Service Inventory > Inventory and Connection Manager

From the Home window of Cisco IP Solution Center (ISC), you receive upon logging in, click the **Service Inventory** tab and you receive a window, as shown in Figure 3-1, "Service Inventory Selections."

Figure 3-1 Service Inventory Selections

Click on **Inventory and Connection Manager** and a window as shown in Figure 3-2, "Inventory and Connection Manager Selections," appears.

Figure 3-2 Inventory and Connection Manager Selections

From **Inventory and Connection Manager**, you can navigate to any of the following functions:

- **Service Requests, page 3-3** Create, deploy, and manage Service Requests (SRs).
- **Traffic Engineering Management, page 3-5** Create, deploy, and manage elements of Traffic Engineering Management.
- **Inventory Manager, page 3-5** Bulk-manage inventory elements.
- **Topology Tool, page 3-5** View topology maps.
- **Devices, page 3-38** Create and manage Devices.
- **Device Groups, page 3-80** Create and manage Device Groups.
- **Customers, page 3-86** Create and manage Customers.
- **Providers, page 3-95** Create and manage Providers.
- **Resource Pools, page 3-102** Create and manage pools for IP address, Multicast address, Route Distinguisher, Route Target, Site of Origin, VC ID, and VLAN.
- **CE Routing Communities, page 3-114** Create and manage CE Routing Communities.
- **VPNs, page 3-117** Create and manage VPNs.
- **AAA Servers, page 3-121** Create and manage AAA Servers.
- **Named Physical Circuits, page 3-123** Create and manage Named Physical Circuits (NPCs).

Service Requests

Service Requests are explained in each of the *User Guides* for each of the licensed services.

Table 3-1, "Summary of Cisco IP Solution Center Service Request States," describes each ISC service request state. The states are listed in alphabetical order.

Table 3-1 Summary of Cisco IP Solution Center Service Request States

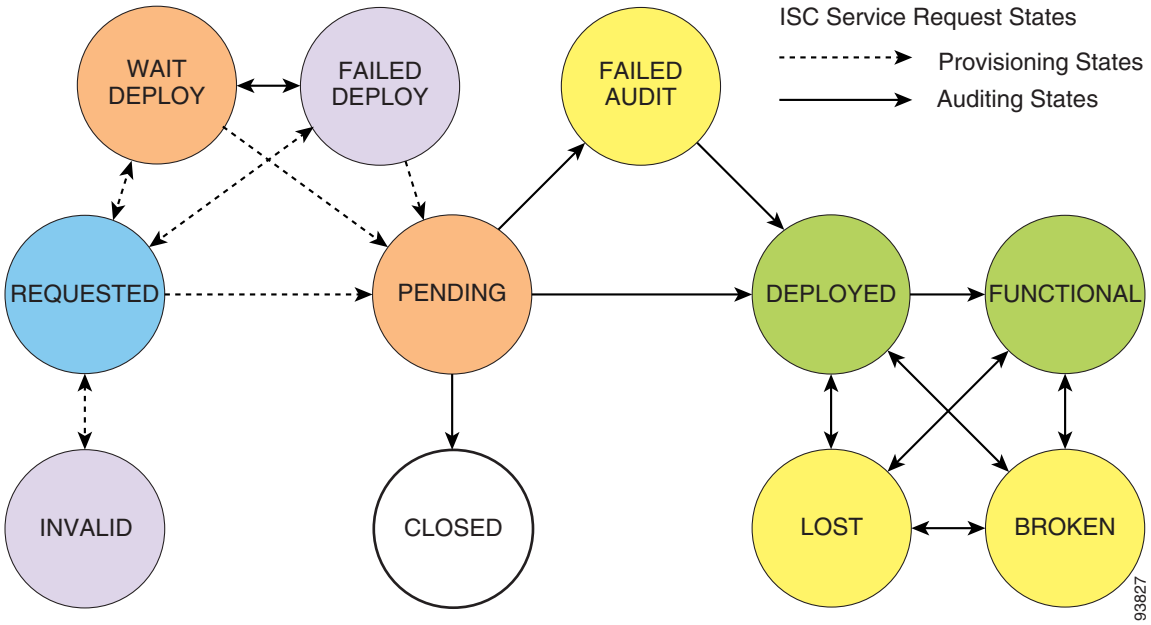
Service Request Type	Description
Broken	The router is correctly configured but the service is unavailable (due to a broken cable or Layer 2 problem, for example). An MPLS service request moves to **Broken** if the auditor finds the routing and forwarding tables for this service, but they do not match the service intent. An IPsec service request moves to **Broken** if a ping fails for all the remote peers of the current device. **- NOT SUPPORTED in this release. -**
Closed	A service request moves to **Closed** if the service request should no longer be used during the provisioning or auditing process. A service request moves to the **Closed** state only upon successful audit of a decommission service request. ISC does not remove a service request from the database to allow for extended auditing. Only a specific administrator purge action results in service requests being removed.
Deployed	A service request moves to **Deployed** if the intention of the service request is found in the router configuration file. **Deployed** indicates that the configuration file has been downloaded to the router, and the intent of the request has been verified at the configuration level. That is, ISC downloaded the configlets to the routers and the service request passed the audit process.
Failed Audit	This state indicates that ISC downloaded the configlet to the router successfully, but the service request did not pass the audit. Therefore, the service did not move to the **Deployed** state. The **Failed Audit** state is initiated from the **Pending** state. After a service request is deployed successfully, it cannot re-enter the **Failed Audit** state (except if the service request is redeployed).
Failed Deploy	The cause for a **Failed Deploy** status is that DCS reports that either the upload of the initial configuration file from the routers failed or the download of the configuration update to the routers failed (due to lost connection, faulty password, and so on).
Functional	An MPLS service request moves to **Functional** when the auditor finds the VPN routing and forwarding tables (VRF) for this service and they match with the service intent. This state requires that both the configuration file audit and the routing audit are successful. An IPsec service request moves to Functional when the auditor finds that the router is configured properly and the IPsec traffic is flowing (ping is used to determine if IPsec traffic is flowing). **- NOT SUPPORTED in this release. -**

Table 3-1 Summary of Cisco IP Solution Center Service Request States (continued)

Service Request Type	Description
Invalid	**Invalid** indicates that the service request information is incorrect in some way. A service request moves to **Invalid** if the request was either internally inconsistent or not consistent with the rest of the existing network/router configurations (for example, no more interfaces were available on the router). The Provisioning Driver cannot generate configuration updates to service this request.
Lost	A service request moves to **Lost** when the Auditor cannot find a configuration-level verification of intent in the router configuration files. The service request was in the **Deployed** state, but now some or all router configuration information is missing. A service request can move to the **Lost** state *only* when the service request had been **Deployed**.
Pending	A service request moves to **Pending** when the Provisioning Driver determines that the request looks consistent and was able to generate the required configuration updates for this request. **Pending** indicates that the service request has generated the configuration updates and the configuration updates are successfully downloaded to the routers. The Auditor regards pending service requests as new requests and begins the audit. If the service has been freshly provisioned and not yet audited, it is not an error (pending audit). However, if an audit is performed and the service is still pending, it is in an error state.
Requested	If the service is newly entered and not yet deployed, it is not an error. However, if a Deploy is done and it remains **Requested**, the service is in an error state.
Wait Deploy	This service request state pertains only when downloading configlets to a Cisco CNS-CE server, such as a Cisco CNS IE2100 appliance. **Wait Deploy** indicates that the configlet has been generated, but it has not been downloaded to the Cisco CNS-CE server because the device is not currently online. The configlet is staged in the repository until such time as the Cisco CNS-CE server notifies ISC that it is up. Configlets in the **Wait Deploy** state are then downloaded to the Cisco CNS-CE server.

Figure 3-3, "Service Request States Transition Diagram," shows the transitions of states.

Figure 3-3 Service Request States Transition Diagram



Traffic Engineering Management

Traffic Engineering Management allows you to create, deploy, and manage elements of Traffic Engineering Management. This is explained in detail in *Cisco IP Solution Center Traffic Engineering Management User Guide, 4.0.*

Inventory Manager

Inventory Manager enables an operator to import network specific data into the ISC Repository in bulk mode. Inventory Manager is explained in detail in Chapter 4, "Service Inventory > Inventory and Connection Manager > Inventory Manager".

Topology Tool

The topology tool provides a graphical view of networks set up through the ISC web client. It gives a graphical representation of the various physical and logical parts of the network, both devices and links.

Introduction

The topology tool includes three types of views:

- VPN view—shows connectivity between customer devices. The VPN view also gives an aggregate view of all services and individual logical and physical views of each of the services.
- Logical view—shows logical connections set up in a selected provider region
- Physical view—displays connectivity of named physical circuits in a provider region.

In addition, this chapter describes the following features:

- Filtering and Searching—filter out unnecessary detail in large graphs or jump straight to a particular device using the search tool
- Using Maps—associate maps with the individual views.

Please note that some details, such as window decorations, are system specific and might appear differently in different environments. However, the functionality should remain consistent.

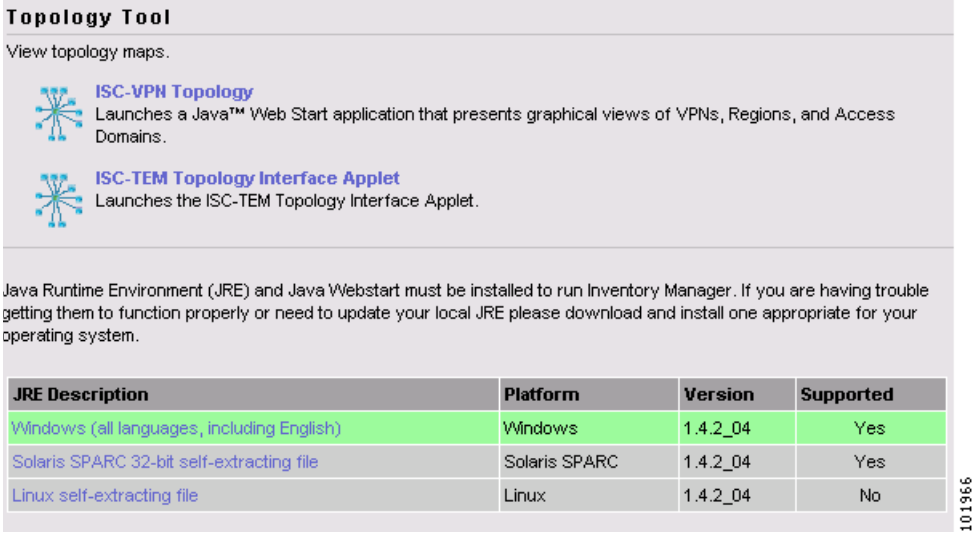
Launching Topology Tool

To launch the Topology Tool, follow these steps:

Step 1 Log into ISC.

Step 2 Navigate **Service Inventory > Inventory and Connection Manager > Topology Tool** and a window appears, as shown in Figure 3-4, "Topology Launch." If you do not have the proper Java Runtime Environment (JRE) as specified at the bottom of the window, click the corresponding link for your system, follow that path, then quit the browser, log in again, and navigate back to the Topology Tool page.

Figure 3-4 Topology Launch



Step 3 Click **ISC-VPN Topology** in Figure 3-4, "Topology Launch" to launch the Topology Tool application on the web client. This starts up the Java Web Start application.

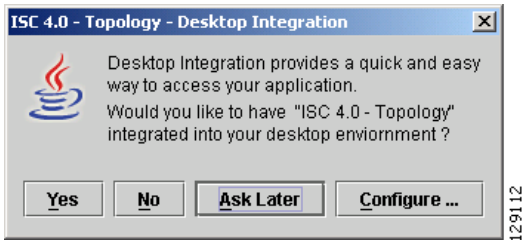
Note Name resolution is required. The ISC HTTP server host must be in the Domain Name System (DNS) that the web client is using or the name and address of the ISC server must be in the client host file.

Step 4 The first time Inventory Manager is activated, the Security Warning window in Figure 3-5 appears. Click **Start** to proceed or **Details** to verify the security certificate.

Figure 3-5 Security Warning

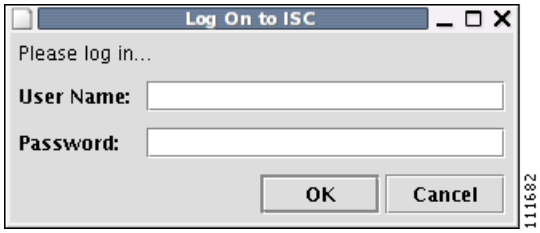
Step 5 The Desktop Integration window in Figure 3-6 appears. Click **Yes** to integrate into your desktop environment, click **No** to decline, click **Ask Later** to be prompted the next time VPN Topology is invoked, or click **Configure ...** to customize the desktop integration.

Figure 3-6 Topology Desktop Integration



The Login window in Figure 3-7, "Log On to ISC." appears whether or not a selection has been made in the Desktop Integration window.

Figure 3-7 Log On to ISC



Step 6 Enter your **User Name** and **Password** and click **OK**. The Topology Tool launches and connects to the Master ISC server.

