CA Spectrum® MPLS-VPN Manager

User Guide

Release 9.4

ca technologies

CA Technologies Product References

This document references the following CA Technologies products:

- CA Spectrum® (CA Spectrum)
- CA Spectrum® Report Manager (Report Manager)
- CA Spectrum® IP Routing Manager
- CA Spectrum® Service Performance Manager (SPM)
- CA Spectrum® Network Configuration Manager (NCM)
- CA Business Intelligence (CABI)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction

This section contains the following topics:

Overview

MPLS VPN Manager lets you discover, model, and monitor Virtual Private Networks (VPNs) within the network environment. MPLS VPN Manager provides VPN and Site discovery and modeling, VPN connectivity status, SNMP trap handling, monitoring of Virtual Routing and Forwarding (VRF) conditions, and performs calculation of and alarming on VPN conditions. MPLS VPN Manager is a distributed application.

MPLS VPN Manager discovers all of the Provider Edge (PE) routers and interfaces that are forwarding traffic for a particular VPN. Based on this discovery, CA Spectrum creates VPN models representing each unique VPN. These VPN models can then be polled for their current operational status (Up or Down).

In addition, MPLS VPN Manager supports VRF Ping and VRF Path Tracing, which enables you to monitor the status of the paths between the sites in each of the modeled VPNs. You can configure threshold alarms to alert you when path changes exceed the configured tolerance.

MPLS VPN Manager provides searches that let you quickly find a particular VPN or all VPNs.The Search results contain a list of the current VPNs configured within the environment and their current status. You can drill into a single VPN to see the current list of PE interfaces participating within that VPN and the current status of the VPN.

VPN Topologies Supported

The common topologies for MPLS Layer 3 VPNs include Full Mesh, Hub and Spoke, and Overlapping VPNs. MPLS VPN Manager supports the following two topologies:

- **Full Mesh**—The service provider provisions the service so that all customer sites communicate directly with each other. Customer sites are members of the same single VPN. This topology is the most common VPN topologies, and it is generally used by enterprise customers to establish their corporate intranet.
- **Overlapping VPNs**—Sites can be members of multiple VPNs. Scenarios requiring sites with multiple memberships include the following:
  - Establishing a management VPN to customer edge devices
  - Establishing a shared service across VPNs
  - Implementing an extranet-based service

Overlapping VPN Considerations and Limitations

For overlapping VPN topologies, consider the following notes and limitations when using MPLS VPN Manager:

- Configurations based on route-map statements are not reflected in the mplsVpnVrfRouteTargetTable. CA Spectrum does not discover or model these configurations.
- The scale of Service Assurance tests in overlapping VPNs becomes more critical because of the greater possibility that connectivity spans multiple VPNs. We recommended enabling Service Assurance tests incrementally to evaluate the performance and resource impacts.
- VPN Sites impact the health of all VPNs in which it has membership. A single VPN Site outage can cause the generation of several alarms (that is, one alarm for each VPN in which the VPN Site has membership). CA Spectrum does not correlate (that is, suppress) the alarms. Areas affected include:
  - VPN condition calculation
  - VRF test results
  - Aggregate VPN performance (bandwidth usage added to each VPN)
- There is no mechanism to detect when new Route Targets are added, removed, or modified in existing VPNs. There is no background discovery mechanism, and this information is not captured by traps.
- When VPN Sites read some of their configuration from their parent VPN, unexpected behavior can occur when VPN Sites are in multiple VPNs. Configure VPNs similarly for the following options:
  - Enable VRF ping and trace
  - Enable site alarms
  - Model security

MIB Support and Device Compatibility

The MPLS VPN Manager currently supports the IETF draft MPLS/BGP VPN MIB (draft-ietf-ppvpn-mpls-vpn-mib-05) and Cisco's MPLS Virtual Private Networks MIB (MPLS-VPN-MIB). Cisco's MPLS-VPN-MIB is based on Draft 3 of the IETF draft MPLS/BGP VPN MIB.

These MIBs provide access to the following configuration information for VPNs configured on PE router interfaces:

- Virtual Routing/Forwarding (VRF) Instance Table (mplsVpnVrf) - Contains the VPN name and the Route Descriptors (RD) for each VRF.
- VPN Interface Configuration Table (mplsVpnInterfaceConf) - Associates entries in the ifTable with a VRF.

MPLS VPN Manager uses the following MIBs to support the VRF Ping and the VRF Trace functionality:

- Cisco- RTTMON MIB
- Juniper- RFC2925, Juniper Ping MIB, and Juniper Traceroute MIB

MPLS VPN Manager also supports the following tables in the Juniper Enterprise VPN MIB:

- Table of Configured VPNs (jnxVpnTable)
- Table of VPN Interfaces (jnxVpnIfTable)

In addition, MPLS VPN Manager provides partial support for the Draft 4 of the IETF MPLS/BGP VPN MIB.

MPLS VPN Manager functionality is supported by Cisco GSR 12000 and 7500 Series routers running Cisco IOS 12.2(15) T8 or higher in networks with properly configured MPLS VPNs. Juniper support is for JunOS 6.1 or later.

Chapter 2: MPLS VPN Manager Interface

This section contains the following topics:

Open MPLS VPN Manager

To view the VPNs modeled in your networking environment, open MPLS VPN Manager in OneClick.

To open MPLS VPN Manager in OneClick

1. Open OneClick.
2. Click the VPN Manager node on the Explorer tab in the Navigation panel.

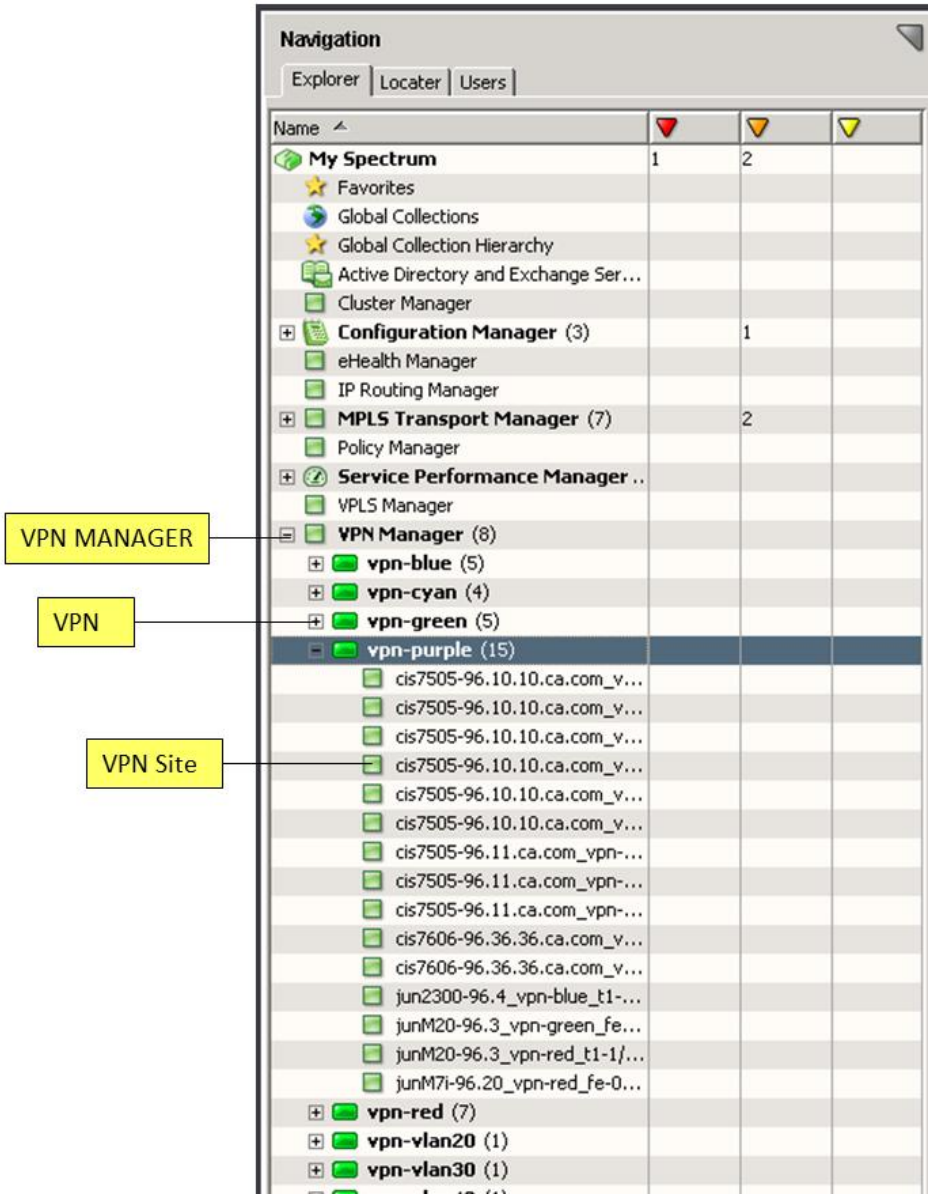
   MPLS VPN Manager opens, and the Contents panel populates with information about the selected VPN Manager.

