

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

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

Software Version: 8.10

[Online Help](#)

Document Release Date: February 2008

Software Release Date: December 2008



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

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

Copyright Notices

© Copyright 2009 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Portions Copyright © 1999-2003 The Apache Software Foundation. All rights reserved.

This product includes ASM Bytecode Manipulation Framework software developed by Institute National de Recherche en Informatique et Automatique (INRIA). Copyright © 2000-2005 INRIA, France Telecom. All Rights Reserved.

This product includes Commons Discovery software developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 2002-2008 The Apache Software Foundation. All Rights Reserved.

This product includes Netscape JavaScript Browser Detection Library software, Copyright © Netscape Communications 1999-2001

This product includes Xerces-J xml parser software developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 1999-2002 The Apache Software Foundation. All rights reserved.

This product includes software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). Xpp-3 Copyright © 2002 Extreme! Lab, Indiana University. All rights reserved.

Trademark Notices

DOM4J® is a registered trademark of MetaStuff, Ltd.

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

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

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

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

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing

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

For the full Oracle license text, see the license-agreements directory on the NNMi product DVD.

Table of Contents

Legal Notices	3
Table of Contents	5
Introducing iSPI for MPLS	8
Using iSPI for MPLS	9
Introducing MPLS L3 VPN	9
More about MPLS VPN Network	9
About the VPN, VRF, and Route Targets	10
About VPN and VRFs	10
About Route Targets	10
About VRFs Grouping for VPN	10
About VPN Topology	10
About VPN Naming	11
Introducing MPLS TE Tunnel	12
Introducing MPLS PseudoWire VC	13
Learning your MPLS Inventory	14
Launching the Views	14
Related Topics	14
MPLS L3 VPN Inventory	15
MPLS TE Tunnel Inventory View	16
LSR (Label-Switched Routers) Inventory	17
MPLS PseudoWire VC Inventory	18
Accessing Forms	19
Launching the Forms	20
VPN Form	20
VPN Form: VRF Tab	21
VPN Form: Status Tab	22
VPN Form: Conclusions Tab	23
VPN Form: Registration Tab	28
VRF Form	24
VRF Form: Interfaces Tab	25
VRF Form: Neighbor VRFs Tab	26
VRF Form : Route Target Tab	26

VRF Form: Status Tab	26
VRF Form: Conclusions Tab	27
VRF Form: Incidents Tab	28
VPN Form: Registration Tab	28
PseudoWire VC Form	28
PseudoWire VC Form: VC LSP Tab	29
Pseudowire VC Form: Status Tab	30
PseudoWire VC Form: Conclusions Tab	31
PseudoWire VC Form: Incidents Tab	31
PseudoWire VC Form: Registration Tab	32
TE Tunnel Form	32
TE Tunnel Form: Attributes Tab	34
TE Tunnel Form: Status Tab	35
TE Tunnel Form: Conclusions Tab	35
TE Tunnel Form: Incidents Tab	36
TE Tunnel Form: Registration Tab	36
Node Form: VRF Tab	36
Node Form: TE Tunnel Tab	37
Node Form: PseudoWire VC LSP Tab	37
Introduction to iSPI for MPLS Administrator	39
Updating the NNMi System Password	40
Updating the iSPI (NNMi WebService Password)	40
MPLS Process and Services	40
About MPLS Process	41
Verify that MPLS Processes Are Running	41
Start or Stop MPLS Processes	41
	42
Start and Stop MPLS Services	42
Verify that MPLS Services are Running	42
Log files for the MPLS Services	42
Start and Stop MPLS Services	42
Configuring MPLS Incidents	43
	43
Types of SNMP traps for MPLS	43
Discovering your MPLS Network	44

Discovering Your L3 VPN Network	45
About VPN, VRF	45
Discovery of VPNs	46
Discovering Your MPLS TE Tunnel Network	46
Discovery of the TE Tunnel	47
Discovering Your MPLS PseudoWire VC Network	47
Discovery of the PseudoWire VC	47
Monitoring MPLS Network Health	47
About MPLS State Poller	48
	48
	48
Using MPLS Causal Engine	48
On-Demand Status Poll	48
Troubleshooting Guidelines	49
User Interface	49
Not able to view the TE Tunnels, VRFs, VC LSPs for a node	49
Able to view the node and corresponding iSPI objects, but not accurately. You want to ..	49
view the correct data for this node	
Discovery Process	50
In the node form, the Id field in the PseudoWire VC LSP tab is zero	50
Incidents	50
Others	51
MPLS Polling Configuration	52
Index	53

Introducing iSPI for MPLS

The HP Network Node Manager (NNM) i-series Smart Plug-in for MPLS (**iSPI for MPLS**) provides real-time data that enables you to monitor the health of MPLS Virtual Private Network (VPN), MPLS PseudoWire VC, and Traffic Engineering (TE) tunnels.

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

You can install iSPI for MPLS on an NNMi management station.

The iSPI for MPLS offers the following features:

- Discovers and identifies VPNs configured in the provider edge devices of the MPLS network.
- Discovers and identifies TE tunnels configured in the routers of the network.
- Discovers and identifies PseudoWire VCs configured in network.
- Displays the VPNs, VRFs, TE tunnels, and PseudoWire VCs attributes in the MPLS views.
- Monitors the status of discovered VPNs, VRFs, TE tunnels, and PseudoWire VCs in the network.
- Generates the incidents for the faults or the changes in the topology.

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

[Introducing MPLS VPN](#)

[Introducing MPLS TE Tunnel](#)

[Introducing MPLS PseudoWire VC](#)

For more information about the help for iSPI for MPLS, see [Using iSPI for MPLS](#).

Using iSPI for MPLS

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

After you install NNMi, iSPI discovers the MPLS enabled nodes participating in the network. The iSPI for MPLS helps you to monitor the PE routers participating to form the VPNs in the network. In addition, the iSPI for MPLS helps you to discover and monitor the TE tunnels and PseudoWire VCs.

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

Tasks	Help Topics
More about the VPNs, TE tunnels, PseudoWire VCs	Introducing the MPLS VPN Understanding VPN, VRFs and Route Targets Introducing the MPLS TE Tunnel Introducing the MPLS PseudoWire VC
Viewing the MPLS inventory	About your MPLS Inventory
Viewing the details of the devices	Accessing Forms
Viewing the MPLS incidents	Configuring MPLS incidents
Monitoring the network	Monitoring your Network

Introducing MPLS L3 VPN

The HP Network Node Manager i-series Smart Plug-in for MPLS (**iSPI for MPLS**) discovers VPN network topology and monitors the connectivity between the PE routers taking part in the MPLS VPNs.

More about MPLS VPN Network

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

The iSPI for MPLS has the following features:

Monitor VPNs, VRFs

The iSPI for MPLS discovers the VRFs, and Route Targets belonging to MPLS network. A VPN is formed by the set of Virtual Routing and Forwarding (VRFs) tables on an edge router (PE). The iSPI helps you to monitor, and view the real time status of the complex VPNs. The iSPI generates the incidents if there are some changes in VPNs such as VRF is down which impacts the VPN status.

Manage Faults:

The iSPI for MPLS identifies the change in the topology such as VRF goes down or detects faults in the network, thereby generates new, enriched incidents with detailed information. The enriched incidents help you quickly understand and react to a problem in your network. For more details, see [MPLS Incidents](#).

To understand more about the VPN, VRFs, see [Knowing About VPN, VRF, and Route Targets](#).

About the VPN, VRF, and Route Targets

To understand how you can manage your MPLS network, we should know more about VPN, VRF and Route Targets.

About VPN and VRFs

A VPN is formed by the set of Virtual Routing and Forwarding (VRFs) tables on an edge router.

A VRF includes the routing information that defines the VPN that is attached to a PE router. Each VRF is on a PE router. All PE routers containing VRFs relevant to the named VPN are grouped in one VPN and displayed in the view. A VRF can only belong to a single VPN and is grouped on the basis of the Route Targets.

About Route Targets

A Route Target (RT) is defined as an extended community that identifies a group of routers and, in each router of that group, a subset of forwarding tables maintained by the router that may be populated for the route. The Route Targets are additional attributes attached to routes to indicate VPN membership. Any number of RTs can be associated in single route.

About VRFs Grouping for VPN

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

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

You can exclude or ignore the Route Targets by using the Polling Configuration UI. This results in re-grouping of VRFs and thus re-computing to form the VPNs. The status is updated after the VPN is formed.

About VPN Topology

The VPN topology covers the types of VPNs in the network. For iSPI for MPLS, we have defined three types of VPN topologies listed below.

- Full-Mesh - Full Mesh VPN is formed if all the VRFs have the same RT. The same RT is used for importing and exporting in all the VRFs in the specific group. Each VRF exports its route targets to all VRFs in the VPN and imports all route targets from the other VRFs in the VPN. All the PE routers are communicating with each other.
- Other - All the VRFs are not communicating with all other VRFs belonging to a VPN. For example, hub and spoke, hybrid topology.
- Isolated - A VRF forming a single VPN (no other VRF imports the route targets of this VRF).

About VPN Naming

All the VPNs are named by the internal system naming convention. You can change and rename the system populated VPN name.

The system generated VPN names are derived from the VRF grouping relationships.


The iSPI for MPLS attempts to assign a meaningful VPN name to each discovered VRF group according to specific rule.

The rules are listed below:

- If the discovered VRFs have the common name, VPN name is derived by the common VRF name. If the name is already used by one of the VPNs, the system generated name will be the common VRF name appended with Id.
- If the discovered VRF group does not have the common VRF name, the iSPI creates a new VPN name by the following rules:
 - If at least 65 percent of the VRFs in the group have the same name and that name would be a unique VPN name, assign that text string as the VPN name for the VRF group.
 - If at least 65 percent of the VRFs in the group have the same name and that name is already a VPN name for another VRF list, assign the VPN name as the VRF name appended with an underscore followed by the VPN internal identification number for this VRF group.
- If at least the first three characters of each name in the VRF group matches, set the VPN name to the initial matching characters.
- For the isolated VPN, name is taken directly from the isolated VRF.