Conventions

Topology software uses several conventions to visually communicate information about displayed objects. The shape and color of a node representing a device depends on the role of the device, as shown in Table 3-2:

Table 3-2 Device Role Shapes

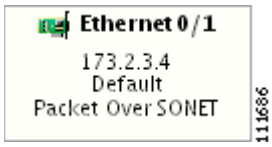
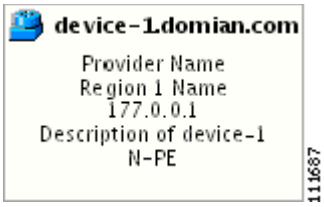
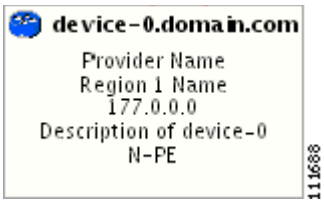
Shape	Description
	Green icon for a CAT OS customer device followed by the following information: - Device name - Customer Name - Site Name - Management IP Address - Description - Role (SPOKE or HUB of a VPN)
	Green icon for a router customer device followed by the following information: - Device name - Customer Name - Site Name - Management IP Address - Description - Role (SPOKE or HUB of a VPN)
	Green icon for a VPN 3000 customer device (**This feature is not supported in this device**) followed by the following information: - Device name - Customer Name - Site Name - Management IP Address - Description - Role (SPOKE or HUB of a VPN)
	Green icon for an interface followed by the following information: - Interface name - Management IP Address - Encapsulation Type - Interface Type

Table 3-2 Device Role Shapes (continued)

Shape	Description
	Blue icon for a CAT OS provider device followed by the following information: - Device name - Provider Name - Region Name - Management IP Address - Description - Role
	Blue icon for a router provider device followed by the following information: - Device name - Provider Name - Region Name - Management IP Address - Description - Role
	Blue icon for a region followed by the following information: - Region name - Provider Name
	Green icon for a site followed by the following information: - Site name - Customer Name - Role in which Site's device joined VPN (HUB, SPOKE, or combination of HUB and SPOKE)
	Green icon for a site followed by the following information: - Site name - Customer Name - Role in which Site's device joined VPN (HUB, SPOKE, or combination of HUB and SPOKE)

A distinct color scheme is used to highlight the link type as shown in Table 3-3:

Table 3-3 Link Type Color Scheme

Color	Connection Type
(green)	End-to-end wire
(purple)	Attachment circuit
(light blue)	IPsec tunnel (**IPsec is not supported in this release**.)
(brown)	MPLS VPN link

Finally, the four patterns shown in Table 3-4 are used to indicate the service request state:

Table 3-4 Link State Pattern Scheme

Pattern	Service Request State
	Deployed, functional, pending
	Failed audit, invalid, broken, lost
	Wait deploy, requested, failed deploy
	Closed

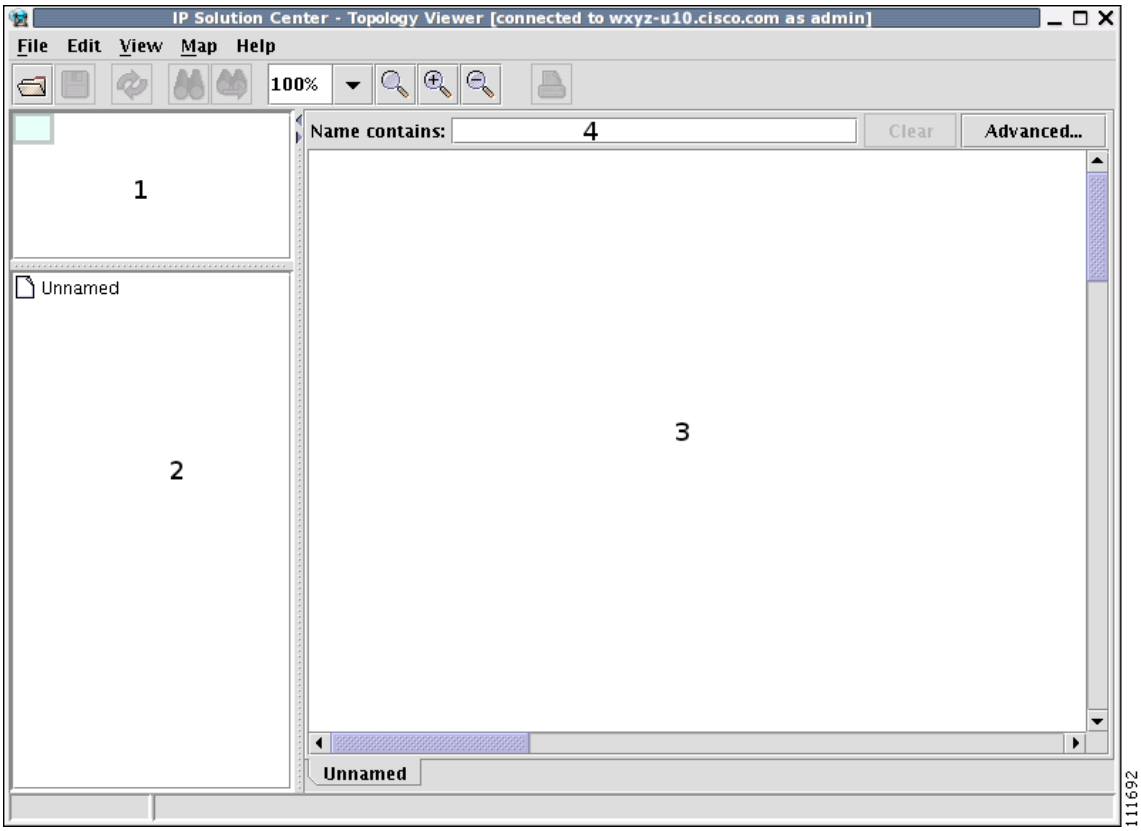
Accessing the Topology Tool for ISC-VPN Topology

Launch the Topology Tool as explained in Figure 3-4, "Topology Launch," in the "Launching Topology Tool" section on page 3-7 and then use the following steps to access the **ISC-VPN Topology** tool.

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Topology Tool > ISC-VPN Topology**.

The Topology window shown in Figure 3-8 appears.

Figure 3-8 Topology Application Window



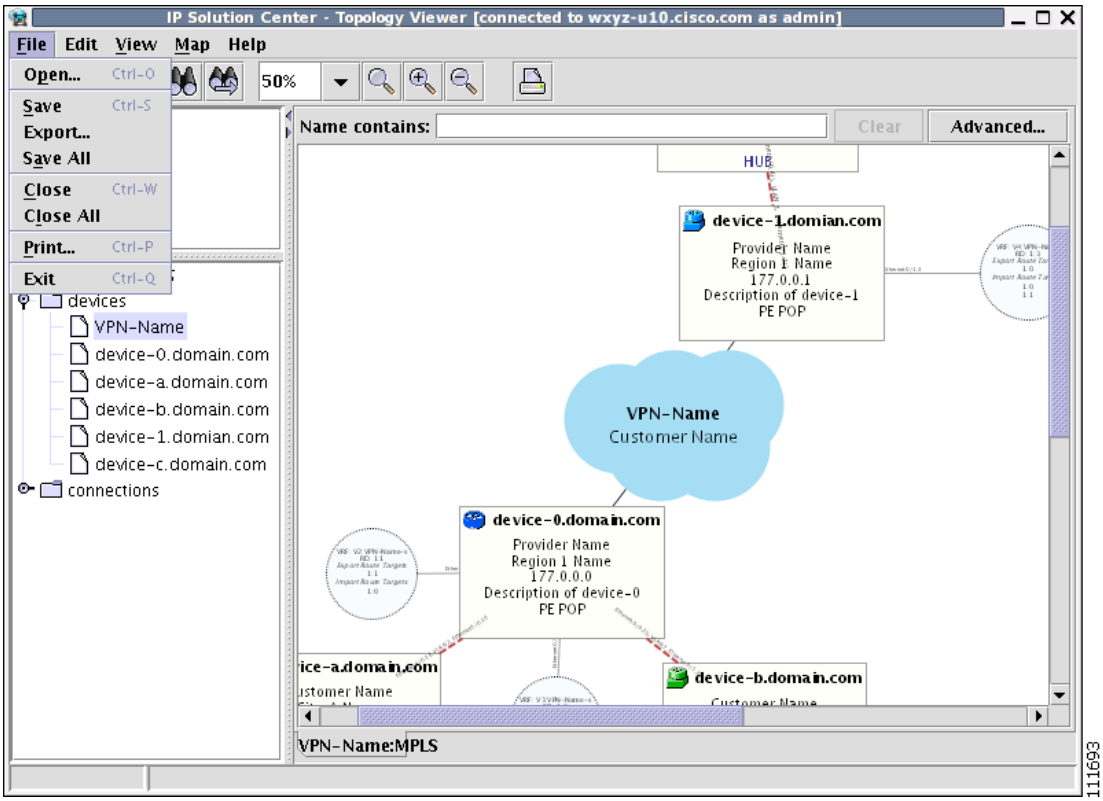
The application window is divided into four areas, as shown in Figure 3-8:

- area (1)—The top left corner shows the Overview area. The colored rectangular panel, called the panner, corresponds to the area currently visible in the main area. Moving the panner around changes the part of the graph showing in the main area. This is particularly useful for large graphs.
- area (2)—The bottom left area shows the Tree View of the graph. When no graph is shown, a single node called **Unnamed** is displayed. When a graph is shown, a tree depicting devices and their possible interfaces and connections is displayed. The tree can be used to quickly locate a device or a connection.
- area (3)—The main area (Main View) of the window shows a graph representing connections between devices. The name of the displayed network is shown at the bottom. When no view is present, the name defaults to **Unnamed**.
- area (4)—Above the main window is the Filter area. It allows you to filter nodes by entering a pattern. Nodes whose name contains the entered pattern maintain the normal level of brightness. All other nodes and edges become dimmed, as shown in Figure 3-30 and the "Filtering" section on page 3-30.

Note The bottom bar below all the areas, is a Status bar.

Views are loaded, saved, and closed using the **File** menu, as shown in Figure 3-9.

Figure 3-9 The File Menu



The **File** menu contains the following menu items:

- **Open**—Opens a view.
- **Save**—Saves the open and active view with the existing file name, if any.
- **Export...**—Exports the active view in either Scalable Vector Graphics (SVG), Joint Photographics Expert Group (JPG), or Portable Network Graphics (PNG) format.
- **Save All**—Saves all open views.
- **Close**—Closes the open and active view.
- **Close All**—Closes all open views.
- **Print...—**Prints the open and active view.
- **Exit**— Exits the Topology tool.

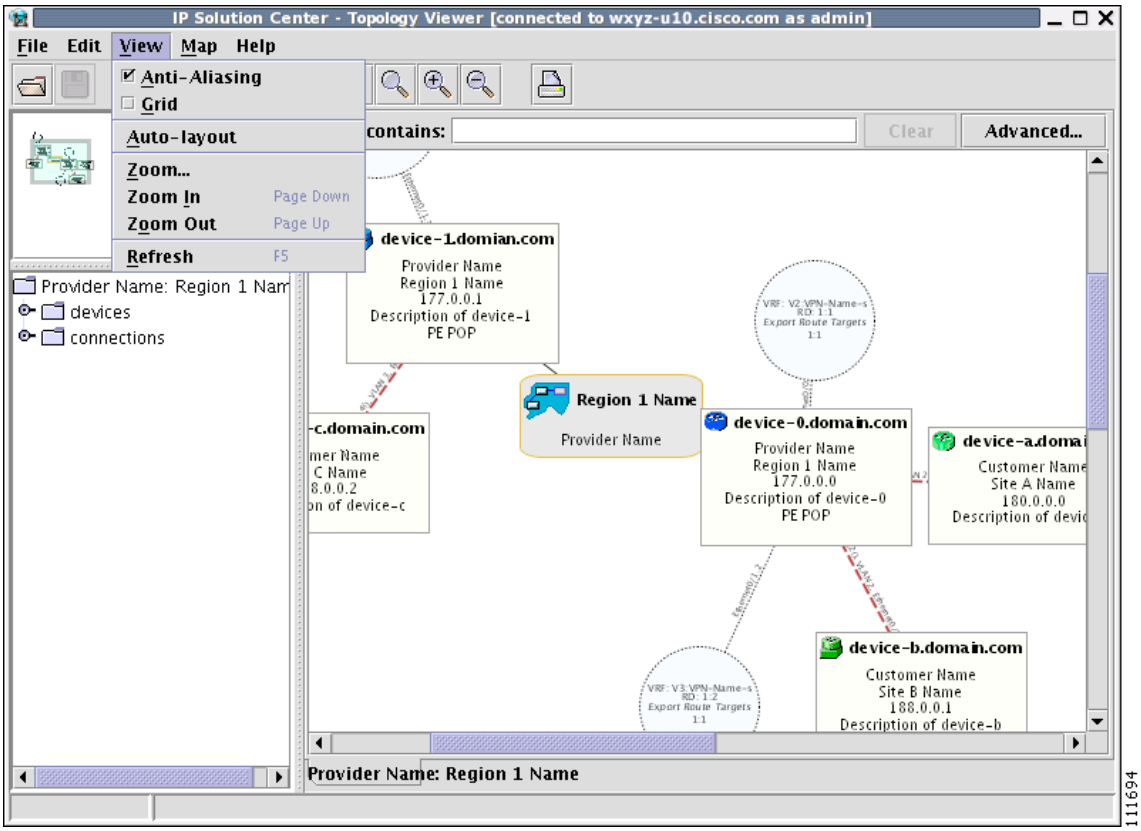
Types of Views

There are three view panes in the topology application and they are described in the following sections:

- VPN View, page 3-15, shows connectivity between devices in a VPN
- Logical View, page 3-19, shows connectivity between PEs and CPEs in a region
- Physical View, page 3-22, shows physical devices and links for PEs in a region.

The view attributes can be changed using the **View** menu, as shown in Figure 3-10.

Figure 3-10 The View Menu



The **View** menu contains the following menu items:

- **Anti-Aliasing**—When drawing a view, this creates smoother lines and a more pleasant appearance at the expense of performance.
- **Grid—**Activates a magnetic grid. The grid has a 10 by 10 spacing and can be used to help align nodes in a view.
- **Auto-Layout**—Generates an automatic layout of nodes in a view. If selected, the program tries to find the most presentable arrangement of nodes.
- **Zoom**—Opens a dialog where the desired magnification level can be specified.
- **Zoom In**— Increases the magnification level.
- **Zoom Out—**Decreases the magnification level.
- **Refresh—**Regenerates the view. This is especially useful if the data in the repository changes. To see an updated view, select **Refresh** or click the Refresh toolbar button.

VPN View

The VPN view shows connectivity between devices forming a given VPN. To activate the VPN view, use the following steps:

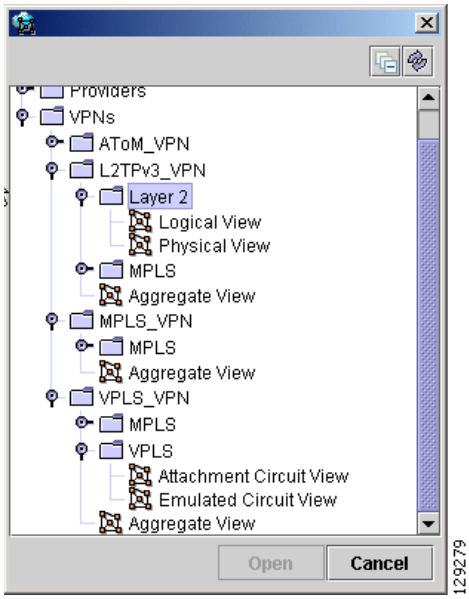
Step 1 In the menu bar, select **File** > **Open**.

or

click the **Open** button in the tool bar.

