CA Spectrum® Infrastructure Manager

Enterprise VPN Manager User Guide

r9.2

CA Product References

This guide references CA Spectrum® Infrastructure Manager (CA Spectrum).

Contact CA

Contact Technical Support

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

- 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

Provide Feedback

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

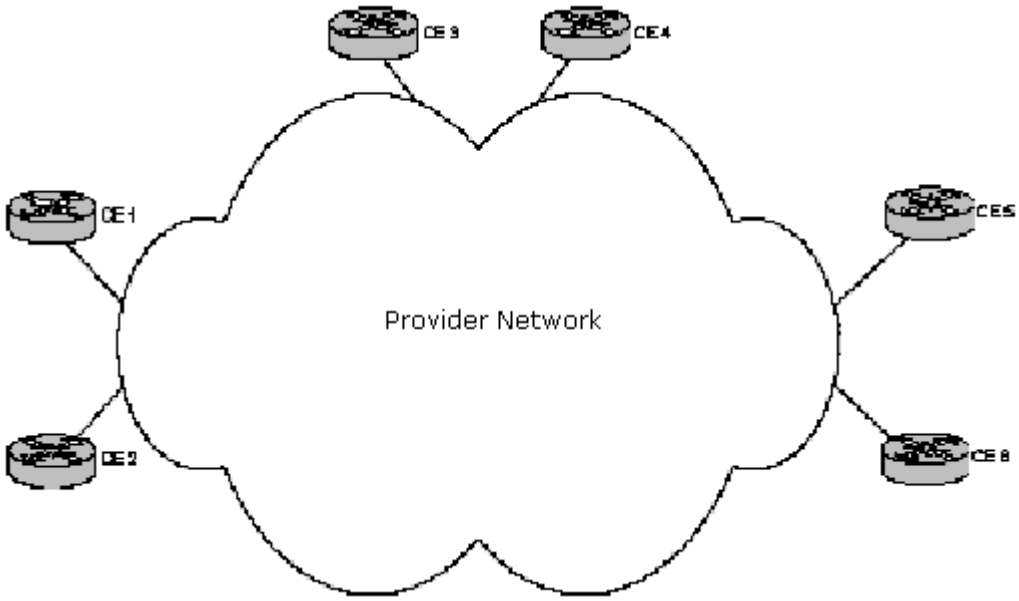
If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.

Contents

Chapter 1: Introduction

Enterprise VPN Manager is a CA Spectrum OneClick application that lets you discover, model, and monitor a provider-provisioned VPN network. As an enterprise customer, your network commonly ends at your customer edge (CE) devices. When you do not have access to provider core (P) or provider edge (PE) routers, you can infer service health by looking at the behavior at the edges of the provider network, where enterprise customer CE devices exist.

The following diagram shows a typical provider-provisioned VPN network from an enterprise customer perspective.



Once you have modeled the links and devices (CE routers) connected to a service provider using the Enterprise VPN Manager discovery, manual modeling, or import functionality, the Enterprise VPN Manager continuously monitors the health and service delivered by a service provider. The Provider_Cloud model represents the service provided to you by a service provider. Outage events are processed and rolled-up into the health of the service provider which is reflected on the Provider_Cloud model. Outage events are detected by actively polling CE routers for availability and by polling the status of interfaces on CE routers which are connected to a service provider. Enterprise VPN Manager can discover, model, and monitor Layer 3 Multiprotocol Label Switching (MPLS) VPN networks. In addition, it can also model (manually or by importing the information) and monitor Layer 2 Virtual Private LAN Service (VPLS).

In addition to active polling, Service Assurance (SA) Ping tests can be provisioned to monitor service delivery and compliance with response time service level agreements (SLAs). Ping tests offer the strongest option for service monitoring since they are end to end rather than just focused on a single resource (a device or interface).

Note: All elements connected to a given service provider must be modeled on a single SpectroSERVER.

Access Enterprise VPN Manager

You can access the Enterprise VPN Manager in the OneClick Navigation panel. Expand the appropriate landscape in the Explorer tab and select Enterprise VPN Manager.

Model information is displayed in the Contents and Component Detail panels.

Chapter 2: Discovery and Modeling

The Provider_Cloud model represents the service offered to you by a service provider. Enterprise VPN Manager offers several methods to model network entities and services, such as discovery, import, and manual modeling functionality to accommodate the unique needs of your enterprise.

This section contains the following topics:

Existing Device Models Upgrade

If you already have CE devices with BGP4_App modeled in CA Spectrum, you can run Enterprise VPN discovery to detect the device's connections to the service provider. If you do not have BGP4_App models on your CE devices, you can delete and remodel the devices or run Application Reconfiguration on those devices. Once the necessary application models are present, you can run Enterprise VPN Discovery.

Add Autonomous System Numbers (ASNs) to the CA Spectrum Database

By default, CA Spectrum includes over two thousand officially registered Service Provider ASNs. You can add additional Service Provider ASNs to the CA Spectrum database with the Model Type Editor by modifying the ASNamesList attribute of the EntVpnManager model type.

Note: For more information about editing model type attributes, see the *Model Type Editor User Guide.*

Enterprise VPN Discovery Prerequisites

Before using the Enterprise VPN Manager Discovery functionality, you must first model the physical components of your network in CA Spectrum. CA Spectrum discovers and models the physical network infrastructure through Discovery, manual modeling, or the Modeling Gateway.

Note: For information about modeling your network see the *Modeling and Managing Your IT Infrastructure Administrator Guide* and the *Modeling Gateway Toolkit Guide*.

Your CE routers must be modeled in CA Spectrum.