For example:

VRFs in the VPN	Selected VPN Name	Explanation
VRF 1- Blue VRF 2- Blue	Blue	Both the VRF name are same.
VRF 1- Blue VRF 2- Green VRF 3- Green VRF 4- Green	Green	The majority name is selected.
Red_East Red_West	Red	The common initial characters.

You can change the system populated name of the VPN. In the [VPN Form](#), rename the VPN and click  Save and Close.

Introducing MPLS TE Tunnel

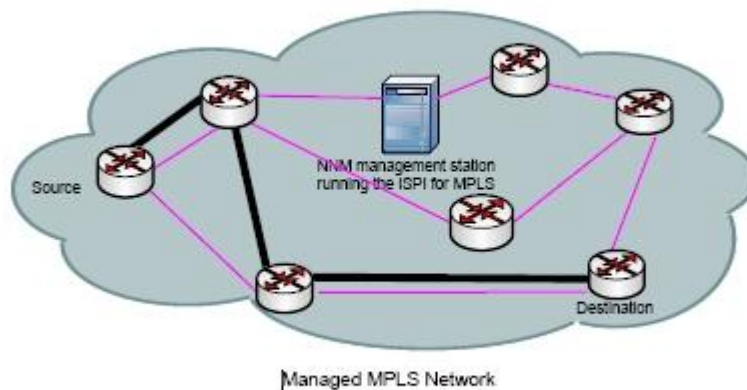
In an MPLS Traffic Engineering network, communication between the routers is through the TE tunnels. The TE tunnels help manage the data transmission from the source to destination.

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 Quality of Service (QoS). Traffic Engineering (TE) is essential for service provider backbones.

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

HP Network Node Manager i-series Smart Plug-in for MPLS (iSPI for MPLS) discovers and monitors the TE tunnels in an MPLS network. The iSPI for MPLS detects the faults in MPLS traffic engineering tunnels.

Example of MPLS Network having TE Tunnel



The iSPI for MPLS has the following TE Tunnel features:

Monitor TE Tunnels:

The iSPI for MPLS discovers the tunnels, and displays the attributes and status of the tunnels participating in the MPLS network. The iSPI generates incidents if any fault or change is detected in the MPLS network. This helps in fault management and reduces the Mean Time to Repair (MTTR).

Manage Faults:

The iSPI for MPLS identifies the fault in the tunnels, and generates a detailed enriched event for the detected fault or the activity. This facilitates in understanding the cause and responding to the fault in your network much faster. This result in better quality of service to customers.

Introducing MPLS PseudoWire VC

In an MPLS network, communication between the routers is through PseudoWire Virtual Channel (VC). PseudoWire VC is the connection link for data transmission between the two endpoints.

A PseudoWire VC is defined as an emulated point-to-point connection over a packet switched network (PSN) that allows the interconnection of two nodes with any L2 technology. There are two types of L2VPNs - [Virtual Private Wire Service \(VPWS\)](#)¹ and [Virtual Private LAN Service VPLS](#)². The data transmission can be through Frame Relay, ATM.

In PseudoWire VC, the transmission of data is bi-directional. For example, if there are two endpoints such as A and B, data is transmitted from A to B and B to A. A bidirectional PseudoWire VC consists of a pair of unidirectional LSPs, one in each direction. The LSPs are identified by the unique VC ID in between two endpoints. For the Pseudowire VC to be discovered fully, make sure that both the endpoints (VC LSPs) are discovered.

The iSPI for MPLS discovers and monitors the PseudoWires VCs in the network. The iSPI for MPLS monitors and detects the faults in PseudoWire VC.

The following list outlines the PseudoWire VC features:

Monitor PseudoWire VC

The iSPI for MPLS discovers the PseudoWires VC and displays the VC ID, attributes, and the status of the PseudoWire VCs participating in the MPLS network. The iSPI for MPLS generates incidents if any fault or change is detected in the network. This ensures better efficiency in managing the PseudoWires VC.

Manage Faults :

The iSPI for MPLS identifies the fault in the PseudoWires VC and generates an incidents for the detected fault or the activity. This facilitates in understanding the cause and responding to the fault in your network much faster. The iSPI helps in fault management and reduces the Mean Time to Repair (MTTR).

¹A Virtual Private Wire Service VPWS is a point-to-point link connecting two Customer Edge devices. The link is established as a logical path through a packet switched network.

²A VPLS is a provider service that emulates the full functionality of a traditional Local Area Network (LAN). A VPLS makes it possible to interconnect several LAN segments over a packet switched network (PSN) and makes the remote LAN segments behave as one single LAN.

Learning your MPLS Inventory

After the regular discovery of the MPLS nodes, you have several options to view the information from MPLS workspace. The MPLS views provide the comprehensive attributes of all the discovered MPLS nodes. See up-to-date information for each of the following:



View Type	Purpose
LSR(Label-Switched Routers) Inventory	Lists all the MPLS enabled routers managed by iSPI for MPLS. The MPLS enabled routers are configured with VPNs, TE Tunnels, and PseudoWire VCs.
TE Tunnel Inventory	Provides information about the Traffic Engineering(TE) tunnels that are discovered by iSPI in the network.
L3 VPN Inventory	Provides information about all the VPNs discovered in the network.
PseudoWire VC Inventory	Provides information about the PseudoWire VCs discovered in the network.

Launching the Views

To launch the MPLS specific views

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

Following features are available in the view:

- Access the forms for detailed information: Click the  Open icon to view the detailed information about a specific MPLS object.
- Quick View information: To know more about the selected object attributes, click  Quick view icon.
- Filter option in the view: You can filter the **Status and Name** column in the table view to categorize and view the relevant information . The filters configured on the views are restored when the views are opened again. This is very useful as you do not have to configure the filtering option again. Right-click the column name to select the columns for filtering.
- Sorting option in the view: You can sort the column in ascending or descending order. Sorting is enabled only for limited columns. Sorting is enabled only for limited columns.

For further reference, see *Help for NNMi, Use Table View*.

Related Topics

[MPLS VPN View](#)

[MPLS TE Tunnels View](#)








[MPLS LSR View](#)

[MPLS PseudoWire VC View](#)

MPLS L3 VPN Inventory



The MPLS L3 VPN Inventory displays high-level information about the Virtual Private Network(VPNs) in the network.

The MPLS L3 VPN view in MPLS workspace is useful for identifying all the routers participating to form a VPN.

Attribute	Description
Name	<p>The subsystem generated name extracted at the discovery.</p> <p>You can update the system generated VPN Name in the forms. Type the new name in the Name box. Click  Save and Close button to update the modified VPN Name in database.</p> <p>For more details about the VPN internal naming rule, refer Knowing About the VPN, VRF, and Route Targets.</p>
Status	<p>The overall status of the VPN. The status of the VPN is derived and calculated based on the status of all the VRFs participating in the VPN. Possible values are as follows:</p> <p> No Status - VPN is newly formed and not polled, status of the VPN is No Status. When all the VRFs participating to form a VPN are in unmanaged mode, the derived status of the VPN is No Status .</p> <p> Normal - The status of the VPN is Normal if all the VRFs in the VPN have the Normal status .</p> <p> Unknown - The status of the VPN is Unknown if all the VRFs are unknown in a VPN.</p> <p> Warning - The status of the VPN is Warning if one or more VRFs in a VPN are unknown and none of them have critical status.</p> <p> Minor - The status of the VPN is Minor if one or more VRFs in a VPN are having critical status.</p> <p> Critical - The status of the VPN is Critical if all the VRFs in a VPN are having critical status.</p>
VPN Type	<p>The type of connectivity within the VPN.</p> <p>Possible values are as follows:</p> <p>Full Mesh - Full Mesh VPN is formed if all the VRFs have the same RT. The same RT is used for importing and exporting in all the VRFs in the specific group. Each VRF exports its route targets to all VRFs in the VPN and imports all route targets from the other VRFs in the VPN. All the PE routers are communicating with each other.</p> <p>Other - All the VRFs are not communicating with all other VRFs belonging to a VPN. for example, hub and spoke, hybrid topology.</p> <p>Isolated - Single VRF forming single VPN (no other VRF imports the route targets to this VRF).</p>
Number of VRFs	<p>This value depicts the number of the VRFs involved in forming a VPN. A VPN is formed by a one or more VRFs. Each VRF is on a PE router.</p>

Attribute	Description
Status Last Modified	The status of the VPN is calculated whenever there is a change in topology. The Status Last Modified is the time when the status was last updated.

Following features are available in the view:




- Access the forms for detailed information: Click the  Open icon to view the detailed information about a specific node.
- Quick View information: To know more about the selected object attributes, click  Quick view icon.
- Filter option in the view: You can filter the **Status** and **Name** column in the table view to categorize and view the relevant information. The filters configured on the views are restored when the views are opened again. This is very useful as you do not have to configure the filtering option again. To filter the table view, Right click the column name to select the type of filter. You can also filter the table view using more than one column. For example: VPN table can be filtered by both VPN Name and Status.
- Sorting option in the view: You can sort the column in ascending or descending order. Sorting is enabled only for limited columns. Sorting is enabled only for limited columns.

For further information for filter, and sorting, refer *Help for NNMi, Use Table View*.

MPLS TE Tunnel Inventory View



The MPLS TE Tunnel Inventory view displays high-level information about the Traffic Engineering(TE) tunnels in the MPLS network.

The MPLS TE Tunnels view in MPLS Inventory workspace is useful for identifying all of the nodes participating in TE tunnels and are managed by Network Node Manager.