MPLS VPN Manager Hierarchy

MPLS VPN Manager can be directly accessed from the Explorer tab of the Navigation panel. Expanding the VPN Manager node displays all of the VPNs managed by the MPLS VPN Manager. Expanding each VPN displays the VPN Sites contained in the VPN.

Note: Each VPN Site displays under the VPN in which it has membership. In an overlapping VPN topology, a specific VPN Site may show up under multiple VPNs.

The following graphic is an example of the MPLS VPN Manager hierarchy in the Navigation panel:



Note: You can no longer view Devices listed under VPN Site models in the VPN Manager Explorer view.

The Contents panel displays the Alarm list for the modeled element that you have selected in the Navigation panel. The Component Detail panel displays the Alarm details for the Alarm selected in the Alarm list shown in the Contents panel. If the Alarm list is empty, the Component Detail panel displays the Information view for the modeled element selected in the Navigation panel.

Using VPN Search options in Locater Tab

The Locater tab includes specific predefined searches for VPNs. These searches support cross-server device modeling.

The Locater tab in the Navigation panel includes the following searches:

VPN

All Route Targets

Locates all Route Targets that are modeled in the CA spectrum database for the selected landscape (Main Location Server, by default) through their Route Target information.

All Sites

Locates All Sites that are modeled in the CA spectrum database for the selected Landscape.

All VPN Managers

Locates all VPN Managers in a list of landscapes that you select for the search in a distributed implementation.

Note: There can never be more than one VPN manager per landscape.

All VPNs

Locates all VPN models in a list of landscapes that you select for the search.

By default, the VPN models are created in the Main Location Server (MLS). If you exclude the MLS from the list of landscapes in the search, no results will be displayed.

Site By

Locates specific sites that meet the search criteria for the following search types:

Interface

Locates and lists all VPN Sites modeled in the CA Spectrum database based on their interface

Name

Locates all VPN Sites modeled in the CA Spectrum database based on site names

PE Router IP

Locates and lists all VPN Sites modeled in the CA Spectrum database based on the specific IP addresses of the PE Router which you specify in the Search> Site By dialog box.

PE Router Name

Locates and lists all VPN Sites modeled in the CA Spectrum database based on the specific PE Router Name which you specify in the Search> Site By dialog box.

VPN Model Names

Locates and lists all VPN Sites modeled in the CA Spectrum database based on the specific Model Name(s) which you specify in the Search> Site By dialog box.

If you wish to list the sites present in multiple VPNs, enter the relevant VPN model names (as comma separated values) in the Search > Site By Dialog box.

VPN By

Locates specific sites that meet the search criteria for the following search types:

Exported Route Target

Locates and lists VPNs based on their Exported Route Target information

Imported Route Target

Locates and lists VPNs based on their Imported Route Target information

Interface

Locates and lists VPNs based on their Interface information

Name

Locates and lists VPNs based on their VPN Names.

PE Router Name

Locates and lists VPNs based on their PE Router Name

Site Model Names

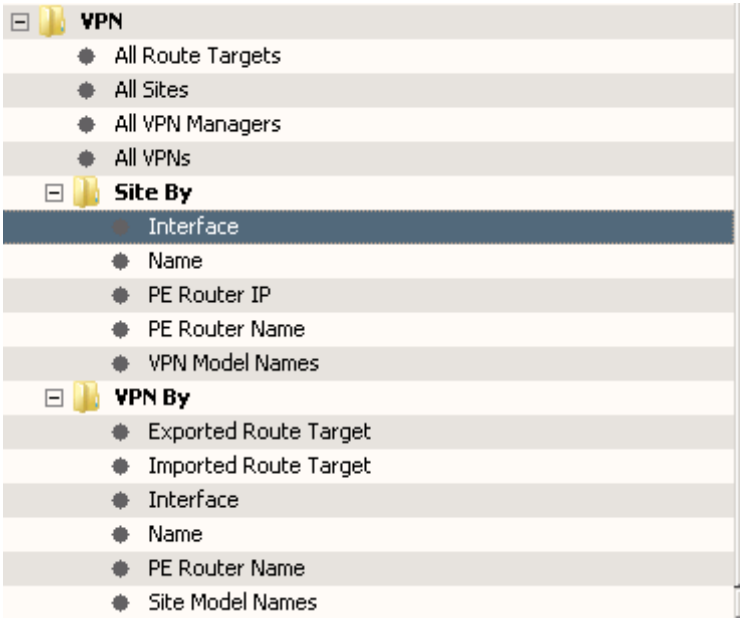
Locates and lists VPNs based on their Site Model Names. A list of common VPNs where there is an intersection of more than one site is displayed.

If you wish to list the common VPNs with overlapping sites, enter the relevant Site model names (as comma separated values) in the Search > Site By Dialog box.

Follow these steps, to search your MPLS VPN Manager environment:

1. Open OneClick.
2. Click the Locater tab in the Navigation panel.

   The search options are grouped under the VPN folder on the Locater tab, as shown:



3. Expand the VPN node and double-click the type of search you want to conduct.

   A relevant Search dialog opens, based on the parameter selected in a list of landscapes that you select for the search.

4. Follow these steps in the Search dialog box:

   - For a specific query, enter relevant values in the text box for the search option selected
   - For multiple searches, click List... and Follow these steps: in the List of Values dialog:
     - Click Import to import a list
     - Enter a list of values

5. Click OK.

   The search results appear in the Contents panel.

More information:

VPN Manager Configuration (see page 28)
Configure VRF Ping Source and Destination (see page 40)
Configuring VPN Condition Alarms (see page 36)
Configure VRF Path Trace Source and Destination (see page 38)

Chapter 3: Discovery and Modeling

To manage the VPNs on your network, you must run VPN Discovery before you can use MPLS VPN Manager. VPN Discovery discovers each VPN and VPN Site currently configured on devices modeled in CA Spectrum.

This section contains the following topics:

Discovery Prerequisites

For VPN Discovery to complete successfully, devices must meet the following prerequisites:

- VPN devices must support the correct MPLS-VPN MIBs.
- You must model the physical components of your network in CA Spectrum before using the VPN Discovery functionality. You can model the physical components using one of these methods: Discovery, manual modeling, or the Modeling Gateway.

  Note: For instructions about using these mechanisms to model your network, see the *Modeling and Managing Your IT Infrastructure Administrator Guide* and the *Modeling Gateway Toolkit Guide.*
- The devices must have MPLS-VPN properly configured.

More information:

MIB Support and Device Compatibility (see page 9)

Configure VPN Discovery Options

Before modeling your MPLS VPN Manager environment, you can select several VPN Discovery options. These options determine how CA Spectrum finds and models the VPNs in your environment.

To configure the VPN Discovery options

1. Open MPLS VPN Manager (see page 11).

   MPLS VPN Manager opens, and the Contents panel populates with information about the selected VPN Manager.

2. Click the Information tab.
3. Expand the Configuration, VPN Discovery subview.
4. Click set in the following fields to select your configuration settings:

   Model Inactive VPNs

   Determines whether inactive VPNs in your network environment are discovered and modeled by VPN Discovery.

   Default: No

   Enable Dynamic Discovery

   Determines whether to start the VPN Discovery automatically when a new PE router is modeled. Starting VPN Discovery automatically helps to keep the VPN information current when new devices are added to the network.

   Note: As the MPLS VPN Manager application is running, VPN sites may be created or destroyed when certain traps are received.

   Default: No

   Use RD instead of VRF name

   Determines whether to use the VRF name or Route Distinguisher information from the MIB as the unique identifier when determining VPN membership. This information is used when discovering and naming your VPN site models. By default, CA Spectrum uses the VRF name. However, if your routers use different VRF names for the same VPN route target, CA Spectrum creates a separate VPN site model for each new name. In this case, you can avoid multiple models for the same VPN site by configuring CA Spectrum to use the Route Distinguisher (RD) from the MIB to model your VPN sites.