The Folder View window in Figure 3-11 appears displaying a directory tree with available VPNs.

Figure 3-11 Folder View



Step 2 Navigate to the desired VPN's folder, select the folder, and click **Open**. This opens the desired folder to display any logical and physical views associated with that VPN.

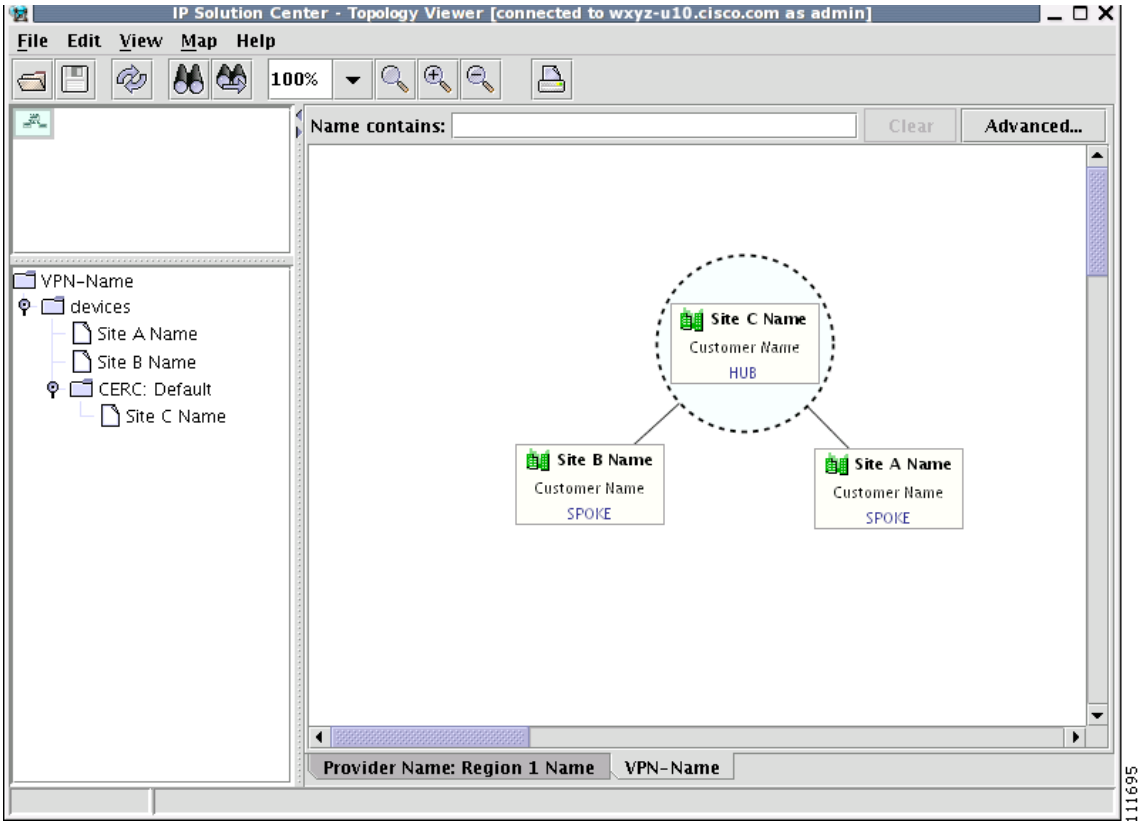
Step 3 Click a logical or a physical view item in the folder tree. The logical view minimizes the amount of detail and shows connectivity between customer devices. The physical view reveals more about the physical structure of the VPN. For example, for MPLS it shows connectivity between customer and provider devices and the core of the provider.

Aggregate View

The Aggregate View, as shown in Figure 3-12, "Aggregate View," shows connectivity between all customer devices, regardless of the type of technology used to connect them.

A single view might show a combination of MPLS, Layer 2, VPLS, and IPsec VPNs (**IPsec is not supported in this release**.). For MPLS and IPsec, only the Customer Premises Equipment devices (CPEs) are shown.

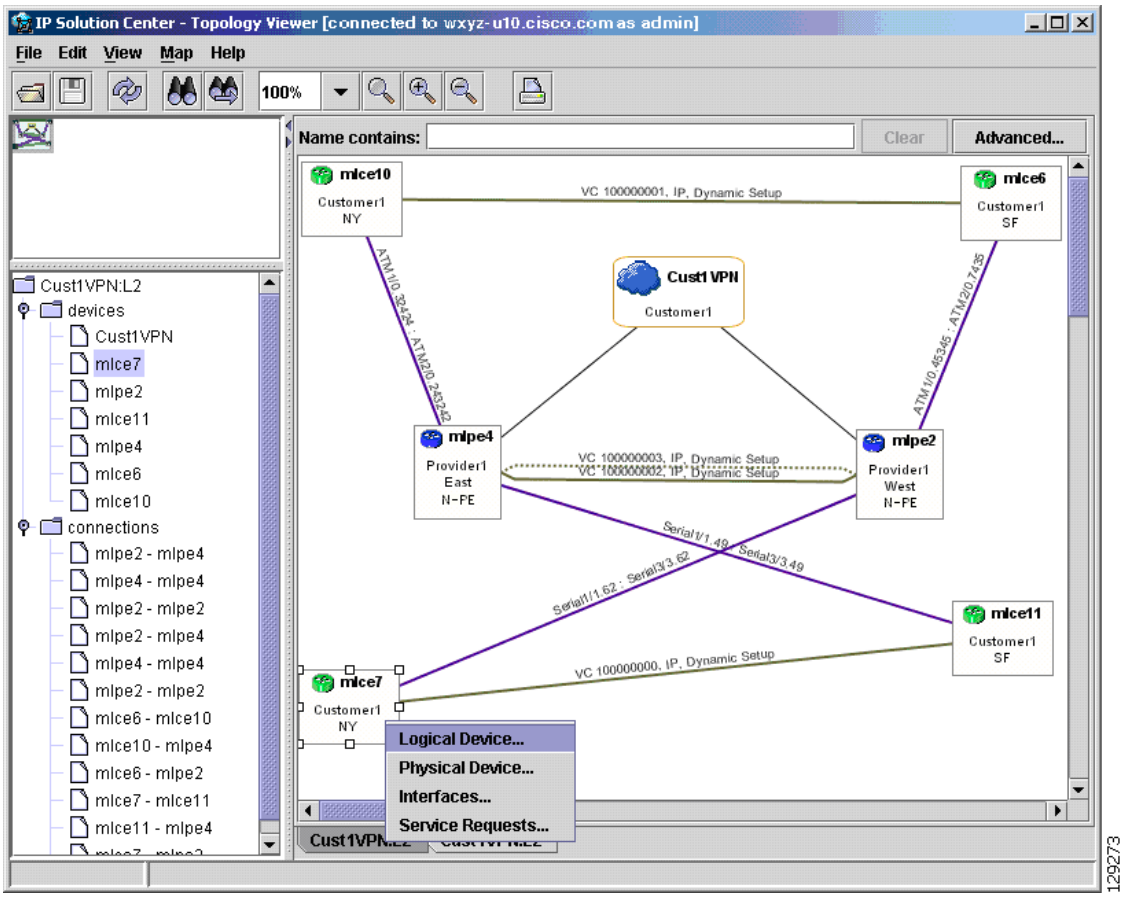
Figure 3-12 Aggregate View



The Layer 2 VPN might in addition to CPEs show connectivity between Customer Location Edge devices (CLEs) or Provider Edge devices (PE). For VPLS, you see connectivity between CPEs. For missing CPEs, you see connectivity to PEs.

In MPLS Layer 2 VPN, the topology displays Virtual Circuit (VC) with MPLS core (as MPLS string) but with L2TPv3, the topology will display Virtual Circuit (VC) with IP core (as IP string) as shown in Figure 3-13.

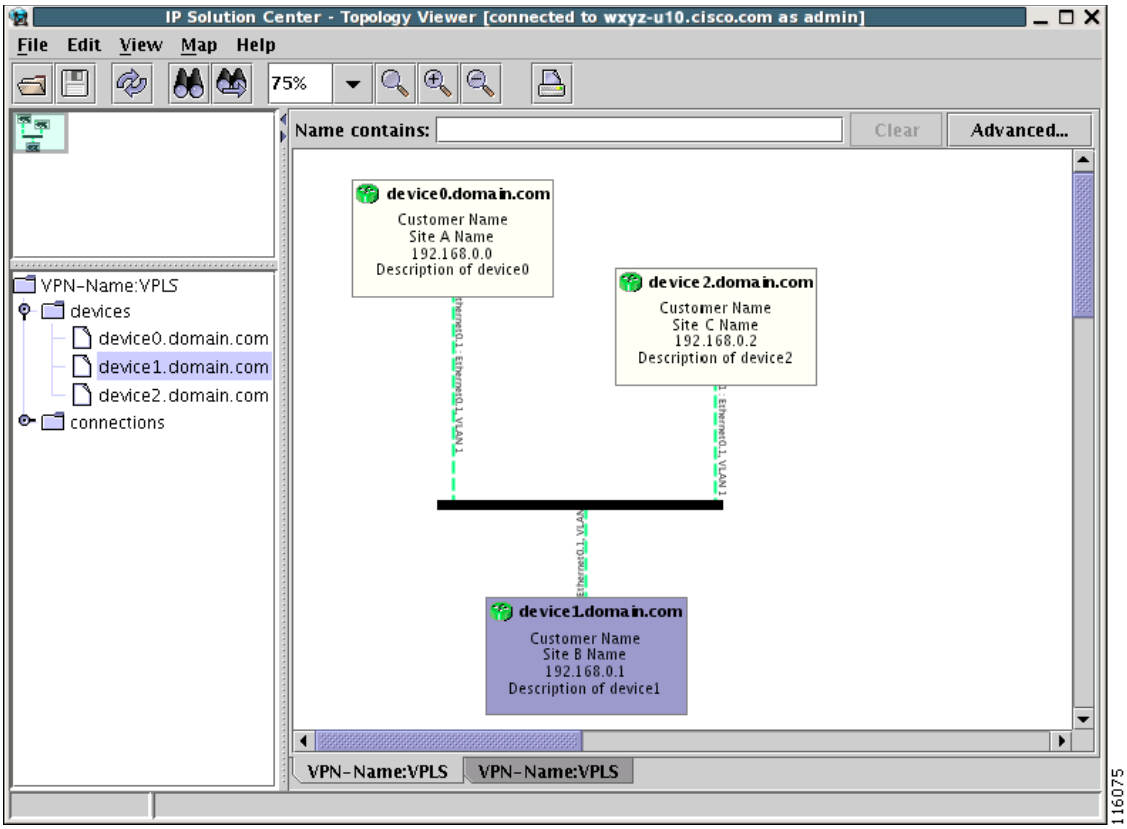
Figure 3-13 Virtual Circuit with IP Core



VPLS Topology

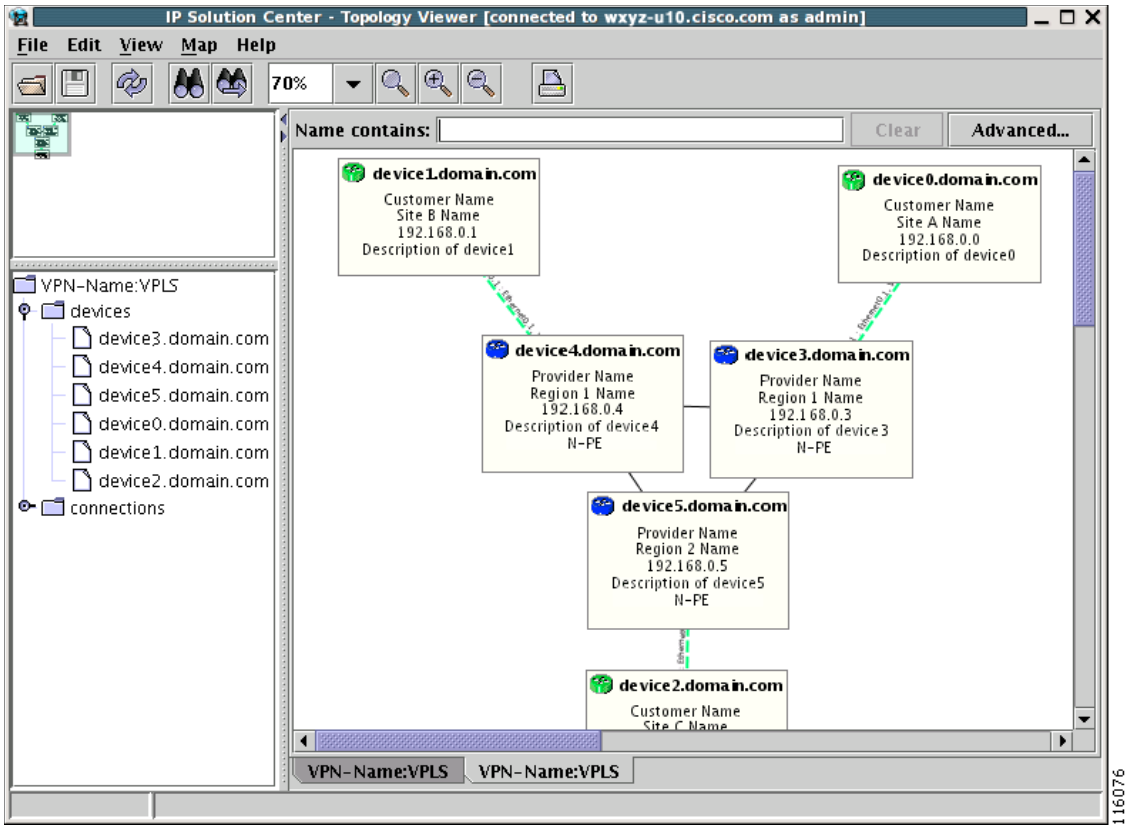
In the case of a VPLS topology, you can access an Attachment Circuit View or an Emulated Circuit View. The Attachment Circuit View corresponds to a logical view in other types of VPNs. It shows customer devices connected to a virtual private LAN, as shown in Figure 3-14, "Attachment Circuit View."