Attribute	Description
Status	<p>Overall status of the TE Tunnel. Possible values are :</p> <p> Normal - If the tunnel is Up, the status of the tunnel is Normal.</p> <p> Critical - If the tunnel is Down, the status of the tunnel is Critical.</p> <p> Unknown - The MIB value reports the value of the node to be unknown. and there is no SNMP response for the selected node and if the tunnel is configured on this node, the status of the tunnel is Unknown.</p>
Name	<p>The name is assigned at the time of configuration of the tunnel by the network administrator and the same name is extracted from the router.</p> <p>This name is not editable in the view.</p>
Head	<p>The head is the starting router from which the tunnel is configured. The head and name together makes the unique identification for the tunnel. Multiple tunnels can originate from the same head router.</p> <p>If a head router is an unmanaged node or does not respond to SNMP at the time of discovery, no tunnels starting from that head are discovered.</p>
Tail	The tail is the end router to which the tunnel is configured. The tail field is blank when the tail node is not discovered or managed by NNMi.
Tail IP Address	The IP address on which the tunnel is configured. The Tail IP address is beneficial when the tail node is not discovered by NNMi.

Attribute	Description
Bandwidth	<p>The bandwidth configured for the particular tunnel. The value is the maximum data rate for the particular tunnel.</p> <p>Note: The bandwidth value for tunnels is sometimes zero. This is due the fact that the router itself is reporting the zero value for the bandwidth even though the tunnel may be having non-zero bandwidth.</p>
Description	The description provides the information about the tunnel given by the administrator at the time of configuration.

Following features are available in the view:









- Access the forms for detailed information : Click the  Open icon to view the detailed information about a specific node.
- Quick View information: To know more about the selected object attributes, click  Quick view icon.
- Filter option in the view: You can filter the **Status** and **Name** column in the table view to categorize and view the relevant information . The filters configured on the views are restored when the views are opened again. This is very useful as you do not have to configure the filtering option again. To filter the table view, Right-click the column name to select the type of filter. You can filter the table view using more than one column. For example: TE Tunnel table view can be filtered by both Name and Status.
- Sorting option in the view: You can sort the column in ascending or descending order. Sorting is enabled only for limited columns.




For further information for filters and sorting, see *Help for NNMi, Use Table View*.

LSR (Label-Switched Routers)Inventory



The LSR Inventory displays high-level information about the routers which are MPLS enabled in the network.

The LSR Inventory is an active table that lists all routers participating in MPLS VPN, PseudoWire VC, and TE tunnels managed by the iSPI for MPLS.

Attribute	Description
Status	<p>The status of the node. Possible values are:</p> <ul style="list-style-type: none">  No Status  Normal  Disabled  Unknown  Warning  Minor  Major  Critical

Attribute	Description
Name	The name is given at the time of configuration by the network administrator and the same name is extracted from the router.
Device Profile	The device and vendor information is extracted from the MIB at the time of MPLS discovery.
L3VPN-PE	The MPLS discovery agents checks for L3 VPN capability in the MPLS enabled routers. If L3VPNs are configured in the MPLS enabled routers, the value is true. The possible values are true or false. True is represented by  .
L2VPN-PE	The MPLS discovery agents checks for PseudoWire VCs capability in the MPLS enabled routers. If the PseudoWire VCs are configured in the router, the value is true. The possible values are true or false. True is represented by  .
TETunnel-Head	The MPLS discovery agents checks for the TE Tunnel capability in the MPLS enabled routers. If the TE tunnel is configured in the router, the value is true. The possible values are true or false. True is represented by  .

Following features are available




- Access the forms for detailed information : Click the  Open icon to view the detailed information about a selected MPLS node.
- Quick View information: To know more about the selected object attributes, click  Quick view icon.
- Sorting option in the view: You can sort the column in ascending or descending order. Sorting is enabled only for limited columns.
- Filter option is not available this view.

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

MPLS PseudoWire VC Inventory



The MPLS PseudoWire VC Inventory view displays high-level information about the PseudoWire VCs in the MPLS network.

The MPLS PseudoWire VC view in MPLS Inventory workspace is useful for identifying all of the nodes configured with PseudoWire VCs.

Attribute	Description
Status	Overall status of the PseudoWire VCs. Possible values are :  Normal - Both the LSPs (Label Switched Path) are Normal, status is Normal.  Critical - Any one or both the LSPs are Critical, status is Critical.  Unknown - Any one or both the LSPs are Unknown, status is Unknown.
Id	The unique index ID given for each virtual circuit.
Type	The kind of service carried in the specific PseudoWire VC. For example, the service can be ATM, Frame Relay.
PE 1	The PE router name extracted from the database. This router is one of the endpoints of the PseudoWire VC.

Attribute	Description
	Note: At the time of discovery, if PE1 is unknown,unmanaged or not discovered , you get no information for the name of PE1 thus the field is blank. If PE2 is managed and discovered, you get information of PE1 Address.
PE 1 Address	The IP address of the PE1 on which the specific PseudoWire VC is configured.
PE 2	The PE router name extracted from the database. This router is one of the endpoints of the PseudoWire VC. Note: At the time of discovery, if PE2 is unknown,unmanaged or not discovered , you get no information for the name of PE2 thus the field is blank. If PE1 is managed and discovered, you get information of PE2 Address.
PE 2 Address	The IP Address of the PE2 on which the specific PseudoWire VC is configured.
Status Last Modified	The status of the PseudoWire VCs are calculated whenever there is a change in topology. The Status Last Modified is the time when the status was last updated.

Following features are available in the view:

- Access the forms for detailed information: Click the  Open icon to view the detailed information about a specific node.
- Quick View information: To know more about the selected object attributes, click  Quick view icon.
- Filter option in the view: You can filter the **Status** and Id column in the table view to categorize and view the relevant information . The filters configured on the views are restored when the views are opened again. This is very useful as you do not have to configure the filtering option again. To filter the table view, Right-click the column name to select the type of filter. You can also filter the table view using more than one column. For example: The table view can be filtered by both Id and Status.
- Sorting option in the view: You can sort the column in ascending or descending order. Sorting is enabled only for limited columns.

Accessing Forms

The iSPI for MPLS provides forms that help you to view all details associated with a iSPI object such as nodes, interfaces, VPNs, and VRFs.

The following MPLS forms are available from the MPLS workspace:

Name of Forms	Description
VPN Form	The VPN form provides the details of the selected VPN listing the details of the VRFs involved in forming the VPN. See VPN Form for details.
VRF Form	The VRF form provides the details about the selected VRF for a VPN. See VRF Form for details.
TE Tunnel Form	The TE Tunnel form provides the details of the selected TE tunnel. See TE Tunnel Form for details.


Name of Forms	Description
PseudoWire VC Form	The PseudoWire VC form provides the details of the selected PseudoWire VC. See PseudoWire VC Form for details.

All the forms have the different tabs such as Status, Conclusions, Incidents specifying the details of the objects such as VRFs, VPN, TE Tunnel, and PseudoWire VC.

Launching the Forms

Steps to launch the forms

(1. From the Left navigation panel, select the MPLS Workspace and click <MPLS> view (for example, **MPLS- > MPLS L3VPN view**).

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

To know more about MPLS incidents, refer the [MPLS Incidents](#) and to understand the incidents attributes, see *NNMi Incident form*

VPN Form


The VPN form provides the details of the selected VPN listing the details of the VRFs involved in forming the VPN.







The VPN form displays the PE routers with VRFs that participate in a specific VPN.

A VPN is formed by a number of VRFs. A VRF includes the routing information that defines the VPN that is attached to a PE router. Each VRF is on a PE router. All PE routers containing VRFs relevant to the named VPN are grouped in one VPN and displayed in the view. A VRF can only belong to a single VPN and is grouped on the basis of the Route Targets. Each VRF exports its route targets to other VRFs in the VPN. Similarly, each VRF imports route targets from other VRFs in the VPN. The import/export relationship creates the logical VRF-VRF adjacency relationship.

The VPN form displays all the VPN details such as Name, VPN type, number of VRFs forming the VPN.

Basic Attributes

Attribute	Description
Name	<p>The subsystem generated name extracted at the discovery. You can update the system generated VPN Name in the forms. Type the new name in the Name box. Click  Save and Close button to update the modified VPN Name in database.</p> <p>For more details about the VPN renaming, refer Knowing About the VPN, VRF, and Route Targets.</p>
VPN Type	<p>The type of connectivity within the VPN.</p> <p>Possible values are as follows:</p> <p>Full Mesh - Full Mesh VPN is formed if all the VRFs have the same RT. The same RT is used for importing and exporting in all the VRFs in the specific group. Each VRF exports its route targets to all VRFs in the VPN and imports</p>

Attribute	Description
	<p>all route targets from the other VRFs in the VPN. All the PE routers are communicating with each other.</p> <p>Other - All the VRFs are not communicating with all other VRFs belonging to a VPN. for example, hub and spoke, hybrid topology.</p> <p>Isolated - Single VRF forming single VPN (no VRF imports the route targets of this VRF).</p>
Status	<p>The overall status of the VPN.</p> <p>Possible values are as follows:</p> <p> No Status - VPN is newly formed and not polled, status of the VPN is No Status. When all the VRFs participating to form a VPN are in unmanaged mode, the derived status of the VPN is No Status.</p> <p> Normal - The status of the VPN is Normal if all the VRFs in the VPN have the Normal status .</p> <p> Unknown - The status of the VPN is Unknown if all the VRFs are unknown in a VPN.</p> <p> Warning - The status of the VPN is Warning if one or more VRFs in a VPN are unknown and none of them have critical status.</p> <p> Minor- The status of the VPN is Minor if one or more VRFs in a VPN are having critical status.</p> <p> Critical - The status of the VPN is Critical if all the VRFs in a VPN are having critical status.</p>
Create Time	The time when the VRFs are discovered and VPN is formed and created in MPLS database.
Status Last Modified	The status of the VPN is calculated whenever there is a change in topology. The Status Last Modified is the time when the status was last updated.
Number of VRFs	A VPN is formed by a one or more VRFs. Each VRF is on a PE router. This value depicts the number of the VRFs involved in forming a VPN.