   Default: No

   VRF/RD Name Filter Type

   Determines if the VRF/RD names in the 'Global VRF/RD Name Filter' field are included or excluded from modeling. This feature can save unnecessary resources by limiting the number of VPN sites that require monitoring. Options include the following:

- Exclusive
- Inclusive

Global VRF/RD Name Filter

Specifies the VRF/RD names to be included or excluded from modeling. This field is used together with the 'VRF/RD Name Filter Type' field.

Default Ping Mode

By default the Ping Mode is set as NoPinging. However you can select DestinationPinging as the Default Ping Mode for VPN discovery using this feature.

Note: This option is applicable only to newly discovered sites. This will not update the Ping mode property of existing sites.

You have successfully configured VPN Discovery options.

More information:

Automatically Creating and Deleting VPN Sites (see page 56)

IfExclusionList

IfExclusionList is an attribute of the VpnManager (attribute ID: 0x4940185) and is not listed with the VPN Discovery configuration options. This attribute is a text attribute with the default value of 24,131. This value means that by default MPLS VPN Manager does not create VpnSite models for loopback interfaces (ifType=24) and tunnel interfaces (ifType=131).

This attribute can be modified to include additional interface types by using the Attribute Editor in OneClick and adding IfExclusionList as a User Defined attribute.

Note: Use the Global_IfExclusionList attribute in Distributed SpectroSERVER environment to apply the changes to all SpectroSERVERs.

Update VPN Models for Overlapping VPN Topology

VPN models created prior to CA Spectrum Release 9.2.1 do not support overlapping VPN topology. CA Spectrum does not automatically update existing VPN models to support overlapping VPNs. To properly manage your overlapping VPNs in CA Spectrum, you must manually migrate the existing VPN models.

To update VPN models to use overlapping VPN topology

1. Open MPLS VPN Manager (see page 11).

   MPLS VPN Manager opens, and the Contents panel populates with information about the selected VPN Manager.

2. Click the List tab.

   The table lists all existing VPN models.

3. Select all VPN models, right-click, and select Delete.

   CA Spectrum deletes all VPN models and their associated VPN Site models.

4. Run VPN Discovery (see page 21).

   CA Spectrum updates your VPN models by recreating the VPN models. These new models support overlapping VPN topologies.

Run VPN Discovery

VPN Discovery is the simplest method of modeling your network. Before you run an on-demand VPN Discovery, ensure that you meet the prerequisites.

Important! Before you run VPN Discovery, be sure that all Provider Edge devices are modeled in CA Spectrum with the read/write community name. MPLS VPN Manager cannot locate your VPNs without these Provider Edge models in the SpectroSERVER.

Follow these steps:

1. Open MPLS VPN Manager (see page 11).

   MPLS VPN Manager opens, and the Contents panel populates with information about the selected VPN Manager.

2. Click the Information tab.
3. Expand the Configuration, VPN Discovery subview.

   The VPN Discovery options and configurations display.

4. Click Run.

   The Select Landscapes dialog opens, requesting the landscapes on which you want to run VPN Discovery.

5. Select the landscapes and click OK.

   VPN Discovery runs. When complete, the VPN Discovery field status indicator lists the status. Also, a tooltip on this field lists the number of discovered MPLS-VPN devices (single SpectroSERVER) or servers (distributed SpectroSERVER).

Configuring VPN Discovery During Modeling

CA Spectrum lets you configure Network Services Discoveries including VPN Discovery, during modeling. As a part of modeling configuration, you can specify which Network Service Discoveries to run with the modeling process.

Note: For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Run VPN Discovery on Selected Models

VPN Discovery is one of the Network Services Discovery options, which are available for models in various OneClick views. Instead of modeling all VPNs in your networking environment, this option lets you quickly model VPNs that are related to selected models in your networking environment.

To run VPN Network Services Discovery on selected models

1. Open OneClick.
2. Select device models related to your VPN environment.
3. Right-click the models and select Tools, Utilities, Network Services Discoveries, VPN Discovery.

   The VPN Discovery process is initiated for the selected models only. You can check the status in the Configuration, VPN Discovery subview for MPLS VPN Manager.

Model Types

CA Spectrum creates several model types during VPN Discovery to represent different aspects of the MPLS/BGP VPN MIB in MPLS VPN Manager.

The MPLS VPN Manager model types include the following:

VPN Manager

Represents the MPLS VPN Manager component installed with CA Spectrum that manages your VPN networking environment. The CA Spectrum model type for MPLS VPN Manager is VpnManager. This model cannot be destroyed.

VPN Site

Represents each unique VPN Site that CA Spectrum discovers during VPN Discovery. CA Spectrum creates the VPN Site model on the same SpectroSERVER as its associated PE Router. The Model Class attribute for the VPN Site model is set to Transport Service. The CA Spectrum model type is VpnSite.

Note: MPLS VPN Manager assumes that each VPN Site is connected to a given PE by a single interface. By default, CA Spectrum does not create VpnSite models for loopback and tunnel interfaces.

VPN Application

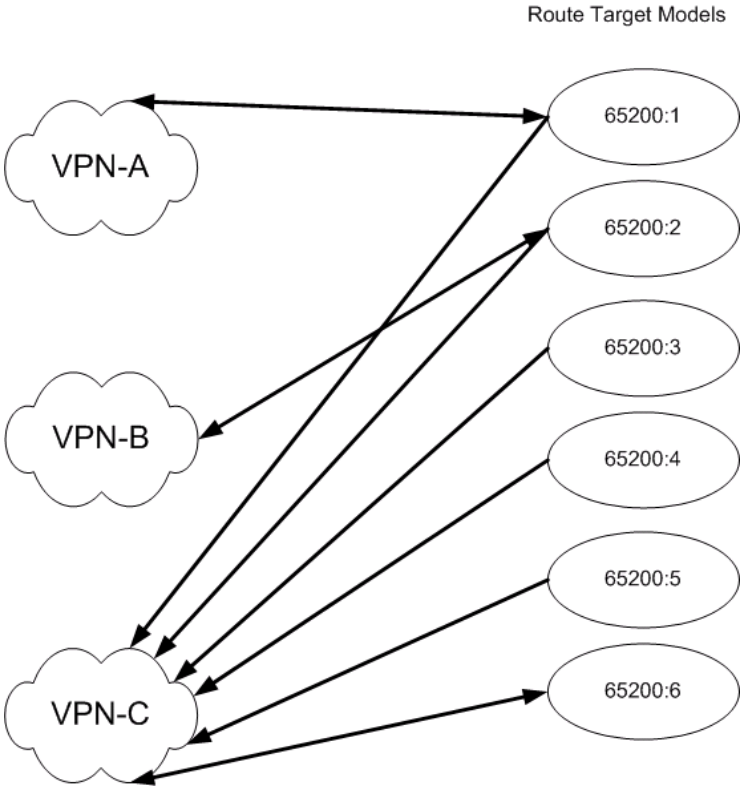
Represents a modeled device that supports the appropriate MPLS-VPN MIB. This application model must be present for VPN Discovery to successfully discover MPLS-VPN information. The CA Spectrum model types are MplsVpnApp (for Cisco devices) and JNPR_VPN_App (for Juniper devices). The Model Class attribute is set to Application for these models.

VPN

Represents each unique VPN that CA Spectrum models. The Model Class attribute for the VPN model is set to Transport Services. The CA Spectrum model type is MplsVpn.

Route Target

Represents the Import and Export of Route Targets. Models of this type do not display in the Navigation view. Instead, they are created on the Main Location Server (MLS). The following diagram shows the Route Target Models created for an overlapping VPN topology scenario:



VPN Site Names

CA Spectrum generates unique names for VPN Sites during Discovery based on the PE model name, VPN name, and IfName of the interface to which the VPN Site is connected. Using these values helps ensure the VPN Site names in CA Spectrum are unique.

The VPN Site name follows this structure:

ModelName_VPNname_IfName

ModelName

Represents the name of the PE Router model to which the VPN Site is connected.

Example: 172.19.38.40

VPNname

Represents the name of the VPN to which the VPN Site is connected.

Example: vpn-blue

IfName

Represents the IfName of the interface to which the VPN Site is connected.