Figure 3-14 Attachment Circuit View



The Emulated Circuit View shows the physical connectivity details omitted in the Attachment Circuit View. Connectivity between provider devices and customer devices connected to provider devices, as shown in Figure 3-15, "Emulated Circuit View."

Figure 3-15 Emulated Circuit View



Logical View

The logical view shows connectivity, created through service requests, between PEs and CPEs of a given region.

To activate the logical view, use the following steps:

Step 1 In the menu bar, select **File > Open**.

or

click the **Open** button in the tool bar.

The Folder View window in Figure 3-11 appears.

Step 2 Navigate to the desired VPN's folder and double-click on the desired folder. Any logical and physical views associated with that VPN are displayed.

Step 3 To open the logical view for the selected VPN, do one of the following:

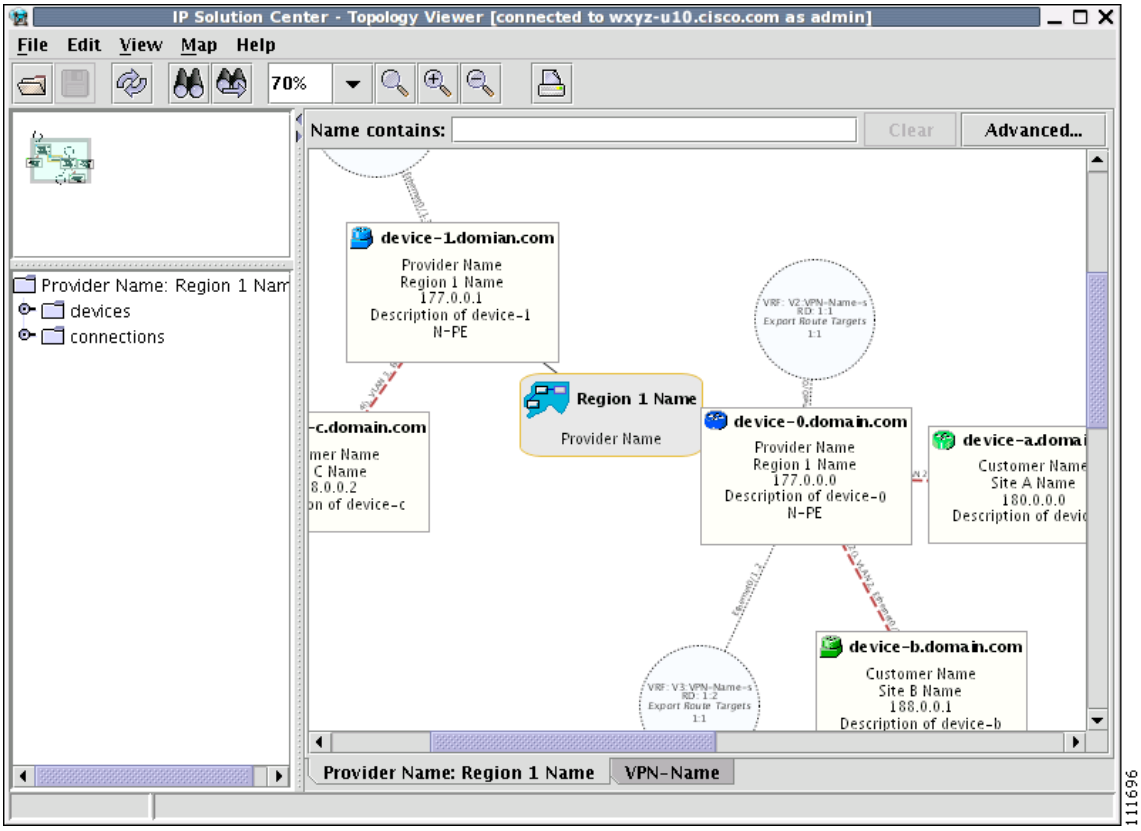
Single-click the **Logical View** icon and click **Open**

or

Double-click the **Logical View** icon.

This creates a logical view for the chosen VPN, as shown in Figure 3-16.

Figure 3-16 Logical View

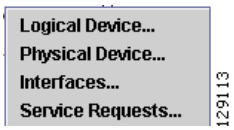


In a created view, the node, usually located in the center of the graph, is the node representing a given region of a provider. The node is annotated with the name of the region and the name of the provider.

Each node directly connected to the regional node represents a PE. The icon of a node depends on the type and the role of the device it represents (see the "Conventions" section on page 3-9).

Each PE is annotated with the fully-qualified device name, provider name, region name, management IP address, description, and role. A right-click on a node displays the details of the logical and physical device, interfaces, and service requests (SR) associated with the node, as shown in Figure 3-17. For the regional node, details are shown in a tabulated form.

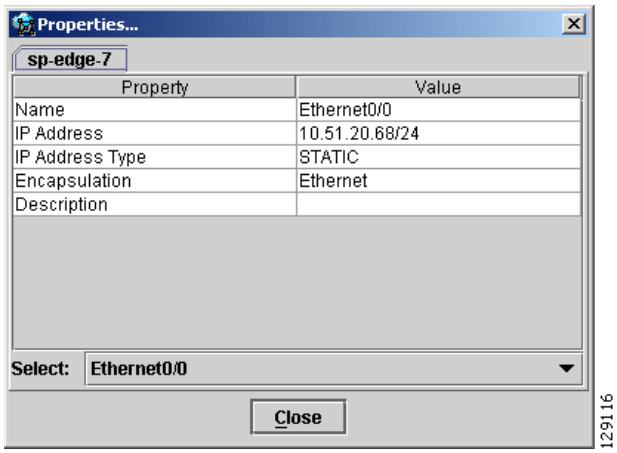
Figure 3-17 Device Properties



The various node and link properties are described in detail in Viewing Device and Link Properties, page 3-23.

Likewise, you can right-click on a link to learn about its link properties. For example, when selecting **Interfaces...** for a sample serial link, a Properties window like the one in Figure 3-18 appears.

Figure 3-18 Interface Details Table



Each PE can be logically connected to one or more CPEs. Such connections are created by either MPLS VPN links, Layer 2 Logical Links, or IPsec service request tunnels (**IPsec is not supported in this release**.). Each such connection is represented by an edge linking the given PE to a CPE. If there are more connections between a particular PE and CPE, all of them are shown. Depending on the state of a connection, the edge is drawn using a solid line (for functioning connections), dotted line (for broken connections), or dashed line (for connections yet to be established).

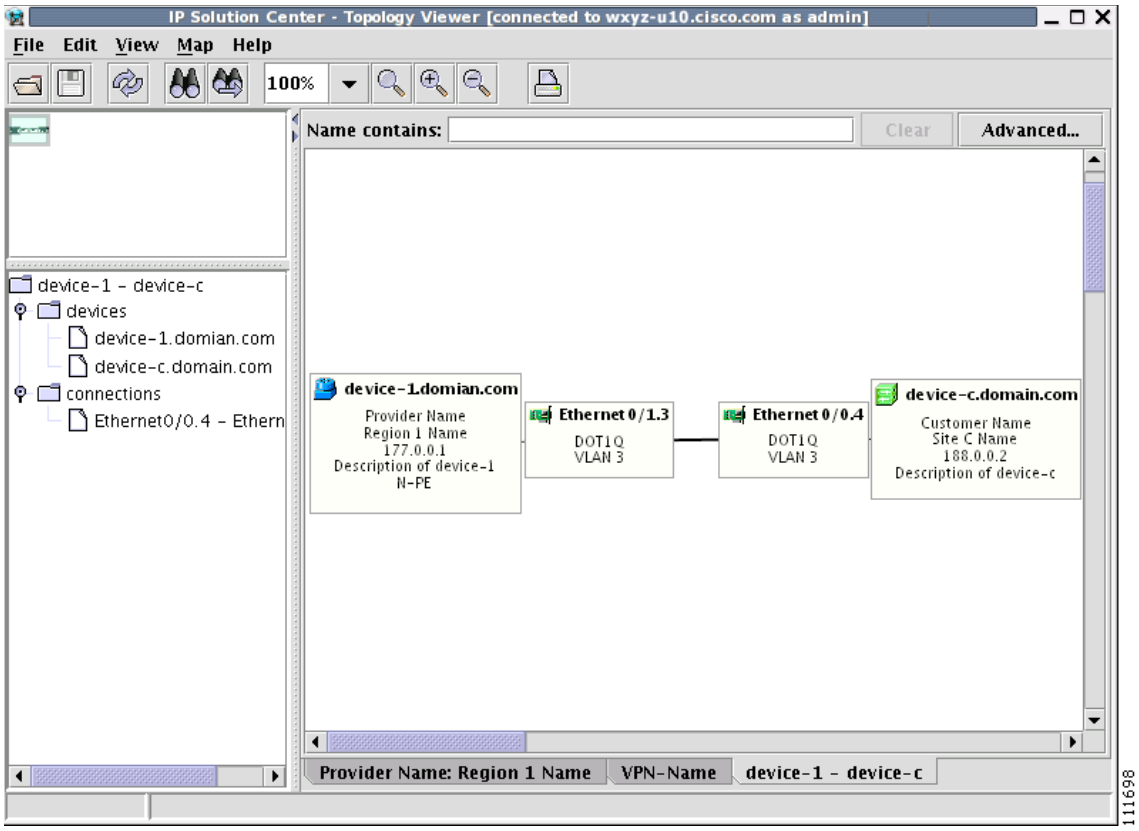
Depending on the connection type, the connection is drawn as described in Table 3-3 and Table 3-4. Each connection is annotated with the PE Interface Name (IP address), VLAN ID number, CPE Interface Name (IP address).

In the Overview area, a direct connection is drawn between a CPE and a PE, even if a number of devices are forming such a connection.

For more about viewing device properties, see Viewing Device and Link Properties, page 3-23.

To view the details of a connection, right-click on it and select the **Expand** option from a pop-up menu. The expanded view, displayed in a new tab, shows all devices and interfaces making a given PE to CPE connection, as shown in Figure 3-19.

Figure 3-19 Detailed Connection View



Physical View

A physical view shows all named physical circuits defined for PEs in a given region. Each named physical circuit is represented as a sequence of connections leading from a PE through its interfaces to interfaces of CLEs or CPEs. All physical links between PEs of a given region and their CLEs or CPEs are shown. Since physical links are assumed to be in a perfect operational order, edges are always drawn with solid lines.

To activate the physical view, use the following steps:

Step 1 In the menu bar, select **File** > **Open**.

or

click the **Open** button in the tool bar.

The Folder View window in Figure 3-11 appears.

Step 2 Navigate to the desired VPN's folder and double-click on the desired folder. Any logical and physical views associated with that VPN are displayed.

Step 3 To open the physical view for the selected VPN, do one of the following:

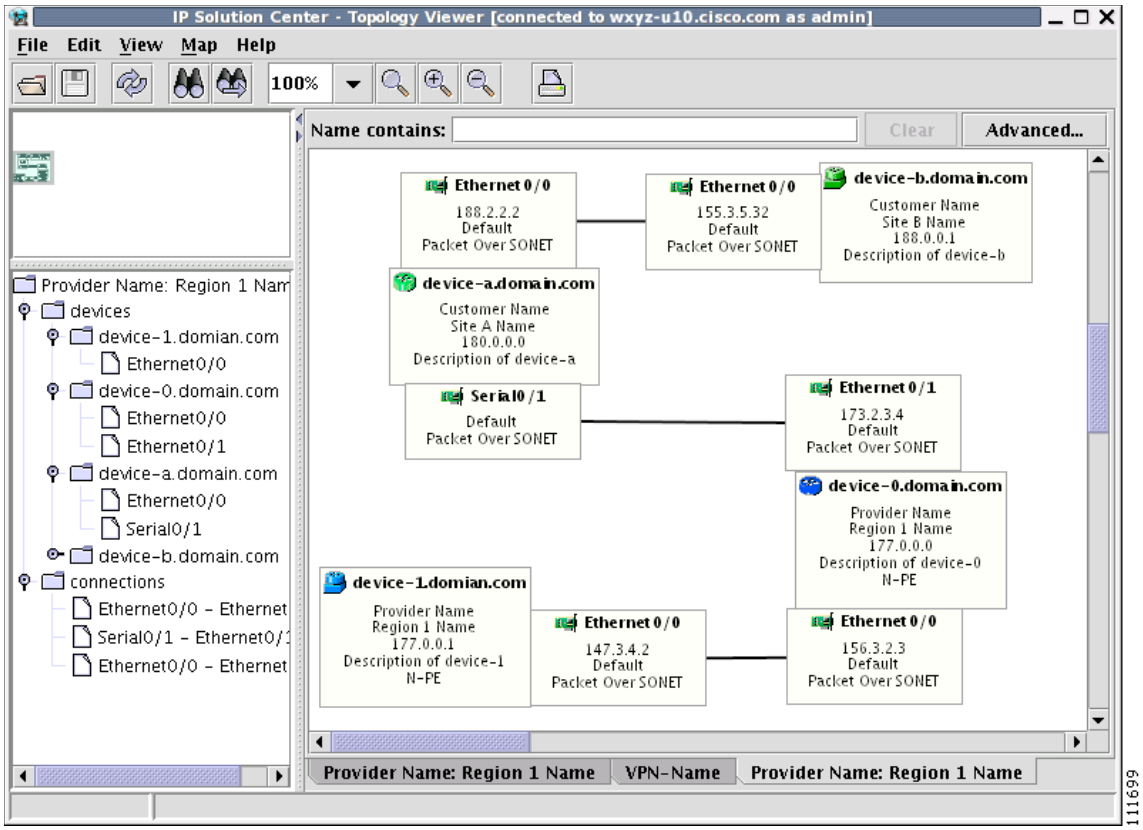
Single-click the **Physical View** icon and click **Open**

or

Double-click the **Physical View** icon.