Your CE routers must have BGP peering to the service provider properly configured. If your devices do not support BGP peering, Enterprise VPN Manager supports import from a CSV text file based on Autonomous System Numbers (ASN) and manual modeling.

More information:

Import Peer/Provider Information (see page 16)
Model Service Provider Manually (see page 18)

Access Enterprise VPN Discovery Configurations

The Enterprise VPN Discovery subview contains discovery controls and configurations.

To access Enterprise VPN Discovery

1. Expand the appropriate landscape in the Explorer tab of the Navigation panel. Select Enterprise VPN Manager.

   Information and configurations display in the Information tab of the Contents panel.

2. Expand the Configuration subview then expand the Enterprise VPN Discovery subview.

   The Enterprise VPN Manager Discovery options display:

   - Run Discovery
   - Import Config File
   - Provider Name Filter Type
   - Provider Name Filter
   - Discover On Activation
   - Create On Trap
   - Enable Background Discovery
   - Background Discovery Interval (minutes)
   - ASN Mapping

More information:

Configure Enterprise VPN Manager to Run Discovery upon Model Activation (see page 12)
Configure Enterprise VPN Manager to Run Discovery when it Receives a bgpEstablished Trap (see page 12)
Enable Background Discovery (see page 13)
Configure the Background Discovery Interval (see page 14)
Run an On-demand Enterprise VPN Discovery (see page 14)
Filter Service Provider Names During Discovery (see page 15)
Map Multiple Autonomous System Numbers to a Single Provider (see page 35)

Configure Enterprise VPN Manager to Run Discovery upon Model Activation

You can configure Enterprise VPN Manager to automatically discover provider networks and CE interfaces using the Discover On Activation option. When Discover On Activation is set to Yes, an Enterprise VPN discovery is initiated each time a device model is activated by CA Spectrum. This could happen on initial device model creation or a SpectroSERVER restart. You should determine whether this processing load (during these times) is appropriate in your environment. If this behavior is not desired, this attribute should be set to No.

To access and change the Discover On Activation attribute

1. Expand the Enterprise VPN Discovery subview as described in Access Enterprise VPN Discovery Configurations.

   Enterprise VPN Discovery options and configurations display.

2. Click set next to Discover On Activation. Select Yes to enable or No (default) to disable.

   Discover On Activation is set. The value you selected is displayed next to Discover On Activation.

More information:

Access Enterprise VPN Discovery Configurations (see page 11)

Configure Enterprise VPN Manager to Run Discovery when it Receives a bgpEstablished Trap

Several devices configured with BGP4_App send a bgpEstablished trap when it establishes connection (a new peering session). You can configure Enterprise VPN Manager to automatically discover provider networks and CE interfaces whenever it receives a bgpEstablished trap. When Create On Trap is set to Yes, an Enterprise VPN discovery is initiated each time a bgpEstablished trap is received. The Create On Trap option offers an alternative to Background discovery. You should determine whether this discovery option is appropriate in your environment. If this behavior is not desired, this attribute should be set to No.

To configure Enterprise VPN Manager to create a model when it receives a trap from a new device

1. Expand the Enterprise VPN Discovery subview as described in Access Enterprise VPN Discovery Configurations.

   Enterprise VPN Discovery options and configurations display.

2. Click set next to Create On Trap and select Yes.

   Enterprise VPN Manager will run discovery when it receives a bgpEstablished trap.

More information:

Access Enterprise VPN Discovery Configurations (see page 11)

Enable Background Discovery

You can configure Enterprise VPN Manager to automatically discover provider networks and CE interfaces using the Background Discovery option. When Enable Background Discovery is set to Yes, an Enterprise VPN discovery is initiated based on the Background Discovery Interval. This lets you to determine the frequency of recurrence that is appropriate for your network. You should determine whether this processing load (during these time) is appropriate in your environment.

To enable background discovery

1. Expand the Enterprise VPN Discovery subview as described in Access Enterprise VPN Discovery Configurations.

   Enterprise VPN Discovery options and configurations display.

2. Click set next to Enable Background Discovery and select Yes.

   Background discovery is enabled and will recur depending on the frequency you set in Background Discovery Interval.

Configure the Background Discovery Interval

If you enable background discovery, you can configure the frequency in which background discovery will recur. For the value you set in the Background Discovery Interval to take effect, Enable Background Discovery must be set to Yes.

To configure the background discovery interval

1. Expand the Enterprise VPN Discovery subview as described in Access Enterprise VPN Discovery Configurations.

   Enterprise VPN Discovery options and configurations display.

2. Click set next to Background Discovery Interval, enter your value (in minutes), and press enter.

   The background discovery interval is set.

More information:

Access Enterprise VPN Discovery Configurations (see page 11)
Enable Background Discovery (see page 13)

Run an On-demand Enterprise VPN Discovery

Enterprise VPN Discovery is the simplest method of modeling your network. Before running an on-demand Enterprise VPN Discovery, you must meet the prerequisites.

To run an on-demand Enterprise VPN Discovery

1. Expand the Enterprise VPN Discovery subview (see page 11).

   Enterprise VPN Discovery options and configurations display.

2. Click Run.

   The Enterprise VPN Discovery runs, and Discovery status is displayed in the window next to the Run button.

More information:

Enterprise VPN Discovery Prerequisites (see page 10)
Access Enterprise VPN Discovery Configurations (see page 11)

Run Enterprise VPN Discovery on Selected Models

You can configure the Enterprise VPN Network Services Discovery from the OneClick views that display models.

To run Enterprise VPN Network Services Discovery on selected models

1. Select the models.
2. Click Tools, Utilities, Network Services Discoveries, Enterprise VPN Discovery.

   The Discovery process is initiated. You can check the status in the Configuration subview.