Example: VPN Site name

CA Spectrum creates the following VPN Site name when the VPN Site is connected to a VPN named "vpn-blue," a PE Router model named "172.19.38.40," and the interface IfName value is "Fa2/0":

```
172.19.38.40_vpn-blue_Fa2/0
```

VPN Site Model Deletion

A VPN Site model can be deleted in any of the following ways:

- VPN Site models can be manually deleted from the Explorer tab.
- VPN Site models automatically delete when the associated VPN model or Provider Edge (PE) Router model is deleted.

  Note: When a VPN is deleted in an overlapping VPN environment, CA Spectrum cannot delete the associated VPN Sites with multiple memberships. CA Spectrum deletes a VPN Site with multiple memberships only when the last VPN referencing the site is deleted.

- VPN models automatically delete when all associated VPN Site models are deleted.
- VPN Site models automatically delete when CA Spectrum receives an mplsVrfIfDown SNMP trap from the associated PE Router model and the same VRF entry was removed from the PE Router's VRF Table.

Chapter 4: Configuring MPLS VPN Manager

After VPN Discovery, you can configure MPLS VPN Manager to manage the VPN environment effectively. MPLS VPN Manager provides configuration options for VPN Manager models, the individual VPN models, and for VPN Site models, as follows:

- The VPN Manager model configuration lets you specify parameters for all of the VPNs managed by the specified VPN Manager. You can configure VRF Ping and VRF Trace parameters that check on the connectivity of the VPNs in your network and you can configure other parameters relating to how traps and alarms are processed.
- VPN configuration parameters let you set threshold values and other alarm specifics for the VPN Sites within that VPN.
- VPN Site configuration lets you set Trace Mode and Ping Mode, which determine how VRF Path Tracing and VRF Ping should operate within the VPN.

This section describes how to access and set configuration options for MPLS VPN Manager.

This section contains the following topics:

Distributed SpectroSERVER Configuration

In a distributed SpectroSERVER (DSS) environment, you can model your PE Routers from any SpectroSERVER. A VPN Site model is created on the SpectroSERVER that its associated PE Router is modeled on. All of the discovered VPNs appear in the VPN Manager area of the OneClick Console. You can enable cross-server Path Tracing and Ping tests to determine the condition of the VPNs that you are managing. The local SpectroSERVERs must have a connection to the Main Location Server (MLS) to support this distributed configuration.

Important! An implementation requirement of the distributed VPN Manager is that all MplsVpn models must reside on the SpectroSERVER that is on the MLS machine. When you change the MLS, the MplsVpn and VpnSite models become invalid and are deleted by each SpectroSERVER in the DSS environment.

Note: For more information about changing the MLS, see the procedures in the *Distributed SpectroSERVER Administrator Guide*.

VPN Manager Configuration

The VPN Manager model manages a set of VPNs on a given CA Spectrum landscape. The following options are controlled by the VPN Manager model:

- Port polling
- Default model priority
- Traps
- VRF pinging
- VRF path tracing

More information:

Using VPN Search options in Locater Tab (see page 14)

Configure Port Polling

Port polling must be enabled to update the condition of VPN Site models. But, polling can impact your MPLS VPN Manager performance. To help you optimize your MPLS VPN Manager performance, you can control port polling.

To configure port polling for MPLS VPN Manager

1. Open MPLS VPN Manager (see page 11).

   MPLS VPN Manager opens, and the Contents panel populates with information about the selected VPN Manager.
2. Click the Information tab.
3. Expand the Configuration, Management Configuration subview.
4. Click set in the following field, select your configuration setting, and click Save:

   Enable Port Polling

   Determines whether MPLS VPN Manager polls ports.

   Default: Yes

   Your port polling option is configured.

Control Default Model Priority

Each model MPLS VPN Manager creates has a priority value. Using priority values, you can quickly sort a list of VPNs or VPN Sites to list those with higher priorities first. During VPN Discovery, CA Spectrum assigns a default priority value. You can configure the default priority value assigned to new VPN and VPN Site models.

To control the default model priority

1. Open MPLS VPN Manager (see page 11).

   MPLS VPN Manager opens, and the Contents panel populates with information about the selected VPN Manager.

2. Click the Information tab.

3. Expand the Configuration, Management Configuration subview.

4. Click set in the following fields, select your configuration setting, and click Save:

   Default VPN Priority

   Defines the default priority value assigned to newly created VPN models in MPLS VPN Manager. This value lets you sort VPNs in order of their priority to your work.

   Default: 10

   Limits: 0–4 billion

   Default Site Priority

   Defines the default priority value assigned to newly created VPN Site models in MPLS VPN Manager. This value lets you sort VPN Sites in order of their priority to your work.

   Default: 10

   Limits: 0–4 billion

   Your default model priority values are configured, and VPN Discovery assigns these values to newly created models.

Configure Trap Options

Traps sent from VPN devices can signal MPLS VPN Manager when a VPN device is newly available or no longer available for management in CA Spectrum. Based on your needs, you can enable or disable these traps from creating or deleting VPN device models.

To configure trap options

1. Open MPLS VPN Manager (see page 11).

   MPLS VPN Manager opens, and the Contents panel populates with information about the selected VPN Manager.

2. Click the Information tab.
3. Expand the Configuration, Management Configuration subview.
4. Click set in the following fields, select your configuration settings, and click Save:

   Create on Trap

   Determines whether the receipt of a mplsVrfIfUp or jnxVpnIfUp trap results in a new VPN Site or VPN being discovered and modeled by MPLS VPN Manager.

   Default: Yes

   Delete on Trap

   Determines whether the receipt of a mplsVrfIfDown or jnxVpnIfDown trap results in a VPN Site or VPN being deleted from MPLS VPN Manager.

   Default: Yes

   Your trap options are configured.

Configure VRF Ping

MPLS VPN Manager can enable or disable cross-server pinging. Enabling cross-server pinging between domains that are not very related is not recommended. For example, conducting a VRF ping between service customer domains that are highly segmented can reduce performance on the PE Routers. Configuring your VRF ping options lets you optimize your MPLS VPN Manager performance.

To control the default model priority

1. Open MPLS VPN Manager (see page 11).

   MPLS VPN Manager opens, and the Contents panel populates with information about the selected VPN Manager.

2. Click the Information tab.

3. Expand the Configuration, VRF Ping subview.
4. Click set in the following fields, select your configuration settings, and click Save:

Enable VRF Ping

Determines whether MPLS VPN Manager sends VRF pings to monitor VPN connectivity. When set to Yes, MPLS VPN Manager sends VRF pings using RTTMON for Cisco devices and Juniper RFC2925, and using Juniper's Ping extension MIB for Juniper devices. When set to No, MPLS VPN Manager infers VPN condition from the VPN Site condition.

Default: Yes

VRF Ping Interval

Determines the time interval between VRF pings. Setting this value to a higher number reduces network traffic.

Default: 1200

VRF Ping Timeout

Determines the time (milliseconds) to wait for a VRF ping to complete.

Default: 5000

Enable Cross-VPN Ping Tests

Controls whether VRF pings test connectivity across overlapping VPN boundaries. For example, a VPN Site from vpn-blue normally does not communicate with a VPN Site from vpn-red. If vpn-blue imports the route target from vpn-red, then they *may* communicate. This attribute (EnableTransVpnPing) determines whether MPLS VPN Manager attempts this Service Assurance (SA) test.

Default: Yes

Enable Cross-server VRF Ping Tests

Determines whether site-to-site connectivity test occur across multiple SpectroSERVERs. When set to No, site-to-site tests occur on a single SpectroSERVER only.

Delete Completed VRF Ping Tests

Determines whether MPLS VPN Manager deletes VRF ping tests upon their completion. Setting this value to Yes reduces router memory usage, but requires additional network usage to set up subsequent tests.

Default: No

Collapse Bidirectional Ping

Determines whether MPLS VPN Manager performs a bidirectional VRF ping. Setting this value to Yes limits the VRF ping to one direction only. Unidirectional VRF pinging works based on the assumption that if one site can successfully receive a response from another, then the network between them is functioning properly. Unidirectional VRF pinging can reduce network traffic by eliminating potentially redundant ping tests.

Important! Before changing the value of this field, you must stop VRF pings by setting the Enable VRF Ping option to No. After changing the Collapse Bidirectional Ping option, restart VRF pings by setting the Enable VRF Ping option to Yes.

Default: Yes

Your VRF ping options are configured.