For more information for the tabs, refer [VRFs Tab](#), [Conclusions Tab](#), [Status Tab](#), [Registration Tab](#).




VPN Form: VRF Tab


The VPN form contains details about the selected VPN from the VPN inventory view.

The VRF tab lists the details of the VRFs involved in the VPN.

VRF Details

Attributes	Description
Status	<p>Overall status for the current VRF.</p> <p>Possible values are:</p> <p> No Status- VRF is newly created and not polled, status of the VRF is No</p>

Attributes	Description
	<p>Status.</p> <p> Normal- Indicates the VRF is Up.</p> <p> Unknown- Indicates VRF is not reachable, not responding, status is Unknown.</p> <p> Critical- Indicates VRF is Down, status of the VRF is Critical.</p>
Name	The name is obtained from the PE router during iSPI for MPLS discovery.
PE Node	The router name extracted from 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 devices and with customer devices.
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. This uniqueness provides for accurate resolution of overlapping IP address domains.






Click the  Open icon to view the detailed information about a specific object. The form displays the information specific to the MPLS object.


VPN Form: Status Tab

The [VPN Form](#) provides details about the all the VRFs participating in VPN.

The Status tab is useful for obtaining a quick summary of the SPI object status to better determine and monitor any significant patterns in behavior and activity.

Overall status

Attributes	Description
Status	<p>The overall derived status of the VPN. The status of the VPN is derived and calculated based on the status of all the VRFs participating in the VPN.</p> <p>Possible values are as follows:</p> <p> No Status- VPN is newly formed and not polled, status of the VPN is No Status. When all the VRFs participating to form a VPN are in unmanaged mode, the derived status of the VPN is No Status .</p> <p> Normal- The status of the VPN is Normal if all the VRFs in the VPN have the Normal status .</p> <p> Unknown- The status of the VPN is Unknown if all the VRFs are unknown in a VPN.</p> <p> Warning- The status of the VPN is Warning if one or more VRFs in a VPN are unknown and none of them have critical status.</p> <p> Minor- The status of the VPN is Minor if one or more VRFs in a VPN are having critical status.</p>







Attributes	Description
	 Critical- The status of the VPN is Critical if all the VRFs in a VPN are having critical status
Time Stamp	Current status is calculated and set by Causal Engine. The Time Stamp data displays the time when the status of the VPN is last updated.

VPN Form: Conclusions Tab

The VPN Form contains details about the all the VRFs participating in the VPN.

The conclusions tab depicts the results of the overall derived status. This tab is useful for obtaining a quick summary of the status and problem description for the selected VPN. The conclusions are derived from the overall status of the VPN.

Conclusions Table

Attribute	Description
Status	<p>The overall derived status of the VPN. The status of the VPN is derived and calculated based on the status of all the VRFs participating in the VPN.</p> <p>Possible values are as follows:</p> <p> No Status - VPN is newly formed and not polled, status of the VPN is No Status.</p> <p> Normal - The status of the VPN is Normal if all the VRFs in the VPN have the Normal status .</p> <p> Unknown - The status of the VPN is Unknown if all the VRFs are unknown in a VPN.</p> <p> Warning -The status of the VPN is Warning if one or more VRFs in a VPN are unknown and none of them have critical status.</p> <p> Minor - The status of the VPN is Minor if one or more VRFs in a VPN are having critical status.</p> <p> Critical - The status of the VPN is Critical if all the VRFs in a VPN are having critical status.</p>
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	<p>The conclusions are set by the Causal Engine after the status calculation.</p> <p>The following conclusions that appears are listed below:</p> <ul style="list-style-type: none"> ● VPNCritical - Indicates all the VRFs participating in the VPN are having Critical status. ● VPNNormal - Indicates all the VRFs participating in the VPN are having Normal status. ● VPNUnknown -. Indicates all the VRFs participating in the VPN are

Attribute	Description
	<p>having Unknown status.</p> <ul style="list-style-type: none"> ● VPNMinor- Indicates that any one of the VRF participating in the VPN is having critical status. ● VPNWarning - Indicates the status of any one of the VRF participating in the VPN is Unknown and none of the VRFs have Critical status.

VPN Form: Registration Tab

The VPN Form contains details about the selected VPN.

Registration Table





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

VRF Form

The VRF form provides details about the selected VRF.

This form also provides details about the [Interfaces](#), [Neighbors VRFs](#), the [Route Targets](#), the [Conclusions](#), and the incidents associated with this node.

Basic Attributes

Attributes	Description
Name	The name is obtained from the PE router during iSPI for MPLS discovery.
PE Node	<p>The router name extracted from 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 devices and with customer devices.</p> <p>The selected VRF is configured in this PE Node.</p> <p>You can access the node details from this field. For more information for the node , see <i>NNMi Help</i>.</p>
Status	<p>Overall status for the current VRF.</p> <p>Possible values are:</p> <ul style="list-style-type: none">  No Status - VRF is newly created and not polled, status of the VRF is No Status.  Normal - If the VRF is Up, status of the VRF is Normal.  Unknown - If the VRF is not reachable, not responding, the status is Unknown.  Critical - If the VRF is Down, status of the VRF is Critical. <p>VRF status is derived from SNMP polling (MIBs).</p>

Attributes	Description
Management Mode	<p>Indicates whether the current node is being managed. This field also lets you specify whether a node is temporarily out of service.</p> <p>Possible values are:</p> <p>Managed – Indicates the node, interface or address is managed by NNMi.</p> <p>Not Managed – Indicates 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.</p> <p>Out of Service – Indicates a node is unavailable because it is out of service. NNMi does not update discovery information or monitor these nodes. This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed.</p> <p>For more information, see the Help for NNMi, <i>View the Management Mode for an Object in Your Network</i>.</p>
Description	The description value is obtained from the PE router during the discovery process.
RD	The numerical route distinguisher of the VRF.
Create Time	The time when the VRF is formed by one or more VRFs.
Status Last Modified	The Status Last Modified is the time when the status was last updated.
VPN	The selected VRF belongs to this specified VPN name. You can access the VPN details from this field.

For more information for the tabs, see [Interfaces Tab](#), [Neighbors Tab](#), [Route Targets Tab](#), [Status Tab](#), [Conclusions Tab](#), [Incidents Tab](#), [Registration Tab](#).

VRF Form: Interfaces Tab

The VRF form contains details of all interfaces participating in the VRFs.

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

General

Attribute	Description
Interface Attributes	<p>The attributes listed in the interface tab are same as available in NNMi Interface form.</p> <p>For more information for the attributes, see the Help for <i>NNMi Interface Form</i>.</p>

VRF Form: Neighbor VRFs Tab

The [VRF Form](#) contains details about the selected VRF.

The Neighbor VRFs tab lists the incoming 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 a RT belongs to more than one VRF, then all the VRFs are grouped by the VPN. The data in the VRF Neighbors tab is a subset of the information from the VRF form listing the inventory of VRFs for a VPN.

The attributes of the Neighbor VRFs provides the basic information such as status, PE node, name of the neighbor VRF, and description.

Basic Attributes

Attributes	Description
Neighbors Group	Table view of all 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 for the attributes, see the VRF Form .

VRF Form : Route Target Tab

The VRF form contains details about the selected VRF having the Route Targets.

The Route Target tab specifies the attributes of the RTs participating in the VRF.

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

Attribute	Description
Route Target	The list of Route Targets participating in the selected VRF.
Export	The Route target which is exported for the selected VRF.
Import	The Route Target which is imported for the selected VRF.
Ignore RT	The Route Targets which are ignored for the selected VRF.





VRF Form: Status Tab

The [VRF Form](#) contains details about the selected VRF.

The Status tab is useful for obtaining a quick summary of the SPI object status to better determine and monitor any significant patterns in behavior and activity.

Status Table

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





Attributes	Description
	 No Status - VRF is newly created and not polled, status of the VRF is No Status.  Normal - Indicates the VRF is Up, status of the VRF is Normal.  Unknown - Indicates the VRF is not reachable or not responding, the status is Unknown.  Critical - Indicates the VRF is Down, status of the VRF is Critical. <p>The status attribute contains the list of the last five changes for the selected node.</p>
Time Stamp	Current status is set by Causal Engine. The Time Stamp data is the time when the status of the VRF is last updated.

VRF Form: Conclusions Tab

The [VRF Form](#) contains details about the selected VRF.

The Conclusions tab provides the results of the overall derived status. This tab is useful for obtaining a quick summary of the status and problem description for the VRF that results in VPN status.

Conclusions Table

Attributes	Description
Status	<p>The status of the selected VRF is dependent on the status of the interface on the selected VRF.</p> <p>Possible values are:</p>  No Status - VRF is newly created and not polled, status of the VRF is No Status.  Normal - If the VRF is Up, status of the VRF is Normal.  Unknown - If the VRF is not reachable, not responding, the status is Unknown.  Critical - If the VRF is Down, status of the VRF is Critical.
Time Stamp	Current status is set by Causal Engine. The Time Stamp data is the time when the status of the VRF is last updated.
Conclusions	<p>The conclusions are set by the Causal Engine after the status calculation.</p> <p>The following conclusions that appears are listed below:</p> <ul style="list-style-type: none"> ● MplsVRFDwn - The status of the VRF is Down. ● MplsVRFUp - The status of the VRF is Normal. ● MplsVRFUnknown - The status of the VRF is Unknown. <p>The VRF down conclusion also generates the incident.</p>

Attributes	Description
------------	-------------

Example: MplsVRFDn generates MplsVRFDn incident

VRF Form: Incidents Tab

The [VRF Form](#) provides details about the selected VRF.

This tab is useful for obtaining a quick summary of the problem description for the VRFs.

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>

VPN Form: Registration Tab

The VPN Form contains details about the selected VPN.