Configuring Enterprise VPN Discovery During Modeling

CA Spectrum lets you configure Network Services Discoveries, including Enterprise 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 Administration Guide*.

Filter Service Provider Names During Discovery

The Enterprise VPN Manager lets you filter the Service Provider names during Discovery run.

To filter the Service Provider Names

1. Select Enterprise VPN Manager in the Explorer tab.
2. Select the Information tab in the Contents panel.

   The configuration options for Enterprise VPN Manager display.

3. Expand the Enterprise VPN Discovery subview.

   The Discovery options are available, including these options:

   Provider Name Filter Type

   Determines if the Provider names in the 'Provider Name Filter' field are included or excluded from modeling. Options include the following:

   - Exclusive
   - Inclusive

   Provider Name Filter

   Lists the Service Provider names to be included or excluded when the Enterprise VPN Discovery is run. This field is used together with the 'Provider Name Filter Type' field.

   Note: The Service Provider names are not filtered and saved if you do not add them in the Provider Name Filter. So, even if the Provider Name Filter Type is inclusive and the Provider Name Filter is empty, all Provider Names are discovered.

More information:

Access Enterprise VPN Discovery Configurations (see page 11)

Import Peer/Provider Information

Enterprise VPN Manager enables you to import service provider information from MPLS and VPLS VPNs to create Provider_Cloud models. Import lets you to associate your Provider_Cloud models with sites if BGP peering is not used to communicate with your provider. The import file must be in a comma separated value (CSV) formatted file. You can create a CSV formatted file with a text editor or export from another application if the format complies with CSV formatting. Import requires that you know the service provider ASN and the IP Address for MPLS VPNs or the Interface Model Name for VPLS VPNs of your sites CE Interfaces.

Devices and interfaces must be modeled in CA Spectrum prior to importing a CSV-formatted text file.

The following are the allowed parameters for a line entry in an import file:

ProviderASN,SiteIfIdentifier,ProviderName,Region,SiteName,SitePriority

ProviderASN

Specifies the Autonomous System Number of the provider. ProviderASN is required.

SiteIfIdentifier

Specifies the IP Address for MPLS VPNs or the Interface Model Name of the site interface for VPLS VPNs. SiteIfIdentifier is required.

ProviderName

Specifies the Name of the service provider.

Region

Lets the Alarm Domains be defined. This is helpful when users have regional responsibility. The following values are available:

- Unavailable = Unavailable
- Arin = United States and Canada
- Lacnic = Latin America
- Ripe = EMEA
- Afrinic = Africa
- Apnic = Asia Pacific

SiteName

Specifies the name of the Provider_Cloud model.

SitePriority

Specifies an integer from 1 to N where 1 represents the primary connection and 2 through N represent backup connections.

The following is an example of a CSV import file:

1234,138.42.14.143,ProvName,Lacnic,SiteName,3

To import peer/provider information

1. Expand the Enterprise VPN Discovery subview as described in Access Enterprise VPN Discovery Configurations.

   The Enterprise VPN Discovery options display.

2. Click Import.

   The Import File dialog appears.

3. Locate your import file and click Open.

   Your peer or provider information is imported.

More information:

Access Enterprise VPN Discovery Configurations (see page 11)

Model Service Provider Manually

Enterprise VPN Manager lets you model the connections to a provider's service manually. Manual modeling is an alternative method of modeling devices that do not support the BGP4_App MIB that is required to run Enterprise VPN discovery. Manually modeling the connections to your service provider requires significant time and maintenance.

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

To model a device manually

1. In the OneClick Universe Topology tab, click  in the Topology toolbar.

   The Select Model Type dialog appears.

2. In the All Model Types tab, select Provider_Cloud and click OK.

   The Create Model of Type dialog appears.

3. Fill in the appropriate information requested in the dialog and click OK.

   This model represents the provider's network.

4. Create models of your CE devices.

5. Select a CE model in the Topology view.

6. Select the Interfaces tab of the Component Detail panel.

7. Locate the interface that is connected to the provider.
8. Right-click the interface and select Start Connection.

   Return to the Universe Topology view and right-click the Provider_Cloud model and select Connect with <interfaceName>.

   This operation associates the CE router's interface with the provider. Repeat for each CE interface that needs to be manually connected to the provider.

Chapter 3: Service Monitoring Configuration

This chapter describes Enterprise VPN Manager's service monitoring configurations. Enterprise VPN Manager can gather information about your provided network by Pinging or Polling. Ping tests offer the strongest measurement of service health since Ping tests are end to end while port polling is focused on a single resource (a device or interface). There are some things to consider when using Ping tests since they place additional resource requirements on your network and equipment. Specifically, Ping tests require the following additional resources:

- Processing time in CA Spectrum
- Network bandwidth to set up the tests
- Processing time in the CE routers
- Network bandwidth to execute the tests

Despite the resource requirements of Ping tests, Ping tests provide a valuable addition to your management capabilities. CA recommends that test sites be chosen.

Note: You must have a Simple Network Management Protocol (SNMP) read or write community name to provision ping tests.

This section contains the following topics:

Polling Configuration

Polling serves as an alternative to Ping testing. Polling does not create as much of a network strain as Ping testing. You do not need a SNMP read/write community name to enable polling.

Port Polling

Enterprise VPN Manager uses the port status of the connected interfaces to update the condition of the Provider_Cloud model. If port polling is disabled, the condition of the Provider_Cloud model may not update. We recommend leaving port polling enabled (the default).

Note: Port polling polls all BGP sessions (active and inactive).