More information:

Scalability of Ping Tests (see page 53)
Calculating the VPN Condition using VRF Ping Response Time Threshold (see page 53)
Calculating the VPN Condition using VRF Ping (see page 52)

Configure VRF Path Trace

MPLS VPN Manager can enable or disable cross-server path traces. Enabling cross-server path traces between domains that are not very related is not recommended. For example, conducting a VRF path trace between service customer domains that are highly segmented can reduce performance on the PE Routers. Configuring your VRF path tracing options lets you optimize your MPLS VPN Manager performance.

To configure VRF Path Trace options

1. Open MPLS VPN Manager (see page 11).

   MPLS VPN Manager opens, and the Contents panel populates with information about the selected VPN Manager.

2. Click the Information tab.
3. Expand the Configuration, VRF Path Trace subview.
4. Click set in the following fields, select your configuration settings, and click Save:

   Enable Path Trace

   Enables all of the path tracing features for all VPN models managed by the selected VPN Manager model. Setting this option to No disables path tracing.

   Default: No

Path Trace Interval (seconds)

Determines the time interval between invocations of site-to-site path tracing.

Default: 1200

Path Trace Timeout (msec)

Determines the time (milliseconds) to wait for a VRF path trace to complete.

Default: 25000

History Limit

Defines the maximum number of paths to be remembered between any pair of VPN Sites. To limit memory usage, the maximum History Limit value is 12.

Limits: 1–12

Default: 5

Enable Cross-VPN Path Traces

Controls whether VRF path traces cross overlapping VPN boundaries. For example, a VPN Site from vpn-blue normally does not communicate with a VPN Site from vpn-red. If vpn-blue imports the route target from vpn-red, then they *may* communicate. This attribute (EnableTransVpnTrace) determines whether MPLS VPN Manager attempts this Service Assurance (SA) test.

Default: Yes

Enable Cross-server Path Traces

Determines whether site-to-site connectivity tests occur across multiple SpectroSERVERs. When set to No, site-to-site tests occur on a single SpectroSERVER only.

Default: Yes

Enable Path Change Alarms

Determines whether CA Spectrum generates alarms when the number of path changes exceeds the thresholds defined by the Critical, Major, and Minor Threshold % values.

Default: No

Critical Threshold %

Defines the critical threshold for the percentage of path changes in a given poll cycle. If this value is set to zero, MPLS VPN Manager generates alarms for any path changes.

Default: 10

Major Threshold %

Defines the major threshold for the percentage of path changes in a given poll cycle. If this value is set to zero, MPLS VPN Manager generates alarms for any path changes.

Default: 5

Minor Threshold %

Defines the minor threshold for the percentage of paths changed in a given poll cycle. If this value is set to zero, MPLS VPN Manager generates alarms for any path changes.

Default: 3

Note: MPLS VPN Manager uses these threshold values for VRF path tracing functionality only.

Your VRF path trace options are configured.

Global Configurations and Local Overrides

In a distributed SpectroSERVER (DSS) environment, the configuration options set on the MLS VPN Manager are applied to the VPN Managers on remote SpectroSERVERs by default. You can override a global configuration on a remote VPN Manager.

Note: Use caution when making overrides. Whenever possible, update the model information on the MLS as a best practice and use local overrides for any changes required on a specific SpectroSERVER.

Overriding Global Configurations

You can override a global configuration value by setting a local override on a remote VPN Manager.

To override global configuration values for select VPN Manager

1. Search using the All VPN Managers predefined search (see page 14).

   The search results appear in the Contents panel.

2. Select the VPN Manager model you want to configure.

   Details about the selected VPN Manager appear in the Component Detail panel.

3. Click the Information tab.

4. Expand the Configuration subview and locate the configuration value to override.

5. Click set for the configuration option.

   The Local Override Panel displays. The Global value is the value set on the MLS VPN Manager.

6. Change the Local value to the desired value, unselect the 'Use global value' check box, and click Save.

   Note: The 'Use global value' check box appears only when the selected value differs from the Global value.

   The global configuration settings are overridden for the selected VPN Manager.

Note: When a local override is being used, the attribute value will have an asterisk appended to the end of it in the Configuration subview.

VPN Model Configuration

For each VPN model, you can configure VPN condition alarms. These settings turn alarming on, determine how MPLS VPN Manager generates information about the VPN models, and determine the alarm severity, based on threshold settings. Each threshold is based on the percentage of VPN Sites that are part of the VPN that are “Down.” VPN Sites are determined to be in a “Down” condition either through VRF ping tests or by analyzing the aggregate VPN Site condition for a VPN.

More information:

Calculating the Condition of a VPN (see page 51)

Configuring VPN Condition Alarms

The Component Detail panel's Information tab for a selected VPN model contains the Configuration Information section. Use this section to set the thresholds that determine what, if any, VPN Condition alarms are generated.

Note: These threshold values are used for both VRF Ping and the Condition value associated with the VPN Site models. These thresholds are not used by the VRF Trace functionality.

Before accessing the VPN configuration options, you must find the appropriate VPN model. To do this:

1. Perform an All VPNs search or select a VPN model in the Explorer tab and skip step 2.
2. In the Contents panel, select the VPN model you want to configure from the Results list.

Once you have selected the appropriate VPN model, the Component Detail panel's Information tab shows all of the configuration options for the VPN Model. Each of these options are explained in the following section.

To change any configuration value, click the value's set link, change the value, and press Enter.

Critical Threshold %

This value is the percentage of down (unreachable) VPN Sites that will result in the generation of a critical alarm for the model.

default: 15%

Major Threshold %

This value is the percentage of down (unreachable) VPN Sites that will result in the generation of a major alarm.

default: 10%

Minor Threshold %

This value is the percentage of down (unreachable) VPN Sites that will result in the generation of a minor alarm.

default: 5%

Response Time Threshold (msecs)

The event threshold for the response time of a successful Ping test.

default: 250 milliseconds

Enable VPN Alarms

Enable VPN Alarms is set to Yes by default. Thus when the condition of the VPN model changes, an alarm is generated. When this value is set to Yes and contact is lost to a VPN (with traps properly configured), an event triggers an alarm that is asserted against the VPN Model. When this value is set to No and contact is lost to a VPN, the VPN model turns red, but no alarm is created.

default: Yes

Enable Site Alarms

Enable Site Alarms is by default set to No. With this default setting, no alarm is generated when the condition of the VPN Site model changes to critical. When this attribute is set to Yes, an alarm is generated when the condition of the VPN Site changes to Critical.

default: No

Note: If a site is participating in multiple VPNs then you need to Enable Site Alarms on the VPN (VRF) which is configured on that site.

VPN Manager Path Tracing Active

This parameter reflects the value set for the VPN Manager Enable Path Trace parameter.

Participate in Path Tracing

This parameter enables path tracing for all of the sites in the selected VPN. VPN Manager Path Tracing Active and Participate in Path Tracing must be set to yes in order for path tracing to be active.

Enable Path Change Alarms

When this parameter is set to Yes, MPLS VPN Manager generates alarms when the number of path changes exceed the thresholds defined in the VPN Manager's VRF Path Trace configuration.

Note: If you use VRF ping connectivity tests instead of an analysis of the VPN's aggregate VPN Site condition to determine the VPN condition, the number of site-to-site VRF ping test failures is used in place of the percentage of VPN Sites down to define threshold violations. For example, a VPN condition of Good is reported when the number of site-to-site VRF ping test failures is less than the Minor threshold.

More information:

Using VPN Search options in Locater Tab (see page 14)
Configure VRF Path Trace (see page 32)
Calculating the VPN Condition using VRF Ping (see page 52)

VPN Site Model Configuration

VRF Path Tracing and VRF Ping are mechanisms for monitoring your VPNs.

You must configure the individual site models within each VPN to be a Source, Destination, Source/Destination, or none of the above. Selecting the most appropriate mode will optimize the communication process to more closely match the role of the sites on your network.

For example, if all sites were placed into SrcDest this would generate a great deal of traffic. For a VPN with 100 sites, there would be tests initiated to and from every site resulting in a full mesh of 10,000 tests. A more network-efficient deployment would be to identify key sites that house critical application servers such as mail, web, or database servers and set only those to Destination.

Configure VRF Path Trace Source and Destination

There are four possible values for Trace Mode:

NoTracing

Tracing is not enabled for this site.

SourceTracing

This site can originate a path trace.