Registration Table




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

PseudoWire VC Form

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

Basic Attributes

Attributes	Description
Id	The unique index ID given for each virtual circuit.
Type	The kind of service carried in the specific PseudoWire VC. For example, the service can be ATM, Frame Relay.
PE 1	<p>The PE router name extracted from the database. This router is one of the endpoints of the PseudoWire VC.</p> <p>The PE router name extracted from the database. This router is one of the endpoints of the PseudoWire VC.</p> <p>Note: At the time of discovery, if PE1 is unknown,unmanaged or not discovered, you get no information for the name of PE1, thus the field is blank. If PE2 is managed and discovered, you get information of PE1 Address.</p>

Attributes	Description
PE1 Address	The IP Address of the PE1 on which the specific PseudoWire VC is configured.
PE 2	The PE router name extracted from the database. This router is one of the endpoints of the PseudoWire VC. Note: At the time of discovery, if PE2 is unknown,unmanaged or not discovered , you get no information for the name of PE2 thus the field is blank. If PE1 is managed and discovered, you get information of PE2 Address.
PE 2 Address	The IP Address of the PE2 on which the specific PseudoWire VCis configured.
Status	Overall status of the PseudoWire VCs. Possible values are :  Normal - Both the LSPs are Normal, status is Normal  Critical - Any one or both the LSPs are Critical, status is Critical.  Unknown - Any one or both the LSPs are Unknown, status is Unknown.
Discovery State	The discovered state of the PseudoWire VCs. Possible values are: Fully Discovered - Both the endpoints (PE1 and PE2) are known and both the LSPs are normal. Partially Discovered - One of the endpoint(PE1) is known and PE2 is unknown, unmanaged or, not discovered. You can only get the PE1 information and PE2 IP Address. This state is partially discovered.
Create Time	The time when the PseudoWire VCs are discovered and created in MPLS database.
Status Last Modified	The status of the PseudoWire VC is calculated whenever there is a change in topology. The Status Last Modified is the time when the status was last updated.

Note: The Quick view is not available in this form.




For more information for the tabs, refer [VC LSP Tab](#), [Conclusions Tab](#), [Incidents Tab](#), [Status Tab](#), [Registration Tab](#)

PseudoWire VC Form: VC LSP Tab

The PseudoWire VC LSP tab provides the detailed information of the selected PseudoWire VC.

The VC LSP tab provides the attributes of the VC LSPs participating in the formation of PseudoWire VC.

VC LSP Table

Attribute	Description
Status	Overall status of the Pseudo Wires. Possible values are :  Normal - Both the LSPs are Normal, status is Normal  Critical - Any one or both the LSPs are Critical, status is Critical.  Unknown - Any one or both the LSPs are Unknown, status is Unknown.

Attribute	Description
Source	Indicates the starting router from which PseudoWire VC is configured.
Destination Address	Indicates the IP Address of the End point 2(destination) on which the specific PseudoWire VC is configured.
Name	<p>The name is assigned at the time of configuration of the PseudoWire by the network administrator and the same name is extracted from the router.</p> <p>This name is not editable in the view.</p>
Description	The description provides the information about the VC LSP given by the administrator at the time of configuration.
PSN Type	Indicates the type of Packet Switched Network (PSN) for the selected VC LSP.
Management Mode	<p>Indicates whether the current node is being managed by NNMi. This field also lets you specify whether a node is temporarily out of service.</p> <p>Possible values are:</p> <p>Managed – Indicates the node, interface or address is managed by NNMi.</p> <p>Not Managed – Indicates the node is not managed by NNMi. For example, the node might not be accessible because it is in a private network. NNMi does not update discovery information or monitor these nodes.</p> <p>Out of Service – Indicates a node is unavailable because it is out of service. NNMi does not update discovery information or monitor these nodes. This node is not updated in iSPI discovery information also. This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed.</p> <p>For more information, see the Help for NNMi, <i>View the Management Mode for an Object in Your Network</i>.</p>




Note : The Quick view is not available in this form.

Pseudowire VC Form: Status Tab

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

The status tab is useful for obtaining a quick summary of the SPI object status to better determine and monitor any significant patterns in behavior and activity.

Status Table

Attribute	Description
Status	<p>Overall status of the Pseudo Wires. Possible values are :</p> <p> Normal - Both the LSPs are Normal, Status is Normal</p> <p> Critical - Any one or both the LSPs are Critical,status is Critical.</p> <p> Unknown - Any one or both the LSPs are Unknown,status is Unknown.</p>




Attribute	Description
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.

PseudoWire VC Form: Conclusions Tab

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

The conclusions tab depicts the results of the overall derived status. This tab is useful for obtaining a quick-summary of the status and problem description for the PseudoWire VC.

Conclusions Table

Attribute	Description
Status	<p>Overall status of the PseudoWire VC. Possible values are :</p> <p> Normal - Both the LSPs are Normal, status is Normal.</p> <p> Critical - Any one or both the LSPs are Critical, status is Critical.</p> <p> Unknown - Any one or both the LSPs are Unknown, status is Unknown.</p>
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.
Conclusions	<p>The conclusions are set by the Causal Engine after the status calculation.</p> <p>The following conclusions that appears are listed below:</p> <ul style="list-style-type: none"> ● MplsPseudoWireVCDown - The status of the PseudoWire VC is Critical. ● MplsPseudoWireVCNormal - The status of the PseudoWire VC is Normal. ● MplsPseudoWireVCUnknown - The status of the PseudoWire VC is Unknown. <p>The PseudoWire VC down conclusion generates the incident to send the alert for the status.</p> <p>Example: MplsPseudoWireVCDown generates MplsPseudoWireVCDown incident</p>

PseudoWire VC Form: Incidents Tab

The PseudoWire VC form contains details about the selected PseudoWire VC.

This tab is useful for obtaining a quick summary of the incident and problem description for the PseudoWire VC.

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</i></p>

Attribute	Description
	<i>Form.</i>

PseudoWire VC Form: Registration Tab

The PseudoWire VC LSP tab provides the detailed information of the selected PseudoWire VC.

Registration Table




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

TE Tunnel Form

The TE Tunnel form provides the details of the selected TE tunnel. The TE Tunnel form displays the tunnel properties and identification attributes.

Basic Attributes

Attribute	Description
Name	<p>The name is assigned at the time of configuration of the TE tunnel by the network administrator and the same name is populated in the view.</p> <p>This name is not editable in the view.</p>
Head	<p>The head is the starting router from which the tunnel is configured. The head and name together make the unique identification for the tunnel. Multiple tunnels can originate from the same head router.</p> <p>If a head router is an unmanaged node or does not respond to SNMP at the time of discovery, no tunnels starting from that head are discovered.</p>
Tail	<p>The tail is the end router to which the tunnel is configured. The tail field is blank when the tail node is not discovered by NNMi.</p>
Description	<p>The description is the information given for the tunnel at the time of configuration.</p>
Management Mode	<p>Indicates whether the current node is being managed. This field also lets you specify whether a node is temporarily out of service.</p> <p>Possible values are:</p> <p>Managed – Indicates the node, interface or address is managed by NNMi.</p> <p>Not Managed – Indicates 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.</p>

Attribute	Description
	<p>Out of Service – Indicates a node is unavailable because it is out of service. NNMi does not update discovery information or monitor these nodes. This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed.</p> <p>For more information, refer the Help for NNMi, <i>View the Management Mode for an Object in Your Network</i>.</p>
Tail IP Address	The IP address on which the tunnel is configured. The Tail IP address is beneficial when the tail node is not discovered by NNM.
Head Interface	The interface of the head node where the tunnel is configured. Click the Head interface to get more details about the node.
Status	<p>Overall status of the TE Tunnel. Possible values are :</p> <p> Normal- The tunnel is Up, the status of the tunnel is Normal.</p> <p> Critical - The tunnel is Down, the status of the tunnel is Critical.</p> <p> Unknown- The tunnel is Unknown when the MIB stops reporting and no SNMP response from the node. This is only possible when the node is not managed or is not reachable at the time of polling.</p>
Bandwidth	<p>The bandwidth used by the particular tunnel.</p> <p>Note: The bandwidth value for tunnels is sometimes zero. This is due the fact that the router is reporting the zero value for the bandwidth even though the tunnel may be having non-zero bandwidth.</p>
Setup Priority	<p>The priority used to determine if this tunnel is eligible to be preempted.</p> <p>The value specifies the priority used when setting up the tunnel. A value of 0 specifies the highest priority and enables the tunnel to preempt all other tunnels except those with a holding priority of 0. A value of 7 specifies the lowest priority and does not enable the 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 specifies the highest priority and protects this tunnel from preemption by all other tunnels. A value of 7 specifies the lowest priority and allows all tunnels with a higher priority to preempt this tunnel.</p>
Create Time	The time when the TE tunnel is discovered and created in MPLS database.
Status Last Modified	The status of the TE tunnel is calculated whenever there is a change in topology. The Status Last Modified is the time when the status was last updated.

For more information for the tabs, refer [Attributes Tab](#), [Status Tab](#), [Conclusions Tab](#), [Incidents Tab](#), [Registration Tab](#).

TE Tunnel Form: Attributes Tab

The [TE Tunnel Form](#) contains details about the selected TE Tunnel.

The Attributes tab provides the TE Tunnel details listing the capabilities.