To enable Port Polling

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the Information tab.
3. Expand the Configuration subview.
4. Expand the Management Configuration subview.
5. Locate Enable Port Polling, click set, and select Yes.

   Port Polling is now enabled.

Peer Session Polling

You can configure Enterprise VPN Manager to poll the status of peer sessions. When Enable Peer Session Polling is set to Yes, Enterprise VPN Manager looks for changes to PeerState. The total number of operative and inoperative BGP peering sessions is used to compute the percent of peering failures. The percent of peering failures is evaluated when Enterprise VPN Manager determines the Provider_Cloud condition.

To enable peer session polling

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the Information tab.
3. Expand the Configuration subview.
4. Expand the Management Configuration subview.
5. Locate Enable Peer Session Polling and click set.
6. Select Yes to enable peer session polling.

More information:

Provider_Cloud Condition (see page 32)

Ping Test Requirements

The following requirements must be performed (in order) for Enterprise VPN Manager to conduct Ping tests:

- Devices must support Cisco RTTMON MIB or RFC2925.
- Devices must be modeled with a read/write community name.

You must configure at least one site as:

- Ping from Site.
- Ping to/from Site.

You must configure at least one (other) site as:

- Ping to Site.
- Ping to/from Site.
- Ping Test Interval, Ping Test Timeout, and Response Time Threshold must be set to appropriate values.
- Enable Ping Tests on each Provider_Cloud model participating in the ping must be set to Yes.
- Enable Ping Tests on the Enterprise VPN Manager model must be set to Yes.

More information:

Configure Ping Tests (see page 24)
Configure Ping Source and Destination (see page 24)
Enable or Disable Ping Tests (see page 26)

Ping Test Scalability

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. Enterprise VPN Ping tests are disabled by default. 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 enterprise 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 Ping Source and Destination (see page 24)

Configure Ping Tests

Enterprise VPN Manager enables you to configure ping tests.

To access ping test configurations

1. Access Enterprise VPN Manager.
2. Select the List tab in the Content panel and select the Provider_Cloud model.
3. Select the Information tab in the Component Detail panel and expand the Ping Test Configuration subview.

   The following Ping test configurations are available:

   Ping Test Interval (sec)

   Determines how often pings are sent. To reduce network traffic, set this to a higher value.

   Default: 1200 seconds

   Note: Significantly lower values of the Ping Test Interval attribute may cause a severe performance impact to networks and routers.

   Ping Test Timeout (sec)

   Sets the time-out value before an event is generated for Ping tests.

   Default: 5 seconds

   Response Time Threshold (ms)

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

   Default: 250 milliseconds

Configure Ping Source and Destination

Remote sites typically communicate more efficiently with a central location than with each other. You can configure which interfaces send and receive ping. By default, interfaces are set to Ping from Site. Therefore, no pinging occurs until at least one interface is set to either Ping to Site or Ping to/from Site.

There are four possible values for Ping:

Ping Disabled

Indicates that ping is not enabled for this interface.

Ping from Site

Indicates that this interface can only originate a ping.

Ping to Site

Indicates that this interface can only receive a ping.

Ping to/from Site

Indicates that this interface can originate and receive a ping.

To configure Ping source and destination

1. Select the appropriate Provider_Cloud model to change all relevant interfaces or select an individual Interface model to make an individual change.
2. Open the Attribute Editor.
3. In the left panel of the Attribute Editor dialog, next to the User Defined folder, click add.

   The Attribute Selector dialog appears.
4. In the left panel of the Attribute Selector, select the Port folder.
5. In the right panel of the Attribute Selector, locate and select the PingTestEnable attribute and click OK.

   PingTestEnable is now displayed in the right panel of the Attribute Editor.
6. Select the appropriate value in the PingTestEnable drop-down list.

   Click OK.

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

Collapse BiDirectional Ping

Collapsing BiDirectional pings reduces network traffic by eliminating potentially redundant ping tests. If one site can receive responses from another, then the network between them functions properly, and there is no need to provision a test in the opposite direction. The default value of Collapse BiDirectional Ping is yes.

To collapse BiDirectional pinging

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the Information tab.
3. Expand the Configuration subview.
4. Set the value of Collapse BiDirectional Ping to Yes.

Enable or Disable Ping Tests

Since Ping tests involve additional resource requirements on your network and equipment, Ping tests are disabled by default. Ping tests are not conducted until:

- Ping source and destination for all Interfaces participating in the ping is configured
- Enable Ping Tests is set to Yes for each Provider_Cloud participating in the Ping test
- Enable Ping Tests is set to Yes on the Enterprise VPN Manager model

To enable or disable ping tests on the Enterprise VPN Manager model

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the Information tab.
3. Expand the Configuration subview.
4. Expand the Ping subview.
5. Set the value of Enable Ping Tests to Yes to enable ping testing. The default value is No.

To enable or disable ping tests on a Provider_Cloud model

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the List tab.
3. Select the appropriate Provider_Cloud model.
4. In the Component Detail panel, select the Information tab.
5. Expand the Ping Test Configuration subview.
6. Set the value of Enable Ping Tests to Yes to enable ping testing. The default value is No.

More information:

Ping Test Requirements (see page 23)

Enable Device Alarms

You can configure Enterprise VPN Manager to create an alarm when a peering session fails. When Enable Device Alarms is set to Yes, Enterprise VPN Manager creates a minor alarm when a device looses its BGP peer session with its provider. Devices must be configured with redundant links for Enterprise VPN Manager to detect when a BGP peer session is lost.