This creates a physical view for the chosen VPN, as shown in Figure 3-20.

Figure 3-20 Physical View



In this view, each device is connected with a thin line to the interfaces it owns. Interfaces are connected to other interfaces with thick lines. If there is more than one connection between two interfaces, they are spaced to show all of them.

The tree shows devices and connections. Each device can be a folder, holding all interfaces connected to it.

Viewing Device and Link Properties

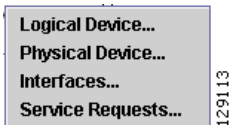
In the logical view, you can view the properties of both devices and links. In the physical view, only properties of physical devices are accessible.

Thus, device properties can be viewed in both the logical and physical views.

Device Properties

To view the properties of a device, right-click the device. The Device Properties menu in Figure 3-17 appears.

Figure 3-21 Device Properties



The following properties are available:

Logical Device...—View the logical properties of the device.

Physical Device...—View the physical properties of the device.

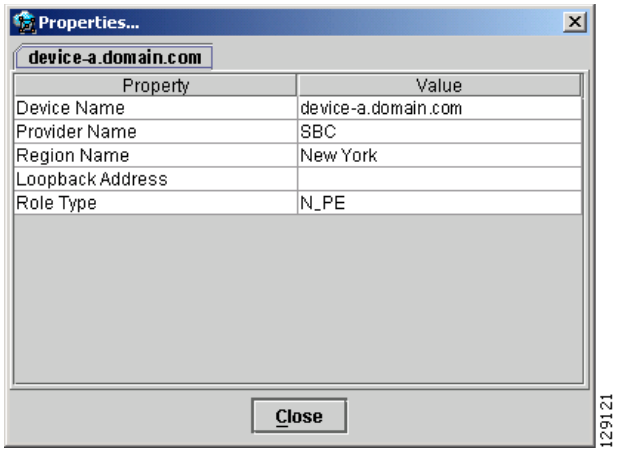
Interfaces...—View interface properties of the device.

Service Requests...—View service request properties associated with the device.

Logical Device

When right-clicking a device and selecting **Logical Device...**, the logical device properties window in Figure 3-22 appears.

Figure 3-22 Logical Device Properties



The logical properties window displays the following information:

Device Name—Name of the device.

Provider Name—Name of the provider whom the device is serving.

Region Name—Name of the provider region.

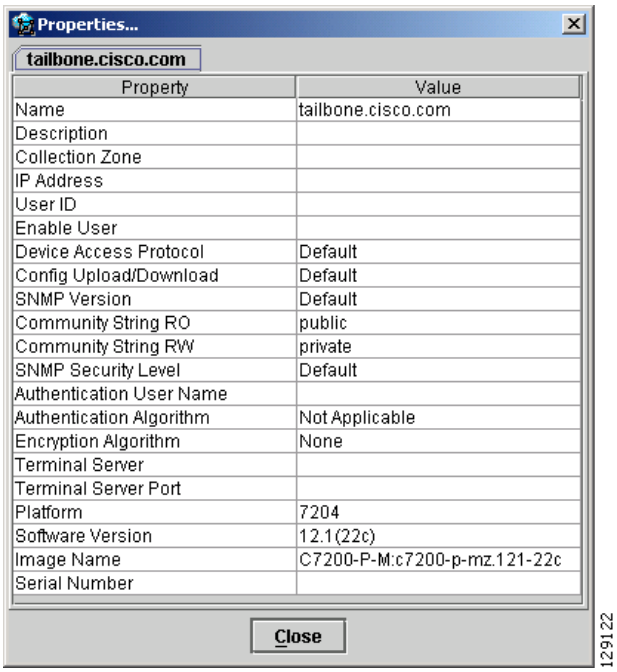
Loopback Address—IP address of the loopback address.

Role Type—Role assigned to the device.

Physical Device

When right-clicking a device and selecting **Physical Device...**, the physical device properties window in Figure 3-23 appears.

Figure 3-23 Physical Device Properties



Property	Value
Name	tailbone.cisco.com
Description	
Collection Zone	
IP Address	
User ID	
Enable User	
Device Access Protocol	Default
Config Upload/Download	Default
SNMP Version	Default
Community String RO	public
Community String RW	private
SNMP Security Level	Default
Authentication User Name	
Authentication Algorithm	Not Applicable
Encryption Algorithm	None
Terminal Server	
Terminal Server Port	
Platform	7204
Software Version	12.1(22c)
Image Name	C7200-P-M:c7200-p-mz.121-22c
Serial Number	

The physical properties window displays the following information:

Name—Name of the device.

Description—User-defined description of the device.

Collection Zone—Collection zone for device data.

IP Address—IP address of the interface used in the topology.

User ID—User ID for the interface.

Enable User—Password for the interface.

Device Access Protocol—Protocol used to communicate with the device.

Config Upload/Download—Upload/download method for the configuration file.

SNMP Version—Simple Network Management Protocol (SNMP) version on the device.

Community String RO—**public** or **private**

Community String RW—**public** or **private**

SNMP Security Level—Simple Network Management Protocol (SNMP) security level.

Authentication User Name—User name for performing authentication on the device.

Authentication Algorithm—Algorithm used to perform authentication.

Encryption Algorithm—Encryption algorithm used for secure communication.

Terminal Server—Name of the terminal server.

Terminal Server Port—Port number used by the terminal server.

Platform—Hardware platform.

Software—IOS version or other management software on the device.

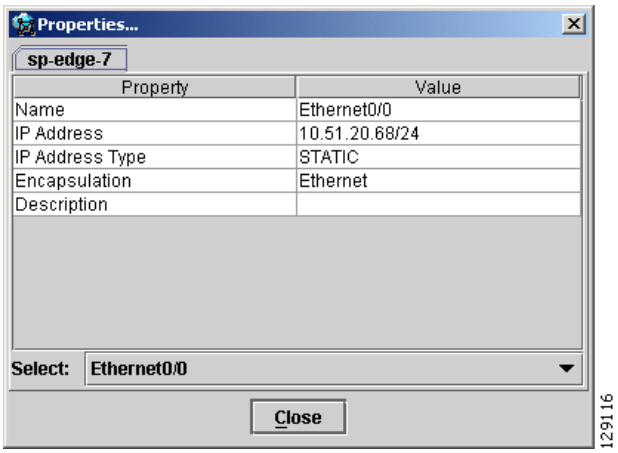
Image Name—Boot image for device initialization.

Serial Number—Serial number of the device.

Interfaces

When right-clicking a device and selecting **Interfaces...**, the interface properties window in Figure 3-24 appears.

Figure 3-24 Device Interface Properties



The interface properties window displays the following information:

Name—Name of the device.

IP Address—IP address of the device.

IP Address Type—STATIC or DYNAMIC.

Encapsulation—Encapsulation used on the interface traffic.

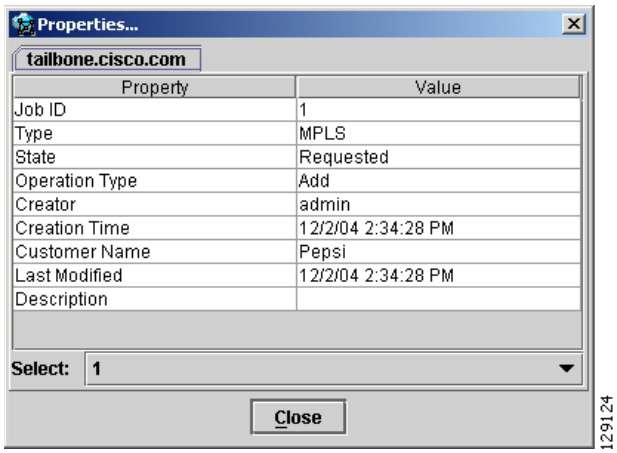
Description—Description assigned to the interface, if any.

Select (link)—If a connection is attached to the interface, a drop-down list at the bottom of the window allows you to choose between the interfaces available on the device.

Service Requests

When right-clicking a device and selecting **Service Requests...**, the service request (SR) properties window in Figure 3-25 appears.

Figure 3-25 Service Request Properties



The service request properties window displays the following information:

Job ID—SR identifier.

Type—Protocol type used in the SR.

State—SR state.

Operation Type—Encapsulation used on the interface traffic.

Creator—Description assigned to the interface, if any.

Creation Time—Date and time when the SR was created.

Customer Name—Name of customer associated with the SR.

Last Modified—Date and time when the SR was last modified.

Description—User-defined description of the SR.

Select (SR)—If more than one SR is associated with the interface, the drop-down list at the bottom of the window allows you to choose between these SRs.

Link Properties

To view the properties of a given link, right-click the link. The Link Properties menu in Figure 3-26 appears.

Figure 3-26 Link Properties

The following options are available:

Expand...—View link details, including devices local to the link not shown in the general topology.

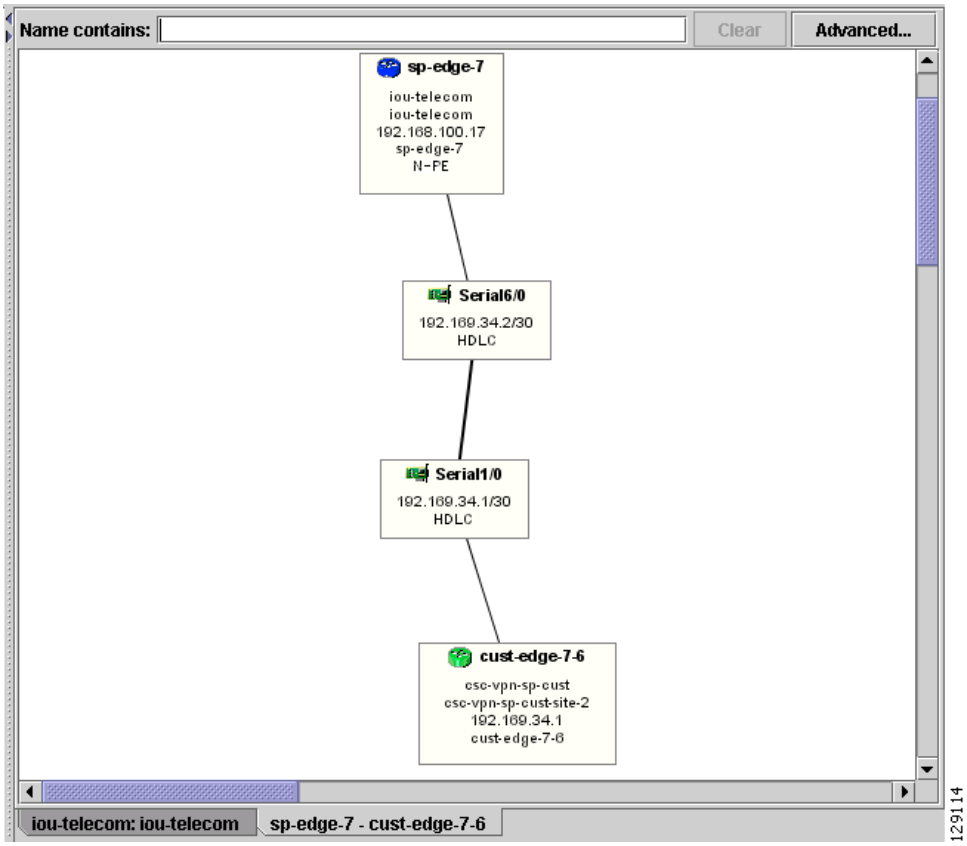
Service Request...—View service request properties associated with the link.

MPLS VPN...—View the MPLS VPN properties of the link. Other link protocol properties than MPLS VPN are currently not available.

Expand

When right-clicking a link and selecting **Expand...**, the Topology Display will display any devices and connections local to that link. An Expand Link window similar to the one in Figure 3-25 will appear.

Figure 3-27 Expand Link

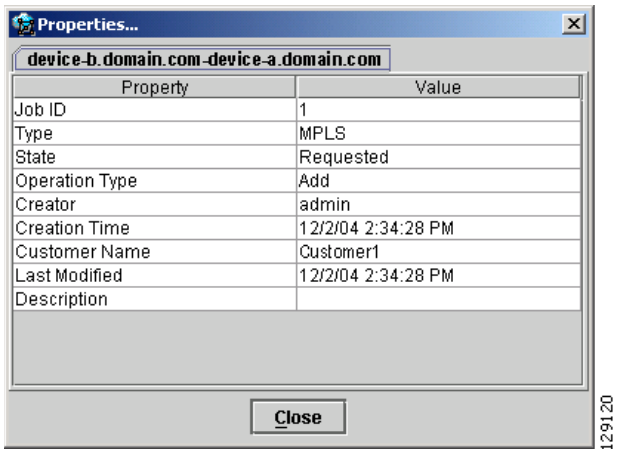


Properties information for devices and links can only be obtained in the master view as described earlier in this section.

Service Request

When right-clicking a link and selecting **Service Requests...**, the service request (SR) properties window in Figure 3-28 appears.

Figure 3-28 Link Service Request Properties



The service request properties window displays the following information:

Job ID—SR identifier.

Type—Protocol type used in the SR.

State—SR state.

Operation Type—Encapsulation used on the interface traffic.

Creator—Description assigned to the interface, if any.

Creation Time—Date and time when the SR was created.

Customer Name—Name of customer associated with the SR.

Last Modified—Date and time when the SR was last modified.

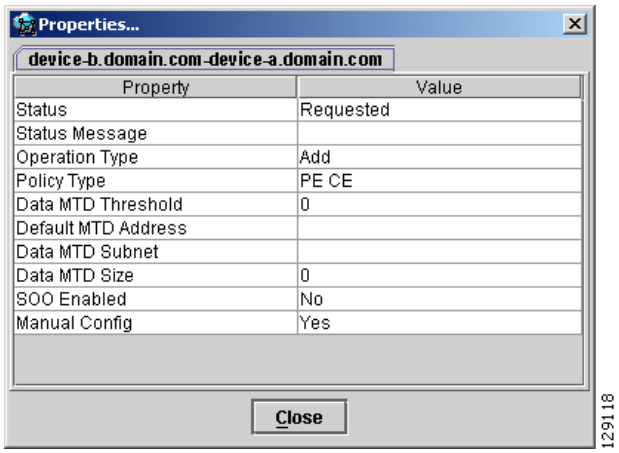
Description—User-defined description of the SR.