Supported Table




Attribute	Description
Record Route	<p>This flag indicates whether or not the signaling protocol should remember the tunnel path after it has been signaled. The status of the flag is either true or false.</p> <p>True is represented by <input checked="" type="checkbox"/>.</p>
FastReroute	<p>This flag indicates that any tunnel may choose to reroute the tunnel without making the status of the tunnel down. When a fault is detected on an adjacent downstream link or node, a midpoint router can reroute traffic for fast service restoration.</p> <p>The status of the flag is either true or false. If the tunnel is configured with the Fast-Reroute attribute, the value is true otherwise it is false. This is valid for both Cisco and Juniper routers. True is represented by <input checked="" type="checkbox"/>.</p> <p>This is valid for both Cisco and Juniper routers</p>
Merging Permitted	<p>This flag permits the routers to merge the session with other RSVP sessions for the purpose of reducing overhead. This helps in providing better network scalability. The status of the flag is either true or false. If the tunnel is configured with the Merging Permitted attribute, the value is true otherwise it is false.</p> <p>True is represented by <input checked="" type="checkbox"/>.</p> <p>This flag is valid for both Cisco and Juniper routers.</p>
isPersistent	<p>This flag indicates whether the tunnel should be restored automatically after a failure occurs. The status of the flag is either true or false.</p> <p>True is represented by <input checked="" type="checkbox"/>.</p> <p>This is valid for Cisco routers.</p>
isPinned	<p>This flag indicates that the tunnel is never rerouted and the path of the tunnel remains the same even when new resources are available. The status of the flag is either true or false.</p> <p>True is represented by <input checked="" type="checkbox"/>.</p> <p>This is valid for Cisco routers.</p>
isComputed	<p>This flag indicates whether the tunnel path is computed using a constraint-based routing algorithm.</p> <p>True is represented by <input checked="" type="checkbox"/>.</p> <p>The status of the flag is either true or false.</p>

TE Tunnel Form: Status Tab

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

The Status tab is useful for obtaining a quick summary of the SPI object status to better determine and monitor significant patterns in behavior and activity.




Status Table

Attribute	Description
Status	<p>Overall status of the TE Tunnel. Possible values are :</p> <p> Normal - If the tunnel is Up, the status of the tunnel is Normal.</p> <p> Critical - If the tunnel is Down, the status of the tunnel is Critical.</p> <p> Unknown - The MIB value reports the value of the node to unknown. Also, no SNMP response for the selected node. If the tunnel is configured on this node, the status of the tunnel is Unknown.</p>
Time Stamp	Current status is set by Causal Engine. The Time Stamp data is the time when the status of the TE Tunnel is last updated.

TE Tunnel Form: Conclusions Tab

The [TE Tunnel Form](#) contains details about the selected TE Tunnel.

The Conclusions tab provides the details about the results of the overall derived status. This tab is useful for obtaining a quick summary of the status and problem description for the TE Tunnel that results in TE Tunnel Status.

Attribute	Description
Status	<p>Overall status of the TE Tunnel. Possible values are :</p> <p> Normal - If the tunnel is Up, the status of the tunnel is Normal.</p> <p> Critical - If the tunnel is Down, the status of the tunnel is Critical.</p> <p> Unknown - The MIB value reports the value of the node to unknown. Also, no SNMP response for the selected node. If the tunnel is configured on this node, the status of the tunnel is Unknown.</p>
Time Stamp	Current status is set by Causal Engine. The Time Stamp data is the time when the status of the TE tunnel is last updated.
Conclusions	<p>The conclusions are set by the Causal Engine after the status calculation.</p> <p>The following conclusions that appears are listed below:</p> <ul style="list-style-type: none"> ● MplsTunnelDown - The status of the tunnel is Down. ● MplsTunnelUp - The status of the tunnel is back Up. ● MplsTunnelUnknown - The status of the tunnel is Unknown.

Attribute	Description
	The TE Tunnel down conclusion generates the incident. Example: MplsTunnelDown sends MplsTunnelDown incident

TE Tunnel Form: Incidents Tab

The [TE Tunnel Form](#) contains details about the selected TE Tunnel.

This tab is useful for obtaining a quick summary of the problem description for the TE Tunnel.

Incidents Table

Attributes	Description
Incidents Attributes	The attributes listed in the incidents tab are same as available in NNMi Incidents form. For more information for the attributes, refer the Help for <i>NNMi Incidents Form</i> .

TE Tunnel Form: Registration Tab

The [TE Tunnel Form](#) contains details about the selected TE Tunnel.

Registration

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



Node Form: VRF Tab

The NNMi Node form contains details about the selected node. The selected node is MPLS enabled and is participating as VRF to form a VPN.

Attributes

Attribute	Description
VRF	Table view of all of the VRFs associated with the current node. Use this table to determine all VRFs in which this node participates. See the VRF Form for more information about a specific VRF.

Following features are available in the tab:

- Access the forms for detailed information: Click the  Open icon to view the detailed information about a specific node.
- Quick View information: To know more about the selected object attributes, click  Quick view icon.

- Filter option in the view: You can filter some of the columns in the table view to categorize and view the relevant information. The filters configured on the views are restored when the views are opened again. This is very useful as you do not have to configure the filtering option again. Right-click the column name to select the columns for filtering.
- Sorting option in the view: You can sort the column in ascending or descending order. Sorting is enabled only for limited columns.

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



Node Form: TE Tunnel Tab

The NNMi Node form contains details about the selected node. The selected node is MPLS enabled and TE Tunnel is configured in the node.

Attributes

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

Following features are available in the tab:

- Access the forms for detailed information: Click the  Open icon to view the detailed information about a specific node.
- Quick View information: To know more about the selected object attributes, click  Quick view icon.
- Filter option in the view: You can filter the **Status and Name** column in the table view to categorize and view the relevant information. The filters configured on the views are restored when the views are opened again. This is very useful as you do not have to configure the filtering option again. Right-click the column name to select the columns for filtering.
- Sorting option in the view: You can sort the column in ascending or descending order. Sorting is enabled only for limited columns.

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

Node Form: PseudoWire VC LSP Tab


The NNMi Node form contains details about the selected node. The selected node is MPLS enabled and PseudoWire VC LSPs are configured in the node.

Attributes

Attribute	Description
PseudonoWire VC LSP	Table view of all of the PseudoWire VC LSPs starting from the current node. Use this table to determine all PseudoWire VC in which this node participates. For more details, see the PseudoWire VC Form

Following features are available in the tab:

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

- Access the forms for detailed information: Click the  Open icon to view the detailed information about a specific node.
- Filter option in the view: You can filter the **Status and Id** column in the table view to categorize and view the relevant information . The filters configured on the views are restored when the views are opened again. This is very useful as you do not have to configure the filtering option again. Right-click the column name to select the columns for filtering.
- Sorting option in the view: You can sort the column in ascending or descending order. Sorting is enabled only for limited columns.

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

Introduction to iSPI for MPLS Administrator

As an iSPI administrator, you can perform the following tasks.

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

Tasks	Description
Polling Configuration	Using the Polling Configuration UI, configure the polling intervals. See MPLS Polling Configuration for more information.

Manage and Unmanage Nodes

You can manage and unmanage nodes by performing the specific tasks from the NNMi inventory views. For more information on how to perform the actions, see *Actions provided by NNMi*.

You cannot specifically manage or unmanage the MPLS objects because the management mode attribute for any MPLS node is inherited from NNMi. If a node is unmanaged, all the MPLS SPI objects such as TE Tunnels, VRFs, VC LSPs are in unmanaged state but the derived objects such as VPN or PseudoWire VC does not have the settings.

The iSPI for MPLS discovery process does not discover any unmanaged nodes. However, if a unmanaged node is changed into a managed mode, discovery process starts and updates the management mode of the SPI objects. Also, a notification is sent to the State Poller about the updated management mode so the state of the iSPI object is set to *Not Polled* and the status is set to *No Status*.

Backup and Restore Actions

You can perform Backup and Restore actions for iSPI for MPLS from NNMi. The backup and restore command for NNMi does the backup and restore for iSPI for MPLS. This is supported only with the embedded database and when iSPI for MPLS and NNMi are located in same management station..

You can check the MPLS file in the location provided for backup and with the extension .pgd.

Example: *C:\tmp\nnm-bak-20080924095922-mplsdb.pgd*.

To perform Back up and Restore operation, see *Back Up and Restore NNMi*.

Configuration Poll

After changing the community string, perform the Configuration poll command. For more information, see *Actions: Configuration Poll command*.

Sign- On to MPLS Configuration

After installing NNMi, use the URL to sign in to the NNMi console. For details on how to sign-in for NNMi, see *Configure Sign-In Access*.

To access the MPLS Configuration UI, no additional login and password is required if your user role defines you to access the NNMi configuration workspace. To know more about the user roles, see *Help for NNMi, Determine Account Roles*.

Single Sign- On (SSO) for MPLS Configuration UI

- Open the URL with Fully Qualified Name (FQDN), and login in as non system admin privileged user. When you access the MPLS Configuration UI ,no username or password is required to view the UI.

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

- Open the URL with hostname/localhost and SSO should work when you login as non system admin privileged user. Follow the steps for SSO to work:
1. From the **User Configuration Interface**, click the **Enable URL Re-direct** checkbox and save the settings.
 2. Login again and check the localhost/hostname automatically displays the FQDN in the URL. The MPLS Configuration UI opens and no need to type the username and password again.
- If you are using the system as username to login, SSO is disabled. You have to type the username/password again to view the MPLS Configuration UI.

At the time of NNMi installation, note down the NNMi port, username and password . Enter the same configuration details while doing the iSPI for MPLS installation. After the installation, if you want to update the password, use the following command.

Updating the NNMi System Password

The iSPI should be configured to use same system password as NNMi. After installation of iSPI, if the system password for NNMi is modified, the iSPI for MPLS should be updated with the new system password.

Run the following command to copy the NNMi password:

```
encryptmplspasswd.ovpl -c <domain>
```

where:

c - NNMi jboss to iSPI jboss communication

domain - mpls(case insensitive)

After updating the password, restart the iSPI for MPLS to use the new system credentials. If the password is not updated the ovstop, ovstart, and ovstatus commands fails.

Updating the iSPI (NNMi WebService Password)

The iSPI should be configured with Webservice Username / Password to communicate with NNMi. The user should be added in NNMi with the role of WebService Admin or System and then use the script to update the password.

Note: Avoid System role for NNMi - iSPI communication. Only user having root permission can run this script.