To enable device alarms

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the Information tab
3. Expand the Configuration subview.
4. Expand the Management Configuration subview.
5. Locate Enable Device Alarms, click set and select Yes to enable alarms on devices.

Chapter 4: Manage Provided VPN Services

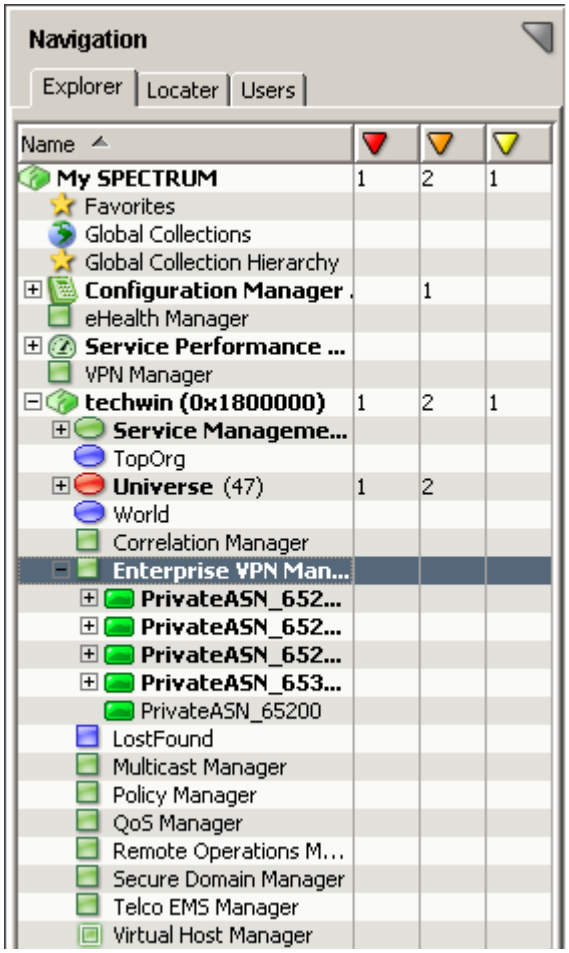
Enterprise VPN Manager enables you to continuously monitor the service provided to you by your service provider. Once service monitoring is enabled, you can see events and alarms pertaining to the health of various sites as well as the overall health of your provider. Enterprise VPN Manager enables you to monitor the service across the three hierarchal levels (Enterprise VPN Manager model, Provider_Cloud model, and the individual interface/site models) of your provided network

This section contains the following topics:

Enterprise VPN Manager Navigation

The OneClick Navigation panel displays a hierarchal view of your provided network. The Enterprise VPN Manager model exists within a particular landscape.

By expanding the Enterprise VPN Manager model, you can see your providers and the sites connected to your providers, as shown in the following image:



Conduct an Enterprise VPN Search

You can access Enterprise VPN searches through the Locator tab. The Enterprise VPN search results, which appear in the Contents tab, help you access views that present management, performance, and configuration information. The Component Detail panel displays detailed information about the device selected in the Contents panel. The following Enterprise VPN searches are available:

- All CE Devices by Provider
- All CE Interfaces by Provider
- All Enterprise VPN Managers
- All Providers

View Provider_Cloud Topology

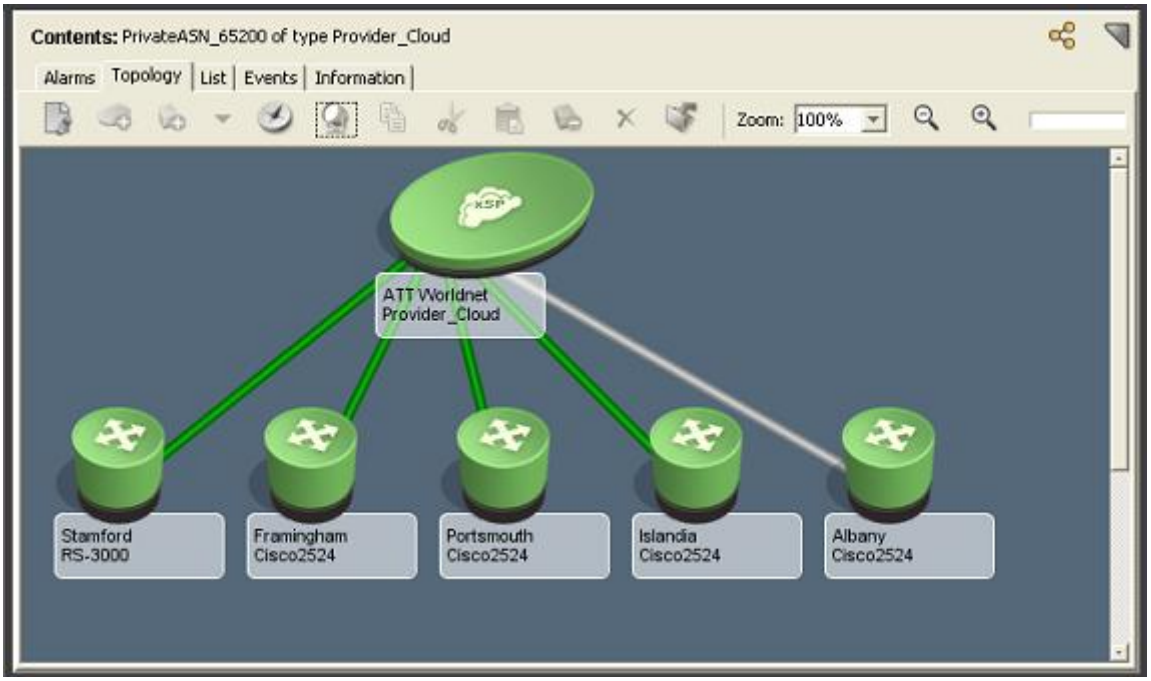
The Provider Topology view displays the CE devices connected to a Provider_Cloud model. Selecting the Provider_Cloud or an interface model icon displays model information in the Component Detail panel.