DestinationTracing

This site can receive a path trace from a source.

SrcDestTracing

This site can either originate or receive a path trace.

The Trace Mode option allows you to select the extent to which a site participates in the automated traceroute functionality. By default all sites are set to SourceTracing. Therefore, no tracing occurs until at least one site is set to either DestinationTracing or SrcDestTracing. These VPN Site models must be members of the same VPN.

You can set the value of the Trace Mode attribute for a particular VPN Site using two methods:

Method 1: Using the Contents Panel

1. Perform an All Sites search (see page 14).

   When the search is complete, the list of VPN Sites is shown in the Results tab of the Contents panel.

2. Right-click the heading row to display the Table Preferences dialog. Make sure that Trace Mode is checked and click OK.

   The Trace Mode column appears in the list of VPN Sites.

3. Click set to select the value of the Trace Mode.

Method 2: Using the Associated Sites List

1. Select the desired VPN Manager from the Explorer tab.
2. In the Component Details panel, select the Information tab.
3. Select the Associated sites section.
4. Right-click the heading row to display the Table Preferences dialog. Make sure that Trace Mode is checked and click OK.

   The Trace Mode column appears in the list of VPN Sites.

5. Click set to select the Trace Mode.

Configure VRF Ping Source and Destination

There are four possible values for Ping Mode:

NoPinging

Pinging is not enabled for this site.

SourcePinging

This site can originate a ping.

DestinationPinging

This site can receive a ping from a source.

SrcDestPinging

This site can either originate or receive a ping.

The Ping option allows you to select the extent to which a site participates in the automated ping functionality. By default all sites are set to NoPinging. Therefore, no pinging occurs until at least one site is set to either DestinationPinging or SrcDestPinging. These VPN Site models must be members of the same VPN.

Note: A Default Ping Mode feature has been added to the VPN Discovery Configuration options, you can select the default ping mode from the options in the list.

You can set the value of the Ping Mode attribute for a particular VPN Site using two methods:

Method 1: Using the Contents Panel

1. Perform an All Sites search (see page 14).
2. When the search is complete, the list of VPN Sites is shown in the Results tab of the Contents panel.
3. Right-click the heading row to display the Table Preferences dialog. Make sure that Ping Mode is checked and click OK.

   The Ping Mode column appears in the list of VPN Sites.
4. Click set to select the value of the Ping Mode.

Method 2: Using the Associated Sites List

1. Select the desired VPN from the Explorer tab.
2. In the Component Details panel, select the Information tab.
3. Select the Associated sites section.
4. Right-click the heading row to display the Table Preferences dialog. Make sure that Ping Mode is checked and click OK.

   The Ping Mode column appears in the list of VPN Sites.

5. Click set to select the Ping Mode.

Chapter 5: Managing VPNs

This section contains the following topics:

The VPN Manager Model

The VPN Manager model manages a set of VPNs on a given CA Spectrum landscape. Each of these VPNs contains a series of VPN Sites which are also modeled and managed within the VPN Manager hierarchy. The following steps show you how to view all of the VPNs known to a specific VPN Manager:

1. Perform an All VPNs search (see page 14).
2. In the Contents panel, VPN Manager displays a list of all VPNs currently known.

Each of these VPNs contain VPN Sites. Both the VPN Models and the VPN Site models display valuable information to assist you in managing the VPNs on your network. The sections in this chapter explain the information available for both VPN and VPN Site models.

More information:

Using VPN Search options in Locater Tab (see page 14)

The VPN Model

When a VPN model is selected, the Information tab contains all of the configurable options for a selected VPN model. The Information tab contains submenus which are described in the following sections.

General Information

The General Information section provides you with some basic information about the VPN model.

Condition

The current condition of the VPN.

VPN Model Name

The VPN model name.

Model Class

The model class of the VPN model.

Note: For more information about CA Spectrum model classes, see the *Concepts Guide*.

Creation Time

The date and time that the VPN model was created.

Security String

The security string for the VPN model.

Landscape

The CA Spectrum landscape to which the VPN model belongs.

Priority

The priority value used for the condition calculation.

Description

A description of the VPN model that is appropriate to your network. Click set, type the description in the field provided, and press Enter.

Notes

You can use this field to save notes about the VPN model. Click set, type the notes into the field provided, and click Save to save the notes.

More information:

Calculating the Condition of a VPN (see page 51)

Configuration Information

This section enables you to configure how the VPN monitors certain threshold values that contribute to alarms and the condition of the VPN.

More information:

VPN Model Configuration (see page 35)

Route Statistics

The route statistics show how many routes have been added to the selected VPN. MPLS VPN Manager calculates these statistics from reading the mplsVpnVrfPerfRoutesAdded, the mplsVpnVrfPerfRoutesDeleted, and the mplsVpnVrfPerfCurrNumRoutes parameters from each device on the VPN. These parameters are added together to produce a VPN-wide total.

For example, when a site is added to a VPN, the mplsVpnVrfPerfCurrNumRoutes and the mplsVpnVrfPerfRoutesAdded parameters are incremented.

These statistics provide a measurement of the current capacity of usage of the VPN.

Associated Sites

This table shows all of the VPN Site models associated with the selected VPN model.

Associated Edge Routers

This table lists all of the edge routers used by the selected VPN model.

The VPN Site Model

When a VPN site model is selected, the Information tab contains all of the configurable options for a selected VPN model. The Information tab contains submenus which are described in the following sections.

General Information

Condition

The current condition of the VPN Site.

Priority

The priority value used for the condition calculation.

Model Class

The model class of the VPN Site model.

Note: For more information about CA Spectrum model classes, see the *Concepts Guide*.

Model Creation Time

The date and time that MPLS VPN Manager created the VPN Site model.

Security String

The security string for the VPN Site model.

Description

A description of the VPN Site model.

Site Creation Time

The date and time that MPLS VPN Manager created the VPN Site.

Landscape

The CA Spectrum landscape to which the VPN Site model belongs.

Notes

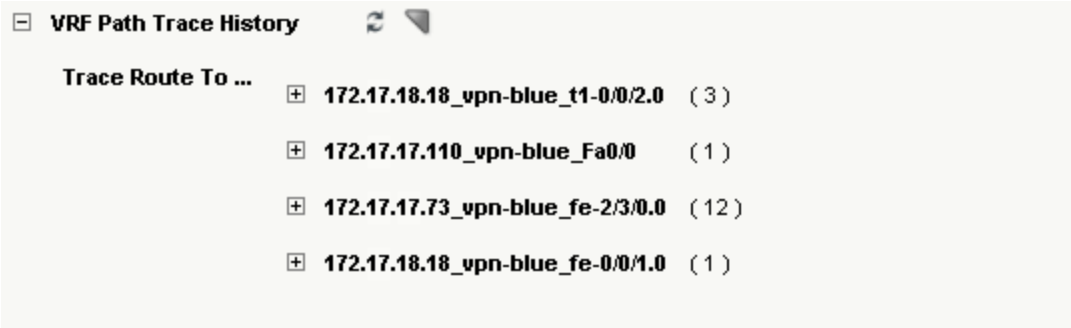
You can use this field to save notes about the VPN model. Click set, type the notes into the field provided, and click Save.

More information:

Calculating the Condition of a VPN (see page 51)

VRF Path Trace History

This section shows the history of all path trace tests from this Site to all peer Sites within the VPN.



Click the **+** symbol to find specific information about a path trace to the specific site listed as shown in the following graphic.

This menu shows the date and time that the path trace occurred and also shows the IP address of the two VPN sites involved in the path trace. The chart shows specific details about the path between the two VPN sites.

Next Hop Addr

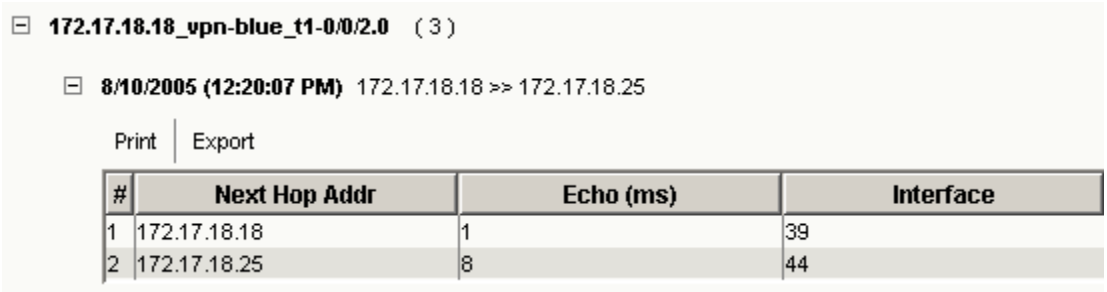
This shows all of the IP addresses of the devices on the path from the originating site to the destination site.