Select (SR)—If more than one SR is associated with the interface, the drop-down list at the bottom of the window allows you to choose between these SRs.

MPLS VPN

When right-clicking a link that is configured for MPLS VPN and selecting **MPLS VPN...**, the MPLS VPN properties window in Figure 3-29 appears.

Figure 3-29 Link MPLS VPN Properties



The service request properties window displays the following information:

Status—Status of the MPLS VPN link.

Status Message—Displays any error or warning messages.

Operation Type—MPLS operation type.

Policy Type—The policy type applied to the link.

Data MTD Threshold—Memory Technology Driver (MTD) data threshold.

Default MTD Address—Default MTD IP address.

Data MTD Subnet—Data MTD subnet.

Data MTD Size—Data MTD size.

SOO Enabled—**Yes** or **No**.

Manual Config—**Yes** or **No**.

Filtering and Searching

On large graphs, the amount of detail can be overwhelming. In such cases, filtering might help eliminate unnecessary details, while searching can lead to a prompt location of a device you want to examine further.

Both advanced filtering and searching use the same dialog to enter conditions on nodes to be either filtered or located. The filtering area also allows you to quickly filter viewed objects by name.

Filtering

The topology view can be filtered in two ways, simple and advanced.

Simple Filtering

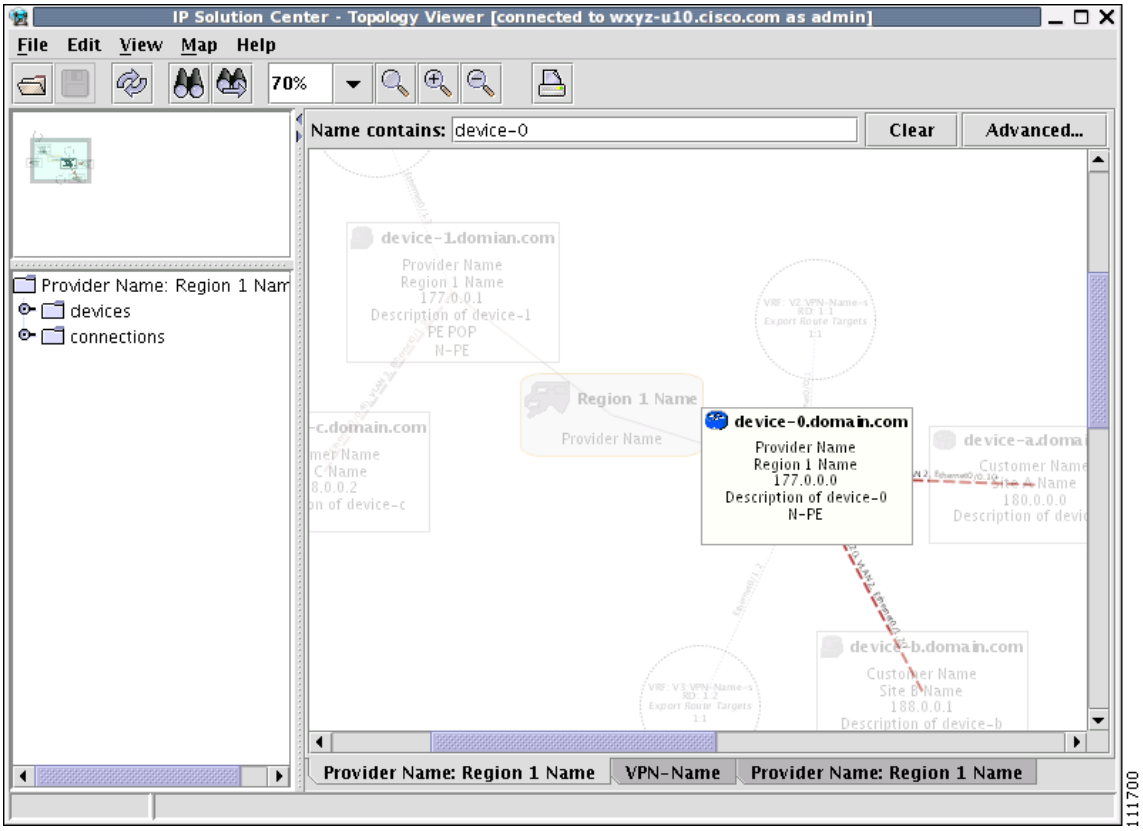
To perform simple filtering of the view, do as follows:

Step 1 Enter a string in area (4) of the main window, as shown in Figure 3-8 on page 3-12.

Step 2 Press **Enter** to dim all objects whose name does not contain the specified string.

For example, to locate nodes that contain string **router** in their name you would enter **router** in area (4) and click **Enter**. All objects whose name does not contain the entered string are dimmed, as shown in Figure 3-30.

Figure 3-30 Physical View with Dimmed Nodes



Note Regular expressions are supported but only in the advanced dialog (click **Advanced...** button). For example, by entering ^foo.*a, you only request nodes that have names starting with "foo" followed by arbitrary characters and containing the letter 'a' somewhere in the name. The regular expressions must follow the rules defined for Java regular expressions.

Advanced Filtering

To perform advanced filtering, do as follows:

Step 1 Open the advanced filtering dialog by clicking the **Advanced...** button. The Advanced Filter dialog appears, as shown in Figure 3-31.

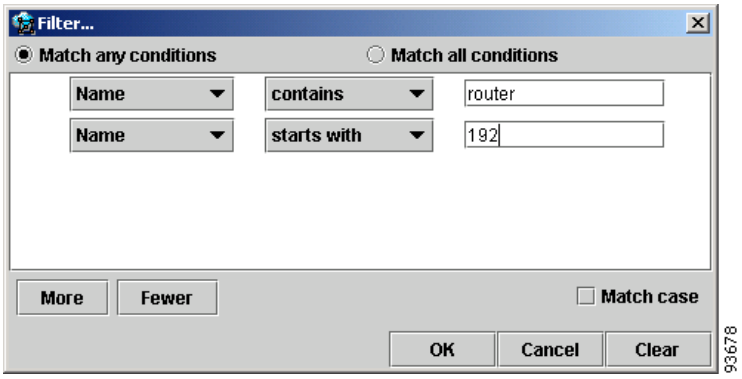
Step 2 Make the desired filtering elections.

The dialog allows you to enter one or more conditions on filtered nodes. The first drop-down menu allows you to specify the attribute by which the filtering is performed. The second allows you to decide how the matching between the value of the attribute and text entered in the third column is performed.

The following matching modes are supported from the drop-down menu:

- **contains**—The attribute value is fetched from the device and it is selected if it contains the string given by you. The string can be located at the start, end, or middle of the attribute for the match to succeed. For example, if the pattern is **cle** the following values match it in the **contains** mode: **clean**, **nucleus**, **circle**.
- **starts with**—The value of the attribute must start with the string given by you. For example, if the pattern is **foot**, **footwork** matches, but **afoot** does not.
- **ends with**—This is the reverse of the **starts with** case, when a given attribute matches only if the specified pattern is at the end of the attribute value. In this mode, for example, the pattern **foot** matches **afoot** but not **footwork**.
- **doesn't contain**—In this mode, only those strings that do not contain the given pattern match. The results are opposite to that of the **contains** mode. For example, if you specify **cle** in this mode, **clean**, **nucleus**, and **circle** are rejected, but **foot** is deemed to match, because it does not contain **cle**.
- **matches**—This is the most generic mode, in which you can specify a full or partial expression that defines which nodes you are interested in.

Figure 3-31 Advanced Filter dialog



By clicking one of the two radio buttons, **Match any conditions** or **Match all conditions**, you can request that any or all of the conditions are matched. In the first case, you can look for devices where, for example, the name contains **cisco** and the management IP address ends with **204**. When all conditions must be met, it is possible to look for devices that, for example, have a given name and platform.

Click **More** or **Fewer** to add more rows of conditions or remove existing rows of conditions.

By default, all matches are performed without regard for upper or lower case. However, in some cases it is beneficial to have a more exact matching that takes the case into account. To do so, select the **Match case** check box.

Step 3 Click **OK** to start the filtering process. Click **Cancel** to hide the dialog without any changes to the state of the filters.

The **Clear** button allows you to clear all conditions. Clicking **Clear** followed by **OK** effectively removes all filtering, restoring all nodes to their default brightness level. If filtering is active, the same can be achieved by clicking **Clear** in area (4) of the main window, as shown in Figure 3-8 on page 3-12.

Searching

Searching can be conducted by using the menus or the tool bar. To perform a search, do as follows:

Step 1 Select **Find** in the **Edit** menu

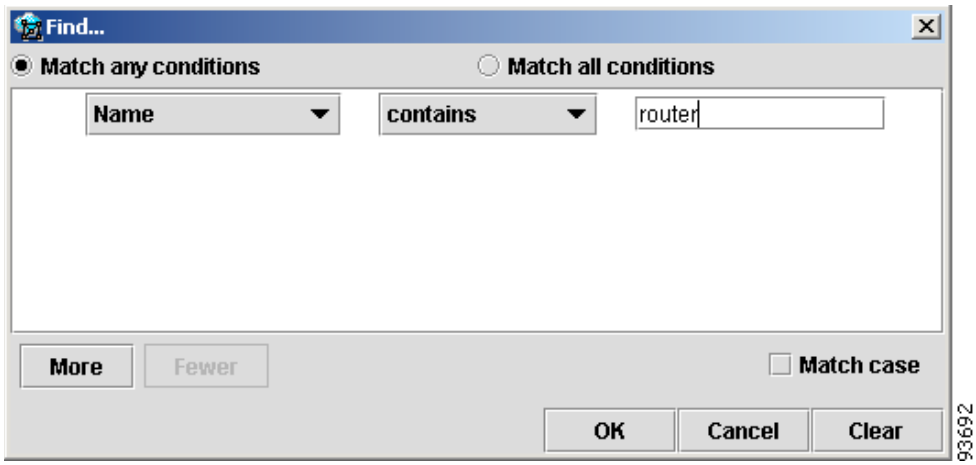
or

Click the **Find** icon in the main toolbar.

Both approaches bring up the same dialog box, as shown in Figure 3-32.

Again, you can enter one or more conditions to locate the node.

Figure 3-32 Find Dialog Box



Step 2 Make the desired filtering selections. Match modes, case check box, and the radio button are used as described under Advanced Filtering, page 3-31, as shown in Figure 3-31.

Step 3 Click **OK** to start searching for the first node that matches the given criteria. If found, the node is highlighted and the view is shifted to make it appear in the currently viewed area of the main window.

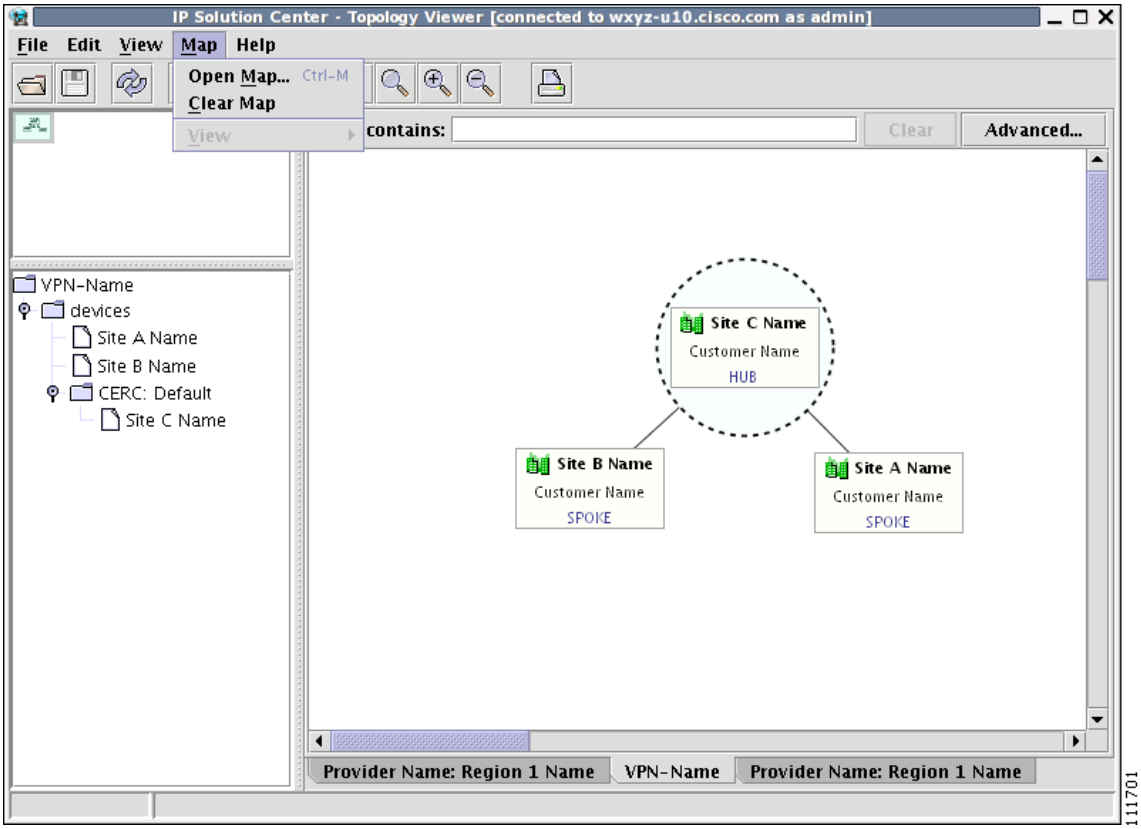
Step 4 After the first search, press **F3** or click the **Find Again** button to repeat the search. If more than one node matches the condition the **Find Again** function highlights each one of them. If no nodes match the entered criteria, the **Object Not Found** dialog box appears.

Using Maps

You can associate a map with each view. Currently, the topology viewer only supports maps in the Environmental Systems Research Institute, Inc. (ESRI) shape format. The following sections describe how to load maps and selectively view map layers and data associated with each map.

The map features are accessed from the **Map** menu shown in Figure 3-33.