Note: For more information about the Component Detail panel, see the *Operator Guide.*

To access the Provider Topology view

1. Select the appropriate landscape from the Explorer tab in the OneClick Navigation panel.
2. Expand the Enterprise VPN Manager subview.
3. Select the appropriate Provider_Cloud model.
4. Select the Topology tab in the Contents panel.

   The Provider Topology view will look like the following example:



More information:

Access Enterprise VPN Manager (see page 8)

View Events and Alarms

Events and Alarms generated on a selected Provider_Cloud model display in the Events tab and Alarms tab of the OneClick Contents panel.

Note: For more information about the Contents panel, see the *Operator Guide*.

Execute OnDemand Ping Test

Enterprise VPN Manager lets you provision an OnDemand Ping test between two sites. OnDemand Ping tests are a good way to troubleshoot connectivity between two sites without the resource requirements that are necessary to provision background Ping tests in a large environment.

To execute an OnDemand Ping test

1. Activate the Topology view for the appropriate Provider_Cloud model.
2. Click Select OnDemand Ping Start Point from the right-click menu of the interface model icon from which you would like to initiate the Ping test.
3. Click Ping test from <source_model_name> from the right-click menu of the interface model icon that is the destination of the Ping test. This starts the on-demand Ping test.

   The results of the Ping test appear in a dialog after the Ping test finishes.

Note: You may also execute an on-demand Ping test using interface models in the Navigation panel.

More information:

View Provider_Cloud Topology (see page 31)

Provider_Cloud Condition

The Enterprise VPN Manager provides you with information about the status or condition of a Provider_Cloud model using the following types of information:

- Condition of the interfaces connected to the Provider_Cloud
- Results of the automated service assurance tests (Ping and Response Time)

Important! In order for the VPN Manager's Provider_Cloud condition to successfully calculate, you must always verify that the Live Pipes field is enabled. Disabling the Live Pipes field causes the VPN condition to not update properly.

The total number of operative and inoperative BGP peering sessions is used to compute the percent of peering failures. The percent of peering failures is evaluated when Enterprise VPN Manager determines the Provider_Cloud condition.

Note: For more information on BGP peering sessions, see *Modeling and Managing Your IT Infrastructure Administrator Guide.*

The default thresholds are available in the Information tab of the Provider_Cloud model. The thresholds and their default value are:

- Critical Alarm Threshold % - 5%
- Major Alarm Threshold % - 3%
- Minor Alarm Threshold % - 1%

Provider_Cloud Roll-Up Condition

The aggregate condition of the interfaces computes the roll-up condition of the Provider_Cloud. For example if there are 100 interfaces (or sites) connected to a provider and 4 of those interfaces are unreachable by CA Spectrum the condition is calculated as follows:

4 of 100 interfaces (4%) are unreachable

This provider has a condition of Major Alarm since the 4% outage is above the default Major Alarm Failure threshold of 3%.

Service Assurance Test

Automated service assurance tests provide the best indication of provider health. These tests assure not only that the interface and the BGP peering session is operating but that the endpoints are able to pass traffic. An additional test verifies that the traffic passing through the provider's network can reach the endpoint within the time thresholds specified in the service agreement.

Hide Symptomatic Alarms

Hiding symptomatic alarms reduces the number of alarms presented to you. You can configure Enterprise VPN Manager to generate a single alarm when a percentage of your interfaces connected to a service provider lose connectivity. When a significant number of sites are experiencing problems at the same time it is likely that the provider is the root cause. The Minor Alarm Threshold is a point where Enterprise VPN Manager suppresses multiple site alarms and instead generates an alarm on the Provider_Cloud model.

For example, you model a network with ten CE devices connected to a Provider_Cloud model with the alarm thresholds set as follows (these settings are unusually high and not recommended for operational use):

- Critical Alarm Threshold %: 35
- Major Alarm Threshold %: 25
- Minor Alarm Threshold %: 15

When one CE device (10% of the devices connected to the service provider) becomes unreachable by CA Spectrum, a red alarm is raised on the device model and the condition of the Provider_Cloud model remains green. The condition of the Provider_Cloud model remains green because 10% is less than the 15% Minor Alarm Threshold. When a second CE device (20%) becomes unreachable, the Minor Alarm Threshold is violated. The condition of the Provider_Cloud model is Minor Alarm and the alarms on the device models are hidden. The condition of the two unreachable devices remain critical but no Contact Lost alarms appear in the alarm log.

To hide symptomatic alarms

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the List tab.
3. Select the appropriate Provider_Cloud model.
4. In the Component Detail panel, select the Information tab.
5. Expand the Configuration Information subview.
6. Specify the following thresholds:

   Critical Alarm Threshold (%)

   Specifies the threshold for hiding Critical alarms.

   Default: 5

   Major Alarm Threshold (%)

   Specifies the threshold for hiding Major alarms.

   Default: 3

   Minor Alarm Threshold (%)

   Specifies the threshold for hiding Minor alarms.