You can use the `encryptmplspasswd.ovpl` script to update the iSPI password. This script changes the iSPI password. Avoid using the System password of NNMi.

```
encryptmplspasswd.ovpl -e <domain> <password>
```

where: -e - encrypt supplied string

domain - mpls (case insensitive)

password - string to be encrypted

After updating the password, restart the iSPI to use the new system credentials. If the password is not updated, ovstop, ovstart and ovstatus commands will fail.

MPLS Process and Services

The iSPI for MPLS includes a group of processes and services. For information about each process or service, see the following:

- [About the iSPI for MPLS Process](#)
- [About the iSPI for MPLS Services](#)

To verify if MPLS processes and services are running properly, you can use the status command:

[Verify that iSPI for MPLS Processes Are Running](#)

About MPLS Process

iSPI for MPLS Process

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

Note: The iSPI for MPLS doesn't show the status of the Oracle database. Also, the iSPI doesn't check if Oracle database is running in the NNMi management station. If the Oracle Database is configured, Database Administrator has to start the database.

Verify that MPLS Processes Are Running

After you install iSPI for MPLS, a group of processes are running on the server.

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

For the basic status, type: **ovstatus -c mplsjoboss**

For the detailed status, type: **ovstatus -v mplsjoboss**

Review the list of processes to ensure that all are running. For more information about each process, see [About MPLS Process](#).

Start or Stop MPLS Processes

You can stop and start NNMi processes from the command line.

Commands to start or stop MPLS process:

You can start and stop the MPLS process from the command line.

- To start the MPLS processes, type: **ovstart -c mplsjoboss**.

This command starts the MPLS processes and also checks whether the NNMi processes(ovjboss, nmsdbmgr) are running or not.

- To stop the MPLS processes, type: **ovstop -c mplsjoboss**.

This command stops the MPLS processes and not the NNMi processes(ovjboss, nmsdbmgr).

To generate the list of processes, [Verify that MPLS Processes Are Running](#)

Start and Stop MPLS Services

You can stop or start all NNMi services at the same time. You cannot start and stop individual services.

To start or stop MPLS services:

At the command line, type the command:

- **ovstart -c mplsjoboss**
- **ovstop -c mplsjoboss**

Verify that MPLS Services are Running

After you install MPLS, a group of services are running on the server.

MPLS Services run inside the mplsjoboss process. The mplsjoboss process controls the jboss Application Server that contains all the MPLS services.

You can verify that all MPLS services are running in any one of the following ways:

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

Log files for the MPLS Services

Log files are found in the following location:

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

Start and Stop MPLS Services

You can stop or start all NNMi services at the same time. You cannot start and stop individual services.

To start or stop MPLS services:

At the command line, type the command:

- **ovstart -c mplsjoboss**
- **ovstop -c mplsjoboss**

Configuring MPLS Incidents

The iSPI for MPLS generates incidents if any fault or change is detected in the network. This helps the in fault management and reduces the Mean Time to Repair (MTTR).

Incidents are information that iSPI considers important for you to check your network.

The incidents generated for iSPI objects are of the following types:

- Incidents generated by the iSPI for MPLS
- Traps generated from SNMP

The iSPI for MPLS generates MPLS incidents whenever the State Poller detects behavioral changes in the network. After the incidents are generated, check the inventory views for the updated status.

Event Name Provided by MPLS

MPLS Incident Configuration Name	Description
MplsTETunnelDown	Generated when the MPLS state poller detects the TE Tunnel is Down. This incidents belong to MPLS Traffic Engineering family.
MplsVRFDOWN	Generated when the MPLS State Poller detects that the VRF is Down. The VRF status results in the VPN status calculation. This incidents belong to MPLS L3 VPN family.
MplsPseudoWireVCDown	Generated when the MPLS State Poller detects that the PseudoWire VC is Down. This incidents belong to MPLS PseudoWire VC family.

Types of SNMP traps for MPLS

SNMP traps for MPLS are generated from the MPLS enabled devices.

SNMP Traps Configurations provided by MPLS enabled devices

MPLS Traps Name	Description
CiscoMplsTETunnelUp	Generated when the configured tunnel is back Up.
CiscoMplsTETunnelDown	Generated when the configured tunnel is Down.
CiscoMplsTETunnelRerouted	Generated when the configured tunnel is Rerouted.
CiscoMplsVRFUp	Generated when the VRF interface is back Up.
CiscoMplsVRFDOWN	Generated when the VRF interface is Down.
MplsPseudoWireVCUp	Generated when the configured PseudoWire VC is back Up.

MPLS Traps Name	Description
MplsPseudoWireVCDwn	Generated when the configured PseudoWire VC is Down.

SNMP Traps related to Cisco IOS-XR devices:

- CiscoMplsL3VpnVrfUp
- CiscoMplsL3VpnVrfDown
- CiscoIOSXRMplsTETunnelUp
- CiscoIOSXRMplsTETunnelDown
- CiscoIOSXRMplsTETunnelRerouted

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

Launching the Incidents View

You can launch the MPLS incidents in the following ways:

- Click the **NNM Incident Browsing** workspace to view the incidents. To view the details, open the iSPI for MPLS forms from the incidents view.
- Access the details for the incidents from Incident tabs in all the forms

Discovering your MPLS Network

The iSPI for MPLS discovery process determines the routers which are MPLS enabled. The discovery starts for all the MPLS enabled nodes to determine the routers configured with Virtual Private Network (VPN), or TE tunnel or PseudoWire VCs. Whenever there are changes in the topology, the discovery process for MPLS fetches the details of the changed topology and populates in the respective views. The discovery process collects the data and you can view the updated information in MPLS views.

The iSPI for MPLS discovery is scheduled in conjunction with NNMi discovery process. By default, you should start the discovery process after the installation of the iSPI of MPLS. The scheduled discovery time is every 24 hours.

The MPLS discovery process is categorized in two portions :

- Automatic Discovery
- On- Request Discovery

Automatic Discovery

The discovery process automatically starts after you add, or delete a node or perform the configuration poll action in the NNMi network. When a node is added in the topology, NNMi discovery process detects the

change in network and start the process. You can start the discovery from the configuration poll. If the node is MPLS enabled node, MPLS discovery process also starts. When a node is deleted, the NNMi discovery process detects the interfaces and deletes the corresponding dependencies for the deleted node in all the views.

Automatic discovery will not discover the nodes which are already discovered by NNMi. You have to wait for next discovery cycle or use command line tool to start complete discovery.

On Request Discovery

You can start the discovery process for iSPI for MPLS in the following ways:

- Start the MPLS discovery process after the installation of iSPI for MPLS.
- Start the discovery process by using configuration poll command.

Command line for MPLS Complete Discovery

Use the following command to do the complete MPLS discovery:

nmsmplsdisco.ovpl -all

You can use command line to discover the MPLS nodes added after the scheduled NNMi discovery.

Discovery of the iSPI for MPLS objects when NNMi is already installed and running in a management server:

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

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

nmsmplsdisco.ovpl [-all | -node <node_name>]

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

For more information for the discovery process, see the following:

- [Discovery of the configured VPNs](#)
- [Discovery of the configured TE Tunnels](#)
- [Discovery of the configured PseudoWires VC](#)

Discovering Your L3 VPN Network

The iSPI for MPLS discovery process determines which routers in the NNMi topology supports Virtual Private Networks(VPN).

About VPN, VRF

A VPN is formed by one or more Virtual Routing and Forwarding(VRFs) table. A VPN in an MPLS network is defined by the presence of a VRF on an edge router in the customer network.

The virtual routing and forwarding tables exist on the Provider Edge (PE) routers only. The VRFs contain the Route Targets (RT)s. Each VRF table includes a list of import and export route targets that identify VRFs in the network. The iSPI for MPLS reads the route targets from the import and export lists to identify the VRF neighbors. The VRF tables determine the routes through the VPN network.

The VRF-VRF neighboring relationship is defined when one of the VRFs export a route target and the same is imported by another VRF. Thus, both the VRFs are grouped into a VPN based on neighboring relationships. If VRF1 and VRF2 are grouped in one VPN based on the neighboring relationship and VRF2 and VRF3 have also grouped, then all the VRFs (1,2,3) together form a VPN.

Discovery of VPNs

The iSPI for MPLS performs SNMP queries on the router devices to determine the provider edge (PE) router configuration and virtual route forwarding (VRF) groupings. VRFs that can be linked directly or indirectly by their neighbor relationships are considered to be in the same VPN. This approach lets the iSPI correctly discover simple network topologies that are fully meshed as well as complex network topologies that are formed from a hub and spoke topology.

At the time of VPN discovery, when the node is discovered or rediscovered, the information for all the VRFs is observed. You can find the following categories of VPN:

- **Full Mesh VPN** - Full Mesh VPN is formed if all the VRFs have the same RT. The same RT is used for importing and exporting in all the VRFs in the specific group. Each VRF exports its route targets to all VRFs in the VPN and imports all route targets from the other VRFs in the VPN. All the PE routers are communicating with each other.
- **Other** - All the VRFs are not communicating with all other VRFs belonging to a VPN. For example, hub and spoke, hybrid topology.
- **Isolated** - A VRF forming a single VPN (no other VRF imports the route targets of this VRF).

You can include or ignore the RTs from the Polling Configuration UI. Adding, deleting, and ignoring the RTs results in merging and splitting of the VPNs.

If a new RT is added, deleted or ignored, iSPI for MPLS identifies the VRFs which will be impacted after this configuration. Also, checks whether it is forming a new VPN, or splitting or merging the existing VPNs. This action starts the discovery process for the updated VRFs and also starts the VPN recalculation. The updated data is populated in the L3 VPN view.

The discovery process is incremental and continues till the topology is stable. Every time a node is added or deleted, discovery starts and retrieves the respective VPN, VRF, and RT information.

Discovering Your MPLS TE Tunnel Network

The iSPI for MPLS discovery process determines which routers are configured with Traffic Engineering (TE) tunnels in the NNMI topology. The discovery process is dynamic and starts whenever there is a change in topology.