Figure 3-33 The Map Menu



The **Map** menu contains the following menu items:

- **Open Map...** Loads a map into the application
- **Clear Map** Clears the active map from the current view
- **View** Allows you to select which layers in the map should be displayed (for example, country, state, city).

Loading a map

You might want to set a background map showing the physical locations of the displayed devices. To load a map, use the following steps:

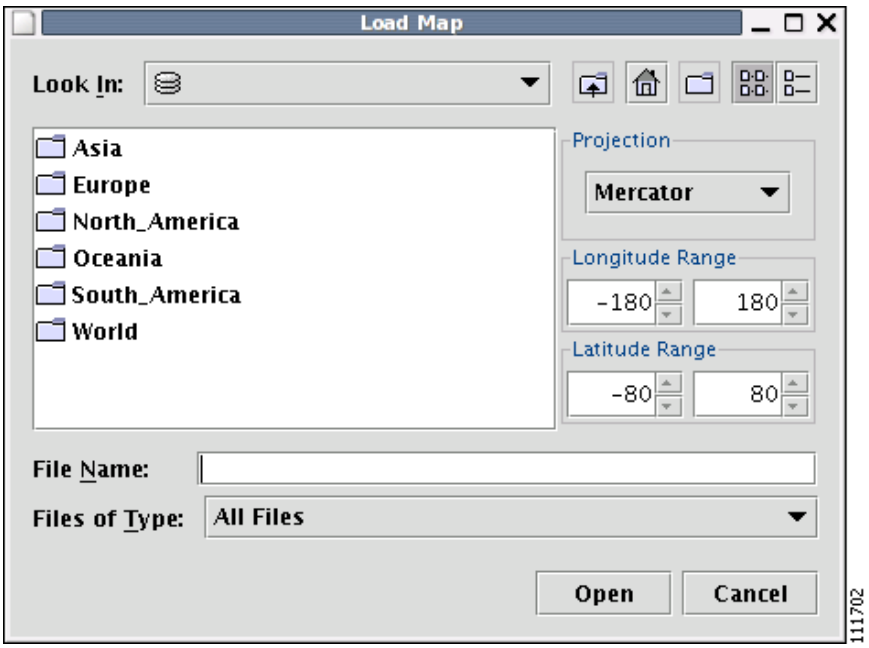
Step 1 In the menu bar, select **Map > Open Map...**.

or

Press **Ctrl-M**

Providing the web map server is running and operational, the Load Map window appears, as shown in Figure 3-34.

Figure 3-34 Load Map Window



Step 2 Make your selections in the Load Map window.

The right-hand side of the window contains a small control panel, which allows you to select the projection in which a map is shown. A map projection is a projection that maps a sphere onto a plane. Typical projections are Mercator, Lambert, and Stereographic.

For more information on projections, consult the Map Projections section of Eric Weisstein's World of Mathematics at:

http://mathworld.wolfram.com/topics/MapProjections.html

For each projection, you can also select the region of the map to be shown. In most cases, the predefined values should be sufficient. The top level the file hierarchy should contain folders for all major regions, such as Europe, North America, Oceania, and so on.

If desired, make changes to the settings in the **Longitude Range** and **Latitude Range** fields.

Step 3 Navigate to the desired folder.

Each folder can contain either complete maps or folders for countries. Each map is clearly distinguished with the **Map** icon.

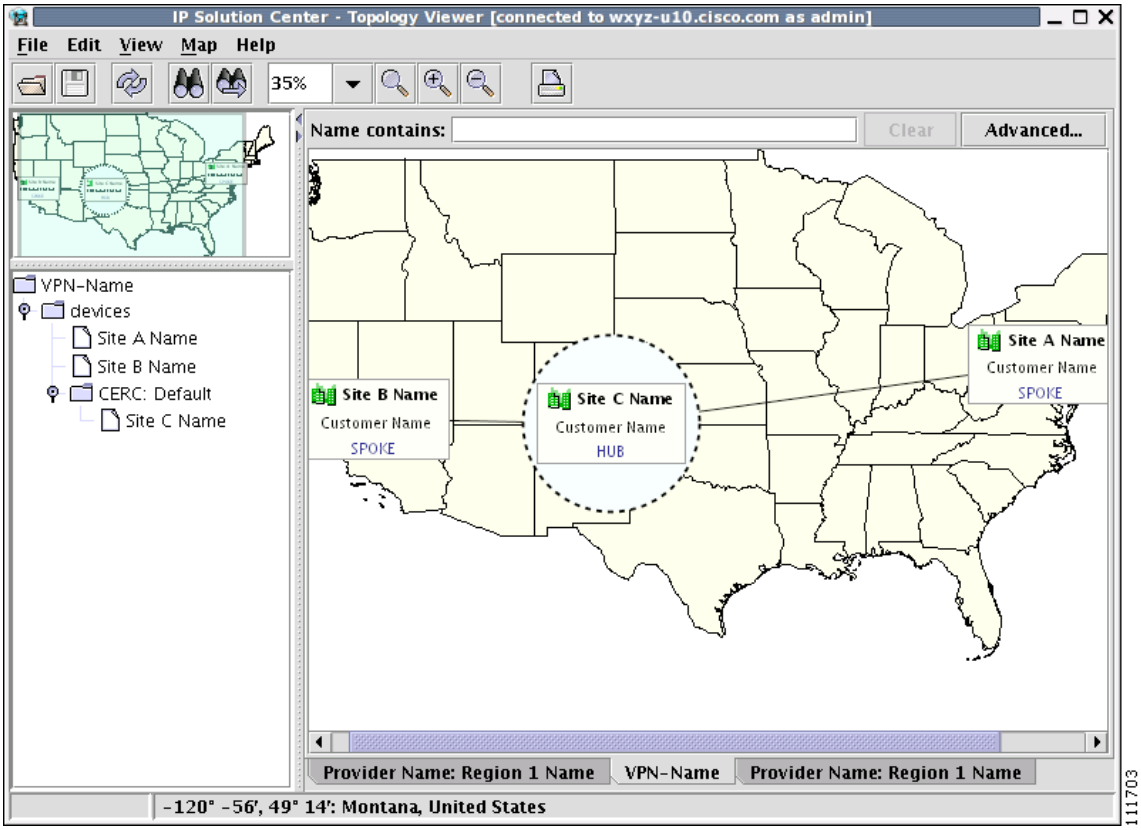
Step 4 Select a map file and click **Open** to load the map.

Selecting the map file and clicking the **Open** button starts loading it. Maps can consist of several components and thus a progress dialog is shown informing you which part of the map file is loaded.

Layers

Each map can contain several layers. For example most country maps have country, region, and city layers, as shown in Figure 3-35.

Figure 3-35 Map Layers



After a map is loaded, the **View** submenu of the **Map** menu is automatically populated for you. A name of each available layer is shown together with the check box indicating visibility of the layer. If a given map shows too many details, you can turn off some or all layers by deselecting the corresponding check box(es). The same submenu can be used to restore visibility of layers.

If an incorrect map is loaded or the performance of the topology tool is unsatisfactory with the map loaded, you can clear the map entirely. To do this, select **Clear Map** from the **Map** menu. Maps are automatically cleared if another map is loaded.

Consequently if you want just to load another map, there is no need to clear the existing map. The act of loading a new map does this.

Map data

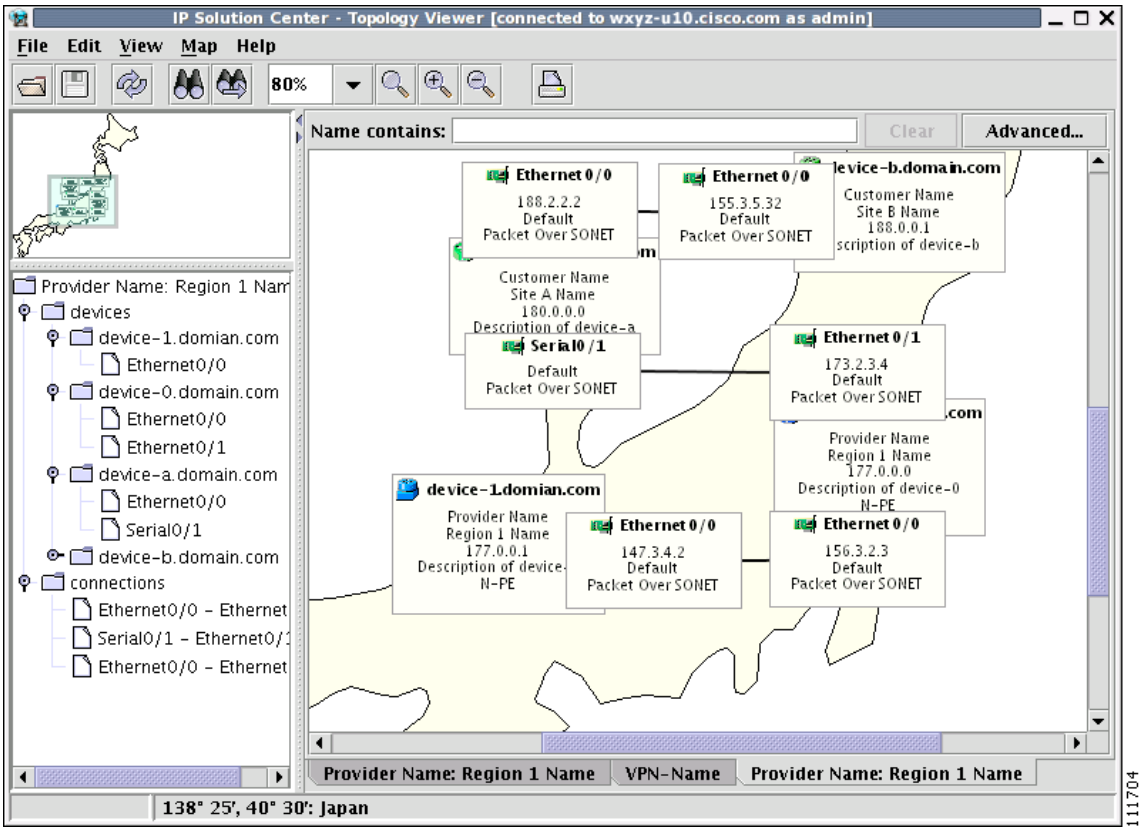
If map data files are successfully loaded with the map, the right field of the Status bar shows the longitude and latitude location of the cursor on the map. If map objects, such as cities, lakes, and so on, have data associated with them, their names are displayed after the longitude and latitude coordinates.

Node locations

After a map is successfully loaded, the view area is adjusted to fully accommodate it, as shown in Figure 3-36. If nodes shown on the window had longitude and latitude information associated with them, they are moved to locations on the map corresponding to their geographical location. If not, their positions remain unchanged.

However, you can manually move them to the desired location and save the positions for future reference. The next time the image of a given network is loaded, node positions are restored and the map file is loaded.

Figure 3-36 Physical View with a Map of Japan



Adding new maps

You might want to add your own maps to the selection of maps available to the topology application. This is done by placing a map file in the desired directory within the ISC installation. To make this example more accessible, assume that you want to add a map of Toowong, a suburb of Brisbane, the capital of Queensland. The first step to do so is to obtain maps from a map vendor. All maps must be in the ESRI shape file format (as explained at the web site: http://www.esri.com). In addition, a data file might accompany each shape file. Data files contain information about objects whose shapes are contained within the shape file. Let us assume that the vendor provided four files:

- toowong_city.shp
- toowong_city.dbf
- toowong_street.shp
- toowong_street.dbf

We must create a map file that informs the topology application about layers of the map. In this case we have two layers: a city and a street layer. The map file, say, Toowong.map, would thus have the following contents:

```
toowong_city
toowong_street
```

It lists all layers that create a map of Toowong. The order is important, as the first file forms the background layer, with other layers placed on top of the preceding layers.

Having obtained shape and data files and having written the map file, decide on its location. As mentioned, Toowong is a suburb of Brisbane, located in Queensland, Australia. All map files must be located in or under the **$ISC_HOME/resources/webserver/tomcat/webapps/ipsc-maps/data** directory. Since by default this directory contains a directory called **Oceania** intended for all maps from that region, simply create a path **Australia/Queensland/Brisbane** under the directory **Oceania**. Next, place all five files in this location. After this is done, the map is automatically accessible to the topology viewer.

Devices

Every network element that ISC manages must be defined as a device in the system. An element is any device from which ISC can collect information. In most cases, devices are Cisco IOS routers that function as edge routers in the IPsec VPN **- IPsec is NOT SUPPORTED in this release. -**, or as Provider Edge Routers (PEs) or Customer Edge Routers (CEs) in the MPLS VPN.

Note To provision services with ISC, you must have IPv4 connectivity.

This section describes how to configure SSH, set up SNMP, manually enable an RTR responder, and create, edit, delete, and configure various types of supported devices. This section includes the following:

Configuring SSH

ISC needs a mechanism to securely access and deploy configuration files on devices, which include routers, switches, Cisco VPN 3000 concentrators **- NOT SUPPORTED in this release. -**, and Cisco PIX Firewalls **- NOT SUPPORTED in this release. -**. And, to securely download a configlet and upload a configuration file from a device, SSH must be enabled.

The following sections describe how to configure SSH on a device.

Configuring SSH on Cisco IOS Routers

This Cisco IOS router configuration procedure assumes that the router's authentication database is stored locally on the router and not on a TACACS or RADIUS server.

The procedure for configuring SSH on a Cisco IOS router is as follows:.

	Command	Description
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`ip domain-name`** `<domain_name>`	Specifies the IP domain name.
Step 3	`Router(config)#` **`username`** `<username>` **`password`** `<password>`	Configures the user ID and password. Enter your ISC username and password. For example: **`username admin password iscpwd`**
Step 4	`Router(config)#` **`crypto key generate rsa`**	Generates keys for the SSH session.
Step 5	You will see the following prompt: `Choose the size of the key modulus in the range of 360 to 2048 for your general purpose keys. How many bits in the modulus (nnn):` Press **Enter** to accept the default number of bits.	Sets the number of bits.
Step 6	`Router(config)#` **`line vty 0 4`**	Enables SSH as part of the vty login transport.
Step 7	`Router(config-line)#` **`login local`**	The **login local** command indicates that the router stores the authentication information locally.
Step 8	`Router(config-line)#` **`transport input telnet ssh`**	Enables SSH transport.
Step 9	`Router(config-line)#` **`Ctrl+Z`**	Returns to Privileged Exec mode.
Step 10	`Router#` **`copy running startup`**	Saves the configuration changes to NVRAM.