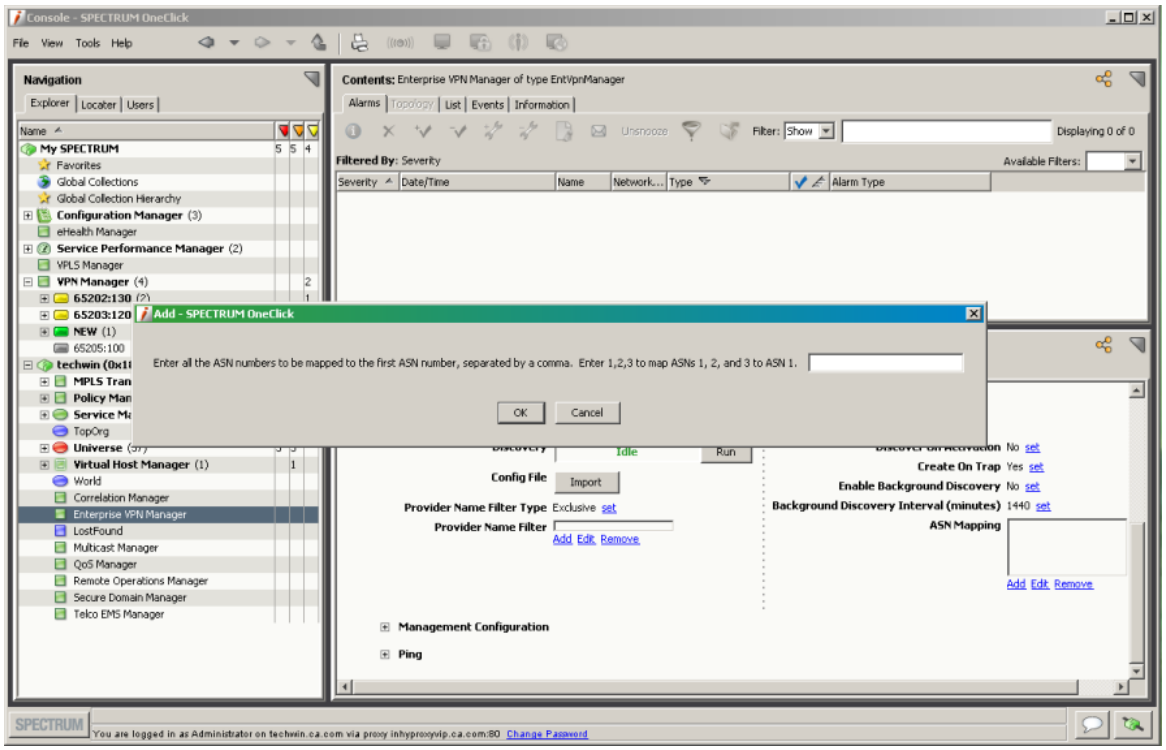
   Default: 1
7. Select the Impact tab.
8. Expand the Symptoms subview.

   You can view the affected device sites.

Map Multiple Autonomous System Numbers to a Single Provider

CA Spectrum's MultipleASNLists attribute is now a list rather than a text string. This lets you easily map multiple Autonomous System Numbers (ASNs) to a single provider.

This is available by selecting Configuration from the Enterprise VPN Manager and then editing the ASN Mapping field. CA Spectrum displays a List Renderer that lets you easily add, edit, or remove each list of ASNs that are mapped to the first ASN in the list, as shown in the following image:



Appendix A: Enterprise VPN Manager Events

The Enterprise VPN Manager events enhance management of provider based services. The majority of these events mirror the roll-up and service assurance methods of provider condition calculation.

This section contains the following topics:

Roll-Up Method

The events in the roll-up method approach reflect the health of the service provider, which is modeled using the Provider_Cloud model type. The supported events are:

Event	Event ID	Description
InitialEvent	0x5180400	Provider is Initial
MinorEvent	0x5180401	Provider is Minor (% sites down)
MajorEvent	0x5180402	Provider is Major (% sites down)
CriticalEvent	0x5180403	Provider is Critical (% sites down)
GoodEvent	0x5180404	Provider is Good (all sites up)
MinorAlarmEvent	0x5180405	Provider Minor Alarm (% sites down)
MajorAlarmEvent	0x5180406	Provider Major Alarm (% sites down)
CriticalAlarmEvent	0x5180407	Provider Critical Alarm (% sites down)

Service Assurance Method

There are a number of events generated using this condition calculation method. They can be classified in several ways:

Scope

- Single test between a Pair of Sites
- Tests from a Site to all its Destinations
- Tests from all Sites to all their Destinations connected to the Provider

Test Type

- Connectivity (Did the Ping Succeed)
- Response Time (Did the Ping Succeed within the threshold)

Test Phase

- Test Model Creation
- Test Setup
- Ping Test Operation
- Response Time Threshold

Test Phases

Events may occur at each phase of test creation, setup or execution. The results reported attempt to determine the most likely root cause rather than events caused by other events. An example of this is shown in the following test phases:

1. Test Model Creation
2. Test Setup
3. Ping Test Operation
4. Response Time Threshold

Each successive test phase builds on the previous one. For example, if the Test Model cannot be created, none of the other phases are attempted. Therefore, the user sees a Test Creation Event (SingleTestCreateFailed) instead of multiple Ping Failure and Response Time Failure events (and alarms). The same is true for the Ping Test Operation and Response Time Threshold phases. If the Ping connectivity test fails (the timeout is 5 seconds) a Response Time failure is not reported. The default value for critical Response Time threshold is 250 milliseconds. Conversely it is possible for the Ping test to succeed but the Response Time threshold to fail. The event sequence may show:

Event	Event ID
SinglePingTestGood	0x5180604
SingleRTThreshFailed	0x5180607

Assume you manage 100 sites and have modified the values of the Ping thresholds to 5, 10 and 20 percent for the minor, major and critical thresholds, respectively. Next assume that 21% of the Ping tests from a site fail. A critical alarm is raised because it exceeds the value of the critical alarm threshold. There are 79 tests that have succeeded. Of these remaining successful ping tests, there are 9 Response Time threshold violations. The calculation is done using 9 of 79 tests leading to a failure rate of 11%; this is a major alarm condition because it exceeds the major alarm threshold. The event sequence which is displayed in this case is:

Event	Event ID
SiteTotalPingTestsCritical	0x5180621
SiteTotalRTThreshMajor	0x5180624

The example demonstrates how the success of each succeeding phase is dependent on the results of the previous phase. An event sequence can have the following events:

Event	Event ID
SiteTotalPingTestsGood	0x5180618
SiteTotalRTThreshCritical	0x5180625

More information:

Service Assurance Method (see page 38)

Single Test Between Sites

The following events may be generated for a single site-to-site test.

