 'wires' that transfer data from one endpoint to another in an MPLS network.

## R

---

### **Route Target**

A Route Target (RT) is added to a VRF. VRFs with the same RTs form a VPN.

### **Route Targets**

A Route Target (RT) is added to a VRF. VRFs with the same RTs form a VPN.

### **RT**

A Route Target (RT) is added to a VRF. VRFs with the same RTs form a VPN.

### **RTs**

A Route Target (RT) is added to a VRF. VRFs with the same RTs form a VPN.

## T

---

### **TE tunnel**

TE tunnel is a way to establish unidirectional label switching path to enhance the quality of data passing through the MPLS network.

### **TE tunnels**

TE tunnels are a way to establish unidirectional label switching paths to enhance the quality of data passing through the MPLS network.

## V

---

### **VPLS VPN**

Virtual Private LAN Service (VPLS) is a way to provide Ethernet based endpoint to endpoint communication within layer 2 of MPLS network.

### **VPLS VPNs**

Virtual Private LAN Service (VPLS) is a way to provide Ethernet based endpoint to endpoint communication within layer 2 of MPLS network.

### **VPWS VPN**

Virtual Private Wire Service VPN is a layer 2 service in an MPLS network that provides end-to-end connection between the core MPLS network and the Customer sites.

### **VRF**

Virtual Routing and Forwarding (VRF) enables multiple instances of a routing table to co-exist within the same router. These table instances are independent of each other, hence can reside on the same router without any conflict.

### **VRFs**

Virtual Routing and Forwarding (VRF) enables multiple instances of a routing table

to co-exist within the same router. These table instances are independent of each other, hence can reside on the same router without any conflict.

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

**Feedback on Online Help (Network Node Manager iSPI for MPLS Software 10.30)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [network-management-doc-feedback@hpe.com](mailto:network-management-doc-feedback@hpe.com).

We appreciate your feedback!