Echo (ms)

The time in milliseconds for the path trace results to be returned.

Interface

The IfIndex value used by the path trace for the device shown in the Next Hop Addr column.



#	Next Hop Addr	Echo (ms)	Interface
1	172.17.18.18	1	39
2	172.17.18.25	8	44

BGP Statistics

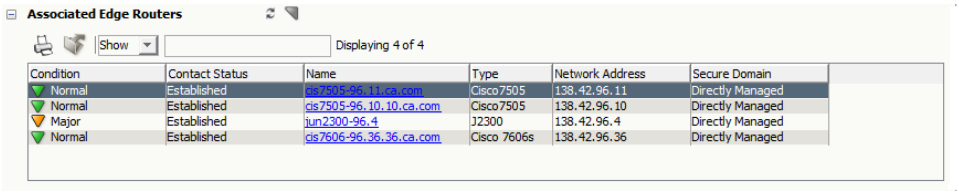
The BGP Statistics subview displays details about the BGP peer session involving the selected VPN site device. Details include the following:

- Local Peer ID
- Remote Peer ID
- Peer State
- Peer Keep Alive
- Peer Hold Time
- Remote AS

Note: For more information about BGP peer session monitoring, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Associated Edge Routers

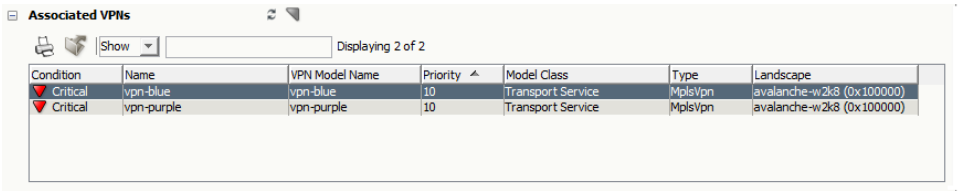
The Associated Edge Routers chart shows the edge routers associated with the selected VPN site.



Note: If you click the hyperlink in the Name column, you will be redirected to the device location in the respective SpectroSERVER universe.

Associated VPNs

The Associated VPNs chart shows the VPNs associated with the selected VPN site.



VPN and VPN Site Performance

The Performance tab displays performance information for a selected VPN Site or VPN Site Performance. For a selected VPN Site, the performance information is based only on the traffic across the single interface to which the VPN Site is connected. VPN Site performance is a real-time value resulting from the polling of the following interface statistics:

- Bytes In Rate
- Bytes Out Rate
- Out/In Unicast Packet Rate
- Out/In Broadcast Rate
- Out/In Multicast Rate

Note: VPN performance data for a selected VPN is an aggregation of the performance data of the component VPN Sites in a VPN.

Spotlighting VPNs

Use the OneClick Spotlight feature to see all models related to a VPN in the Topology view. Spotlighting VPNs in the Topology view helps you more easily determine relationships between VPNs and your network, and between VPNs and other models on your network.

Note: When spotlighting in either the VPN or VPN Site Topology views, you can select only a single VPN.

To spotlight a VPN

1. Open OneClick.
2. Expand the desired landscape on the Explorer tab and select Universe.

   Details about the selected Universe appear in the Contents panel.
3. Click the Topology tab.

   The topology of the Universe is displayed.
4. Click  (Spotlight View) and select VPN List.

   The VPN List dialog opens.
5. Select a VPN.

   CA Spectrum spotlights the selected VPN by dimming all models in the topology that are not part of the selected VPN.

Note: To view information about the selected VPN, click  (View the Component Detail) on the VPN List dialog.

Checking the Status of VPN Paths with VRF Path Tracing

MPLS VPN Manager lets you monitor paths within a VPN in two ways. You can enable background path monitoring, which allows paths to be monitored consistently at a preset interval. You can also issue a path trace command on demand to check the path between two VPN sites.

Important! You must use a read/write community string when modeling devices in CA Spectrum for VRF Path Tracing to function properly.

Background Path Monitoring

Background path monitoring traces the paths between VPN Sites based on the configuration options you have chosen. The results of the path traces appear in the VPN Site model's VRF Path Trace History menu.

To use background path monitoring, you must configure the following parameters:

- In the configuration for the VPN Manager model, you must configure the VRF Path Trace parameters. Each of these parameters is explained in the section on VRF Path Trace.
- In the configuration for the VPN model, you must configure the VPN to participate in path tracing, and, if desired, turn on alarms relating to VRF path tracing threshold violations.
- In the VPN Site list, you must configure each VPN Site's trace mode. For instructions see VPN Site Model Configuration.

The VPN Path Trace history results are shown in the VPN Site model's VRF Path Trace History menu in the Information tab.

More information:

Configure VRF Path Trace (see page 32)
VPN Site Model Configuration (see page 38)
VRF Path Trace History (see page 47)

On-Demand Path Monitoring

An on-demand path trace traces a path between two VPN sites that you have selected. The two VPN sites must belong to the same VPN.

To initiate an on-demand path trace

1. Perform an All Sites search (see page 14), or locate the desired VPN Site model from the Explorer tab in the Navigation panel and skip step 2.
2. In the Contents panel, locate the VPN Site model you want to configure from the Results list.
3. Right-click the VPN Site model from which you would like to initiate the path trace.
4. Select Select Vrf Trace Start Point.
5. Right-click the VPN Site model that is the destination of the path trace and select Vrf Trace From <VpnSite>. This starts the on-demand path trace.

   The results of the path trace appear in a dialog after the path trace finishes.

More information:

Using VPN Search options in Locater Tab (see page 14)

Calculating the Condition of a VPN

The overall condition of a VPN is of critical importance to providers of VPN services. VPN Sites impact the health of all VPNs in which it has membership. MPLS VPN Manager provides the following two mechanisms to calculate the VPN condition:

- VRF Ping to determine the state of connectivity
- Condition values determined by alarm threshold values set on each VPN Site model and rolled up to the VPN model

You can choose either mechanism. However, CA Spectrum cannot use both at the same time. When enabled, VRF Ping takes precedence over the VPN Site condition rollup method. To use the condition rollup method, make sure VRF Ping is disabled.

A single VPN Site outage can cause the generation of several alarms (that is, one alarm for each VPN in which the VPN Site has membership). CA Spectrum does not correlate (that is, suppress) the alarms. Areas affected include the following:

- VPN condition calculation
- VRF test results
- Aggregate VPN performance (bandwidth usage added to each VPN)

Calculating the VPN Condition using VRF Ping

By default, MPLS VPN Manager uses the state of connectivity between the VPN sites to determine the condition of the VPN. VRF Ping connectivity tests calculate condition for a VPN Site from information obtained from the VRF Table. Using Cisco's VRF Aware Ping (configured through the RTTMON-MIB) and the Juniper Ping MIB extensions to RFC2925, the PE Router can initiate and send pings to any VPN Site on the network. Each entry in the VRF table has information pertaining to one unique Site.

Note: If you use VRF ping connectivity tests instead of an analysis of the VPN's aggregate VPN Site condition to determine the VPN condition, the number of site-to-site VRF ping test failures is used in place of the percentage of VPN Sites down to define threshold violations. For example, a VPN condition of Good is reported when the number of site-to-site VRF ping test failures is less than the Minor threshold. This option is applicable only to newly discovered sites. This will not update the Ping mode property of existing sites.

To ensure that MPLS VPN Manager can use VRF Ping to test for connectivity

1. Verify that you have modeled in CA Spectrum the devices that are part of the VPN network.
2. Verify that you have used a read/write community string when modeling devices in CA Spectrum.
3. Verify that Enable VRF Ping is set to Yes on the VPN Manager model.
4. Verify VRF Pings are being run on the device by examining the appropriate MIB on the VPN device (RTTMON for Cisco devices, Juniper Ping MIB extensions to RFC2925 for Juniper devices).
5. Verify that the condition of the VPN and VPN Site models is updated correctly and that VRF Pings are successful.
6. Verify the appropriate VPN sites are set as Ping Sources and Destinations.