The iSPI for MPLS performs the SNMP queries on the devices to determine the router configuration and tunnel groupings.

Discovery of the TE Tunnel

After determining the MPLS enabled routers, MPLS discovery process starts determining the TE tunnels configured in the node. The discovery of a TE tunnel is done through SNMP queries on the tunnel's head(source) router. After discovery, the TE tunnel information is available in MPLS TE Tunnel view.

The discovery process is incremental and continues till the topology is stable. Every time you add or delete a node,,discovery process starts and retrieves the TE tunnel information.

Discovering Your MPLS PseudoWire VC Network

The iSPI for MPLS discovery process determines which routers are configured with PseudoWire VCs in the NNMi topology. The discovery process is dynamic and starts whenever there is a change in topology.

The iSPI for MPLS performs the SNMP queries on the router devices to determine the router configurations.

Discovery of the PseudoWire VC

After determining the MPLS enabled routers, MPLS discovery process starts determining the PseudoWire VC configured in the MPLS nodes. The discovery of PseudoWire VC is done through SNMP queries on the router. After discovery, the PseudoWire VC information is available in MPLS PseudoWire VC view.

The discovery process is incremental and continues till the topology is stable. Every time you add or delete a node, discovery process starts and retrieves the information.

Monitoring MPLS Network Health

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

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

To know more about how the MPLS network is monitored, refer the [MPLS Sate Poller](#) and [Causal Engine](#) topics.

In addition, see the *NNMi State Poller and Causal Engine* .

About MPLS State Poller

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

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

The default value of the State Poller is 5 minutes.

You can change the polling duration from the **Polling Configuration UI**.

Using MPLS Causal Engine

Causal Engine gathers information from the State Poller, scheduled discovery, SNMP traps, and incidents. Causal Engine collects information to calculate the *Status* of the devices, TE tunnels, VRFs, and VPN. Thus, Causal Engine helps in monitoring the health of the network.

Causal Engine updates the Status attributes in the respective views and forms. Causal Engine calculates Status for the following objects:

- VPN status
- VRF status
- TE Tunnel status
- PseudoWire VC status

The health status is dynamic.

See the *NNMi Causal Engine and Monitoring* for further details.

On-Demand Status Poll

The status poll command launches a real-time check of the state of the specified device. If the state has changed since the last monitoring cycle, iSPI for MPLS calculates an updated status reading for the

selected device.

You can initiate 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 explicitly the iSPI information but the starts the discovery process for MPLS enabled nodes.

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

Troubleshooting Guidelines

The following information helps you to resolve common problems and provides troubleshooting tips for easy usage and navigation.

User Interface

The following information helps you to troubleshoot some of the tasks required for MPLS views.

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

- Verify the node is configured, managed and discovered in NNMi topology. Start the Configuration poll for that node.

Note: The configuration poll starts the poll for NNMi nodes. This poll display does not explicitly contain the iSPI information but starts the process for MPLS enabled nodes also.

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

- Perform the Demand Poll for the nodes. See *NNMi Help for Demand poll*.

Note : The demand poll starts the status poll for NNMi nodes. This poll does not explicitly contain the iSPI information but starts the Status polling process for MPLS enabled nodes.

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

- Delete the node in NNMi. This action deletes the corresponding iSPI objects. Now you can start again by adding the node in the topology.

PseudoWire VC is having only one VC LSP.

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

- Ensure that the other VC LSP of the PseudoWire VC is configured in NNMi with proper community strings. Also, the other VC LSP should be discovered.

TE Tunnel is not having the name of the router for tail.

- Ensure that the tail of the TE Tunnel is configured in NNMi with proper community strings.

Not able to view the iSPI objects in the MPLS views. Not able to view the NNMi nodes also. Wants to re-start the processes, configurations.

- Reset the Database. This should be used 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 forming the VPNs seems to be inaccurate.

- VPN discovery is based on the Route targets. If you have Management-VPNs, Extranets, the corresponding Route Targets are used in VPN formation. To avoid any discrepancy in formation of VPNs, it is important that you ignore the specific RTs from the configuration UI which you want not to participate in the VPN formation.

VPNs are not having relevant names.

- The system generated VPN names are based on the by the internal rule. You can change the name as per your requirement. For more details, see [VPN Naming Procedure](#).

Discovery Process

The following information helps you to troubleshoot the MPLS discovery process.

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 Pseudowire VC LSPs does not get associated with the PseudoWire VC. You have to wait for sometime for PseudoWire VC to be discovered and then start the configuration poll for the node.

Note : The configuration poll starts the polling process for the NNMi nodes. This poll display does not contain explicitly the iSPI information but the starts the discovery process for MPLS enabled nodes.

After Config /Demand poll, you do not get iSPI specific information.

- Limitation in this version of the product. Though the configuration and demand poll starts the iSPI related action but does not display in iSPI for MPLS, 8.10.

You performed various configuration actions on a node (for example: Updated community strings, ...). But, iSPI still shows the old data in the views.

- Wait till the next discovery cycle. However, you can start by performing Configuration poll on the node.

Note : The configuration poll starts the polling process for the NNMi nodes. This poll display does not contain explicitly the iSPI information but the starts the discovery process for MPLS enabled nodes.

Incidents

The following information helps you to know more about the MPLS incidents.

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

- Not all the source objects are a part of VC LSP, TE Tunnels or VRF.

After the traps are generated, polling does not start.

- Status and incidents are updated and generated after polling. For this release, polling will not start after the traps are generated by the devices.

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.

Others

The following section contains some general troubleshooting tips and workarounds:

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

- Update using the NNMi SNMP Configuration. See *Help for NNMi, SNMP Configuration*.
- Start the Configuration Poll.

The configuration poll starts the poll for the NNMi nodes. This poll display does not contain the iSPI information but it starts the discovery process for MPLS enabled nodes.

Update the polling intervals.

- Update the Polling Configuration UI. Configuration UI is only available if you login with Admin privileges.

Not able to view Configuration UI.

- Administrative privileges are needed to view the Configuration UI.

MPLS Polling Configuration

The iSPI for MPLS provides you the default polling interval to monitor the near real time status of the iSPI objects. You may choose to modify the polling configurations provided by iSPI. The following table provides the polling configuration information:

Type of Configuration	Description
TE 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 seconds between the two consecutive polls for VRF. The default value is 5 minutes.
PseudoWire VC Frequency	Interval specified in minutes and seconds between the two consecutive polls done by the Poller. The default value is 5 minutes.
Exclude Route Targets	<p>Specified Route Targets are ignored at the time of discovery. You can enter the list of Route targets to be ignored.</p> <p>Click Add to include the list in the Route target field. To update the database so that the specified list of Route Targets are ignored in the discovery process, click Save.</p> <p>Click Remove, to deselect any one Route target. To update the database so that the specified list of Route Targets are ignored in the discovery process, click Save.</p> <p>Click Select All to select all the Route targets to perform the action(Add and Remove).</p> <p>This action starts the VPN recalculation.</p>

Launching the Configuration UI

(From the Left navigation panel, select the Configuration Workspace and click <MPLS Configuration> view (for example, **Configuration - > MPLS Configuration**).

Note: The Configuration UI is supported only with Microsoft IE 7. You can only view (Read Only mode) but not perform any tasks such as Exclude Route Targets or polling interval if you are using any browser other than Microsoft IE 7.

Index

A		D	
About		Discovery process	
Grouping for VPN	10	L3 VPN	45
Route Targets	10	MPLS	44
VPN	10	PseudoWire VC	47
VPN Naming	11	TE Tunnel	46
VPN Topology	10	F	
VRFs	10	FastReroute	34
Attributes		Features	
TE Tunnel Form	32	iSPI for MPLS	8
VPN Form	20	L3 VPN	9
VRF form	24	PseudoWire VC	13
Attributes tab		TE Tunnel	12
TE Tunnel form	34	Form	
Automatic Discovery	44	PseudoWire VC	28
B		TE Tunnel	32
Backup and Restore	39	VPN	20
C		VRF	24
command		Full Mesh VPN	46
MPLS process status	41	I	
Command line		Incidents tab	
change the password	40	TE Tunnel form	36
complete discovery	45	VRF form	28
Conclusions tab		Incidents Tab	
TE Tunnel form	35	PseudoWire VC form	31
VPN form	23	Interfaces tab	
VRF form	27	VRF form	25
Conclusions Tab		Introducing	
PseudoWire VC form	31	L3 VPN	9
Configuration Poll	39	MPLS Inventory	14
		PseudoWireVC	13
		TE Tunnel	12
		Introduction	
		Accessing Forms	19
		MPLS Administrator	39

Inventory		P	
L3 VPN	15	Polling Configuration	52
LSR View	17	Polling Frequency	52
PseudoWire VC	18	PseudoWire VC	13
Inventory;TE Tunnel	16	R	
isComputed	34	Record Route	34
Isolated	46	Registration tab	
isPersistent	34	TE Tunnel form	36
isPinned	34	VPN form	24, 28
L		Registration Tab	
Launch		PseudoWire VC form	32
Forms	20	Route Target tab	
MPLS Inventory	14	VRF form	26
Log files		S	
MPLS Services	42	Single Sign-On	39
M		Status tab	
Manage nodes	39	PseudoWire VC form	30
Merging Permitted	34	TE Tunnel form	35
Monitoring		VPN form	22
Causal Engine	48	VRF form	26
overview	47	T	
State Poller	48	Tab	
MPLS forms		Node Form-PseudoWire VC LSP	37
Overview	19	Node Form-TE Tunnel	37
MPLS Incidents	43	TE Tunnels	12
MPLS process		troubleshooting	49
Stop	41	U	
MPLS Process	41	Unmanage nodes	39
start	41	Using iSPI for MPLS	9
MPLS Services	42	V	
N		VC LSP Tab	
Neighbors tab	26	PseudoWire VC form	29
O		VRF-VRF neighboring	46
On Request Discovery	45	VRF tab	
Other	46	VPN form	21