Event	Event ID	Description
SingleTestCreateGood	0x5180600	Individual test created successfully
SingleTestCreateFailed	0x5180601	Individual test creation failed
SingleTestSetupGood	0x5180602	Individual test setup succeeded
SingleTestSetupFailed	0x5180603	Individual test setup failed
SinglePingTestGood	0x5180604	Individual ping test succeeded
SinglePingTestFailed	0x5180605	Individual ping test failed
SingleRTThreshGood	0x5180606	Individual RT test succeeded
SingleRTThreshFailed	0x5180607	Individual RT test failed

The following tests are part of each event cycle:

- Ping Connectivity
- Ping Response Time

A Ping cycle can pass the Ping Connectivity test but fail the Response Time test when the ping response returns outside the specified response time window. In this case, the user sees SinglePingTestGood event followed by a SingleRTThreshFailed event.

Summary from One Site to All its Destinations

The following events may be generated for a test from a single site to all its destinations.

Event	Event ID	Description
SiteTotalCreatesGood	0x5180610	All of the site to site test created are good
SiteTotalCreatesMajor	0x5180612	Major % of site to site tests created failed
SiteTotalSetupsGood	0x5180614	All of the site to site test setups are good
SiteTotalSetupsMajor	0x5180616	Major % of site to site test setups failed
SiteTotalPingTestsGood	0x5180618	All of the site to site pings are good
SiteTotalPingTestsMinor	0x5180619	Minor % of site to site pings failed

Event	Event ID	Description
SiteTotalPingTestsMajor	0x5180620	Major % of site to site pings failed
SiteTotalPingTestsCritical	0x5180621	Critical % of site to site pings failed
SiteTotalRTThreshGood	0x5180622	All of the site to site RT thresholds are good
SiteTotalRTThreshMinor	0x5180623	Minor % of site to site RT thresholds violated
SiteTotalRTThreshMajor	0x5180624	Major % of site to site RT thresholds violated
SiteTotalRTThreshCritical	0x5180625	Critical % of site to site RT thresholds violated

Summary for All Sites to All Destinations in Provider

The following events may be generated for tests from all sites to all destinations in a provider.

Event	Event ID	Description
TotalTestCreatesGood	0x5180700	All Ping tests for provider created successfully
TotalTestCreatesMinor	0x5180701	Minor % of tests created for provider failed
TotalTestCreatesMajor	0x5180702	Major % of tests created for provider failed
TotalTestCreatesCritical	0x5180703	Critical % of tests created for provider failed
TotalTestSetupsGood	0x5180704	All Ping tests for provider setup successfully
TotalTestSetupsMinor	0x5180705	Minor % of test setups for provider failed
TotalTestSetupsMajor	0x5180706	Major % of test setups for provider failed
TotalTestSetupsCritical	0x5180707	Critical % of test setups for provider failed
TotalPingTestsGood	0x5180708	All Ping tests for provider executed successfully
TotalPingTestsMinor	0x5180709	Minor % of Ping tests for provider failed
TotalPingTestsMajor	0x5180710	Major % of Ping tests for provider failed
TotalPingTestsCritical	0x5180711	Critical % of Ping tests for provider failed
TotalRTThreshGood	0x5180712	All RT tests for provider executed successfully
TotalRTThreshMinor	0x5180713	Minor % of RT Threshold for provider violated

Event	Event ID	Description
TotalRTThreshMajor	0x5180714	Major % of RT Threshold for provider violated
TotalRTThreshCritical	0x5180715	Critical % of RT Threshold for provider violated
DevTestCreatesGood	0x5180800	All RT tests for provider executed successfully
DevTestCreatesMinor	0x5180801	Minor % of tests created for provider failed
DevTestCreatesMajor	0x5180802	Major % of test created for provider failed
DevTestCreatesCritical	0x5180803	Critical % of tests created for provider failed
DevTestSetupsGood	0x5180804	All Ping tests for provider setup successfully
DevTestSetupsMinor	0x5180805	Minor % of test setups for provider failed
DevTestSetupsMajor	0x5180806	Major % of test setups for provider failed
DevTestSetupsCritical	0x5180807	Critical % of test setups for provider failed
DevPingTestsGood	0x5180808	All Ping tests for provider executed successfully
DevPingTestsMinor	0x5180809	Minor % of Ping tests for provider failed
DevPingTestsMajor	0x5180810	Major % of Ping tests for provider failed
DevPingTestsCritical	0x5180811	Critical % of Ping tests for provider failed
DevRTThreshGood	0x5180812	All RT tests for provider executed successfully
DevRTThreshMinor	0x5180813	Minor % of RT Threshold for provider violated
DevRTThreshMajor	0x5180814	Major % of RT Threshold for provider violated
DevRTThreshCritical	0x5180815	Critical % of RT Threshold for provider violated

Index

S

T

V