More information:

VPN Manager Configuration (see page 28)
Configure VRF Ping Source and Destination (see page 40)
Configuring VPN Condition Alarms (see page 36)

Calculating the VPN Condition using VRF Ping Response Time Threshold

The result of a VRF Ping test alone informs you of the success or failure of the Ping test. Adding a Response Time Threshold to your VRF Ping tests provides more detailed results than just success or failure.

To ensure that MPLS VPN Manager can use VRF Ping Response Time Threshold

1. Verify you satisfy the requirements listed in Calculating the VPN Condition using VRF Ping.
2. Verify the Response Time Threshold parameter is set to the appropriate value.
3. Verify your Minor, Major and Critical Alarm Threshold % attributes are set to the appropriate values.

More information:

Configuring VPN Condition Alarms (see page 36)
Calculating the VPN Condition using VRF Ping (see page 52)

Scalability of Ping Tests

The scalability of Ping tests should be considered in large environments where fully meshed testing is performed. Performance testing has shown that full mesh testing beyond 50 sites greatly increases network traffic. The number of Ping tests and the resource requirements can be efficiently managed by organizing your Ping tests.

We recommend that you select a relatively small number of important sites to perform Ping testing. One approach, when the number of sites or remote offices is beyond 50, is to have larger regional offices test back to corporate headquarters or among themselves. For example, in an environment that consists of several regional offices and a corporate headquarters, configuring your corporate headquarters as Ping to Site and your larger regional offices as Ping from Site reduces the network load.

More information:

Configure VRF Ping Source and Destination (see page 40)

Calculating the VPN Condition using the VPN Site Condition

If you disable VRF Ping by setting the VPN Manager's Enable VRF Ping parameter to No, MPLS VPN Manager can calculate VPN condition based on an analysis of the VPN's aggregate VPN Site conditions. If the Condition value for every Site is “Good,” then the VPN condition is “Good.”

A VPN Site model can have one of four conditions: Initial, Maintenance, Down, or Good. Each of these conditions is explained in the following table. The following values are used to compute the Condition value for a Site:

- Value of ifOperStatus for the physical interface
- Contact status of the PE Router
- Receipt of an mplsVrfIfUp or mplsVrfIfDown trap

VPN Site Condition	Calculation
Initial	No associated IF or IF is initial.
Maintenance Condition	The associated router is in maintenance mode.
Down	IFOperStatus is Down.
Good	All associated IFs are Up.

The condition of the VPN Model is determined by the condition of all of the VPN Sites contained in the VPN. The following list shows how the condition of a VPN is determined.

Initial

No VPN Sites are modeled or all VPN Site models are “Initial.” The percentage of VPN Sites that are “Initial” is greater than the Minor Threshold.

Maintenance Condition

All the VPN Site models are in maintenance mode.

Minor

The percentage of VPN Sites down (Site Rollup condition) is greater than the Minor Threshold and less than the Major Threshold.

Major

The percentage of VPN Sites down is greater than the Major Threshold and less than the Critical threshold.

Critical

The percentage of VPN Sites down is greater than the Critical Threshold.

Good

The percentage of VPN Sites down is less than the Minor Threshold.

You can set threshold values for each VPN Model that control whether the VPN Manager generates VPN Condition alarms.

More information:

Configuring VPN Condition Alarms (see page 36)

Trap Support

The following table lists the MPLS-VPN MIB SNMP traps supported by MPLS VPN Manager. Receipt of either an mplsVrfIfUp trap or an mplsVrfIfDown trap typically results in a change of the VPN Site condition. Events are created based on changes in condition.

Note: Each device must be configured to send SNMP traps to the CA Spectrum VNM machine.

SNMP Trap	Result of Receiving Trap
mplsVrfIfUp	If the VPN Site model already exists, a change in status is reported. Otherwise, a new VPN Site model is created.
mplsVrfIfDown	If both the VPN Site model and the VPN Site on the device sending this trap exist, a change in status is reported. Otherwise, the VPN Site model is deleted.
mplsNumVrfRouteMidThreshExceeded	Event/Alarm
mplsNumVrfRouteMaxThreshExceeded	Event/Alarm
mplsNumVrfSecIllegalLabelThreshExceeded	Event/Alarm

The following table lists the Juniper traps supported by MPLS VPN Manager.

Trap	Result of Receiving Trap
jnxVpnIfUp	If the VPN Site model already exists, a change in status is reported. Otherwise, a new VPN Site model is created.
jnxVpnIfDown	If both the VPN Site model and the VPN Site on the device sending this trap exist, a change in status is reported. Otherwise, the VPN Site model is deleted.

Automatically Creating and Deleting VPN Sites

Currently, MPLS VPN Manager creates a new VPN Site model if a mplsVrfIfUp or jnxVpnIfUp trap is received from a device and a VPN Site model does not already exist for that VPN Site. If a VPN Site model does exist for that VPN Site, MPLS VPN Manager reports a change in its status.

Conversely, if MPLS VPN Manager receives a mplsVrfIfDown or jnxVpnIfDown trap from a device and the VPN Site is already modeled and it exists on the device sending the trap, MPLS VPN Manager reports a change in the status of that VPN Site. If the VPN Site no longer exists on the device that sent the trap, then MPLS VPN Manager deletes the applicable VPN Site model.

Note: These actions also depend on the configuration settings for MPLS VPN Manager.

Threshold Traps

MPLS VPN Manager supports threshold traps by creating events and alarms. These traps can be used to monitor the utilization of a PE router:

- mplsNumVrfRouteMidThreshExceeded
- mplsNumVrfRouteMaxThreshExceeded
- mplsNumVrfSecIllegalLabelThreshExceeded

As the number of VPN Sites increases, these traps indicate that the PE router is approaching its capacity. The mplsNumVrfSecIllegalLabelThreshExceeded threshold trap is used to detect configuration or security violations, such as a PE-CE interface mis-configuration or an attempted VPN break-in using spoofed labels.

The VPN model can be configured to generate alarms based on the condition of the VPN model or VPN Site model.

Model	Attribute	Alarms
MplsVpn	EnableVpnAlarms	04940405 (Minor)
		04940406 (Major)
		04940407 (Critical)
		04940422 (Maintenance)
MplsSite	EnableSiteAlarms	04940403 (Critical)

Model	Event Condition
MplsVpn	Initial, Maintenance, Minor, Major, Critical, Good
MplsSite	Initial, Down, Good

More information:

Configuring MPLS VPN Manager (see page 27)

Chapter 6: Troubleshooting

Common problems and solutions of MPLS VPN Manager are described in the following table.

Description	Solution
MPLS VPN Manager does not currently support the creation of a customer model or the entering of customer VPN information.	You can name a VPN with an associated customer name.
The condition of the VPN Site model may not be updated correctly.	Ensure that Port Polling is enabled in MPLS VPN Manager and that the connections between ports have been resolved by CA Spectrum. Additionally, traps may be used to determine the condition of a VPN Site. The device must be configured to send traps to CA Spectrum on behalf of interfaces and VPNs.
A VPN Site alarm is not cleared in cases where the network cable is unplugged and then plugged back in, even though traps are enabled. The mplsVrfIfUp trap is not being sent when the cable is plugged back into the router.	This is a Cisco IOS firmware issue. The mplsVrfIfUp trap is sent in other cases when a VPN Site goes back online (as when the interface is Administratively set to “down” and then back to “up” or when the interface is turned off and then on using Cisco IOS).
A description is added to the VRF configuration on a router after its associated VPN Site has been modeled by MPLS VPN Manager. When you view information for the site in MPLS VPN Manager, the new description is not displayed in either the Description column of a site search Results list or in the Description field of the Component Detail panel's General Information section.	Destroy the VpnSite model, then run a new VPN Discovery that models the site. MPLS VPN Manager then displays the VRF description where appropriate.
A VRF Path Trace will timeout with the error message Trace Failed.	Increase the Path Trace Timeout value.

Description	Solution
MPLS VPN Manager does not create VpnSite models for each unique VRF entry on Juniper M-Series devices running JUNOS 8.2 R1.7.	Upgrade to JUNOS 8.2 R2.4 or later.
The current implementation creates only a single test model for each source site. This could lead to latency problems (at high site counts) because each test takes a fixed amount of time (typically 5 seconds). With a default poll time of 1200 seconds the system would support approximately 240 sites / vpn. In such cases the number of ping failures might change from one poll cycle to the other.	Increase the VRF Poll interval based on the number of destination sites

Index

T

U

V