Configuring SSH on VPN 3000 Concentrators

- NOT SUPPORTED in this release. -

The procedure for configuring SSH on a VPN 3000 concentrator is as follows:

Step 1 Telnet to the VPN 3000 device through the console port. The command line appears.

Step 2 Select **Administration** > **Certificate Management** > **SSL Certificate**.

Step 3 Click **Generate**. The system uses parameters set on the Configuration > System > Management Protocols > SSL window and generates the certificate. The new certificate replaces any existing SSL certificate.

Step 4 If you must modify the SSH In and SSH Out Rules, select **Configuration** > **Policy Management** > **Traffic Management** > **Rules**. Select the rule you want to modify, and then click **Modify**.

Step 5 For SSH In and/or SSH Out, make any modifications that you require. Click **Apply** when you are finished making changes to a rule.

Step 6 Select **Configuration** > **Policy Management** > **Traffic Management** > **Filters**. You must assign the SSH In and SSH Out rules to the Public interface.

Step 7 Select Public from the **Filter List**.

Step 8 Click **Assign Rules to Filter**. The Configuration > Policy Management > Traffic Management > Assign Rules to Filter window appears.

Step 9 Select **SSH In** from the Available Filters list and then click **<< Add**.

Step 10 Select **SSH Out** from the Available Filters list and then click **<< Add**.

Step 11 Click **Done**.

Step 12 Go back to the main menu and then click **Logout**.

Configuring SSH on PIX Firewall Devices

- NOT SUPPORTED in this release. -

ISC needs a mechanism to securely deploy configuration files to PIX Firewall devices in the network.

Note SSH permits up to 100 characters in a username, and up to 50 characters in a password.

To configure SSH on a PIX Firewall device, perform the following steps:

	Command	Description
Step 1	`Pix#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Pix(config)#` **`domain-name`** *`<domain_name>`*	Specifies the IP domain name.
Step 3	`Pix(config)#` **`ca generate rsa key 1024`**	Generates the RSA key pair for the SSH session. A modulus size of 1,024 bits is recommended for use with the Cisco IOS Software. Key generation could take several minutes.
Step 4	`Pix(config)#` **`ca save all`**	Saves the RSA key pair to Flash memory.

	Command	Description
Step 5	`Pix(config)# ssh <ip_address> <subnet_mask> <interface>`	You can grant permission to one or more hosts to start an SSH session to the PIX Firewall through the specified interface (usually **outside** or **inside**). For example, with **ssh 128.107.128.108 255.255.255.255 outside** Also, you can permit all hosts in the specified subnet to establish an SSH session with the PIX Firewall through the specified interface. For example, **ssh 128.107.0.0 255.255.0.0 outside**
Step 6	`Pix(config)# write mem`	Saves the configuration changes.

When starting an SSH session, a dot (.) appears on the PIX Firewall console before the SSH user authentication prompt appears. For example:

```
pixfirewall(config)# .
```

The dot does not affect SSH functionality. The dot appears at the PIX Firewall console before authentication occurs when generating a server key or decrypting a message that uses private keys during an SSH exchange. These tasks can take up to two minutes or so. The dot is a progress indicator that verifies that the PIX Firewall is busy and not frozen.

Setting Up SNMP

To work with ISC, SNMP must be configured on each CPE device in the customer network. In ISC, SNMP is used to:

- collect from the Interface MIB
- provision and collect SLA data.

Two security models are available: SNMPv1/v2c and SNMPv3. Table 3-5 identifies the combinations of security models and levels.

Table 3-5 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Description
v1/v2c	No Authentication/ No Encryption	Community String	No	Uses a community string match for authentication.
v3	No Authentication/ No Encryption	Username	No	Uses a username match for authentication.
v3	Authentication/ No Encryption	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	Authentication/ Encryption	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms, and provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

SNMPv3 provides for both security models and security levels. A *security model* is an authentication strategy that is set up for a user and the group in which the user resides. A *security level* is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines the message is from a valid source.
- Encryption—Encoding the contents of a packet to prevent it from being read by an unauthorized source.

SNMPv3 objects have the following characteristics:

- Each user belongs to a group.
- The group defines the access policy for a set of users and determines the list of notifications its users can receive. The group also defines the security model and security level for its users.
- The access policy defines which SNMP objects can be accessed for reading, writing, or creation.

Setting Up SNMPv1/v2c on Cisco IOS Routers

To determine whether SNMP is enabled, and to set the SNMP community strings on a Cisco IOS router, perform the following steps for each router:

	Command	Description
Step 1	`Router>` **`enable`** `Router>` *`<enable_password>`*	Enters enable mode, and then enters the enable password.
Step 2	`Router#` **`show snmp`**	Check the output of the **show snmp** command to see whether the following statement is present: "`SNMP agent not enabled.`" If SNMP is not enabled, complete the steps in this procedure.
Step 3	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 4	`Router(config)#` **`snmp-server community`** *`<userstring>`* **`RO`**	Sets the community read-only string.
Step 5	`Router(config)#` **`snmp-server community`** *`<userstring>`* **`RW`**	Sets the community read-write string.
Step 6	`Router(config)#` **`Ctrl+Z`**	Returns to Privileged Exec mode.
Step 7	`Router#` **`copy running startup`**	Saves the configuration changes to NVRAM.

Tip The SNMP community strings defined in ISC for each target device must be identical to those configured on the device.

Setting SNMPv3 Parameters on Cisco IOS Routers

This section describes how to set the SNMPv3 parameters on Cisco IOS routers. SNMPv3 is only supported on IOS crypto images. For Authentication/Encryption, the IOS image must have DES56.

Tip The SNMP users defined in ISC for each target device must be identical to those configured on the device.

To check the existing SNMP configuration, use these commands in the router terminal session:

- **show snmp group**
- **show snmp user**

To set the SNMPv3 server group and user parameters on a Cisco IOS router, perform the following steps.

Note The group must be created first and then the user.

	Command	Description
Step 1	Router> **enable** Router> *<enable_password>*	Enters enable mode, then enter the enable password.
Step 2	Router# **configure terminal**	Enters global configuration mode.
Step 3	Router(config)# **snmp-server group** [*<groupname>* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}] [**read** *<readview>*] [**write** *<writeview>*] [**notify** *<notifyview>*] [**access** *<access-list>*]	The **snmp-server group** command configures a new SNMP group or a table that maps SNMP users to SNMP views. Each group belongs to a specific security level. Example: **snmp-server group v3auth v3 auth read v1default write v1default**
Step 4	Router(config)# **snmp-server user** *<username>* [*<groupname>* **remote** *<ip-address>* [**udp-port** *<port>*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *<auth-password>* [**priv des56** *<priv-password>*]] [**access** *<access-list>*]	The **snmp-server user** command configures a new user to an SNMP group. Example: **snmp-server user user1 v3auth v3 auth md5 user1Pass**
Step 5	Router(config)# **Ctrl+Z**	Returns to Privileged Exec mode.
Step 6	Router# **copy running startup**	Saves the configuration changes to NVRAM.

Manually Enabling RTR Responder on Cisco IOS Routers

Note SNMP must be configured on the router.

To manually enable an RTR Responder on a Cisco IOS router, execute the following steps:

	Command	Description
Step 1	Router> **enable** Router> *<enable_password>*	Enters enable mode, and then enters the enable password.
Step 2	Router# **configure terminal**	Enters the global configuration mode.
Step 3	Router(config)# **rtr responder**	Enables the SA responder on the target router of SA Agent operations.
Step 4	Router(config)# **Ctrl+Z**	Returns to Privileged Exec mode.
Step 5	Router# **copy running startup**	Saves the configuration changes to NVRAM.

Accessing the Devices Window

The Devices feature is used to create, edit, delete, and configure devices, and e-mail the device owner.

To access the Devices window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in Figure 3-37.

Figure 3-37 Devices List Window

The Devices window contains the following:

- **Device Name** Lists the fully qualified host and domain name of the device. You can sort the list of devices by device name.
- **Management IP Address** Lists the management IP address or the IE2100 address. You can sort the list of devices by this field.
- **Type** Lists the type of the device. Types include: Cisco IOS Device, CatOs Device, Terminal Server, VPN 3000 **- NOT SUPPORTED in this release. -**, PIX Firewall **- NOT SUPPORTED in this release. -**, and IE2100.

In the Devices window, you can create, edit, delete, or configure devices or e-mail the device owner using the following buttons:

- **Create** Click to create new devices. Enabled only if no devices are selected.
- **Edit** Click to edit selected device (select device by clicking the corresponding box). Enabled only if a single device is selected.
- **Delete** Click to delete selected device (select device by clicking the corresponding box). Enabled only if one or more devices are selected.

- **Config** Click to change the selected device configuration (select device by clicking the corresponding box). Enabled only if a single device is selected.
- **E-mail** Click to send e-mail to the owner of selected device (select device by clicking the corresponding box). Enabled only if one or more devices are selected.

Creating a Device

From the Create window, you can define different types of devices.

To create a device, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices**.

Step 2 Click the **Create** button.

The Create options appear, as shown in Figure 3-38.

Figure 3-38 Create Options Window

The **Create** options include the following:

- **Catalyst Switch** A Catalyst device running the Catalyst Operating System.
- **Cisco IOS Device** Any router that runs the Cisco IOS. This includes Catalyst devices running Cisco IOS.
- **Terminal Server** A device that represents the workstation that can be used to provision edge routers.
- **VPN 3000** Any router in the Cisco VPN 3000 Series Concentrator family. **- NOT SUPPORTED in this release. -**
- **Firewall** Any Cisco PIX Firewall. **- NOT SUPPORTED in this release. -**
- **IE2100** Any Cisco Intelligence Engine (IE) 2100 series network device.

Step 3 See the following sections for instructions on creating each type of device.

- Creating a Catalyst Switch, page 3-46

- Creating a Cisco IOS Device, page 3-52
- Creating a Terminal Server, page 3-58
- Creating a VPN 3000, page 3-63
- Creating a Firewall, page 3-66
- Creating a Cisco CNS IE2100, page 3-72

Creating a Catalyst Switch

To create a Catalyst switch, do the following:

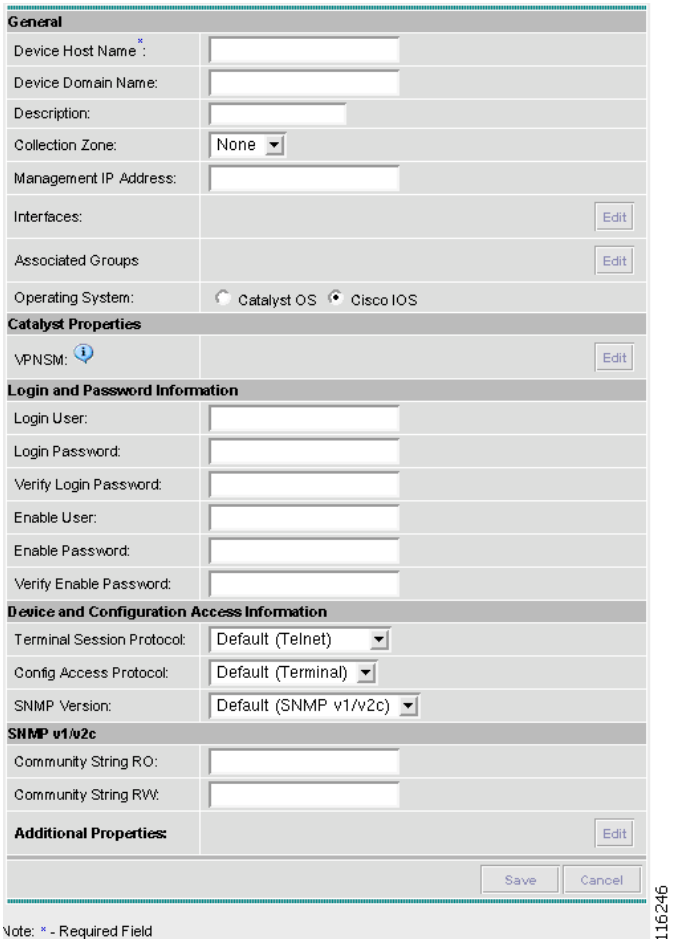
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **Catalyst Switch**.

The Create Catalyst Device window appears, as shown in Figure 3-39.

Figure 3-39 Create Catalyst Device Window



The General section of the Create Catalyst Device window contains the following fields:

- **Device Host Name** (required) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional) Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional) Drop-down list of all collection zones within the ISC. Choices include: None and all collection zones within the ISC. Default: None.
- **Management IP Address** (optional) Valid IP address of the device that ISC uses to configure the target router device.
- **Interfaces** (optional) Click the **Edit** button to view, add, edit, and delete all interfaces associated with the device. See Table 3-6 for a description of the Interfaces fields.

Table 3-6 Create Catalyst Device Interfaces Fields

Field	Description	Additional
Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
IP Address	IP address associated with this interface.	

Table 3-6 Create Catalyst Device Interfaces Fields (continued)

Field	Description	Additional
Port Type		NONE ACCESS TRUNK ROUTED
VLAN ID	The VLAN ID to assign to this interface.	

- **Associated Groups** (optional) Click the **Edit** button to view, add, and remove all Device Group associations.
- **Operating System** (optional) Click the radio button for the operating system currently running on the CAT switch. Choices include: CatOs or IOS. Default: CatOs. When you choose the IOS operating system, VPNSM is available under the heading Catalyst Properties.
- **VPNSM** (optional) This is only available if you chose the Operating System radio button of **Cisco IOS**. If you click the **Edit** button, an Edit Device VPNSM Blades window (for VPN Service Modules) appears. This is the only place to create a VPNSM. It uses this IOS operating system of the catalyst switch as a parent device. You can do the following:
  - **Create** Click this button and a VPNSM Blade window appears. Here you can enter the following:
  - **Name** (optional)
  - **Module Number** (required) The default is 1.

  After you enter this information, click **OK** and you return to the Edit Device VPNSM Blades window, which is updated to include the new information. (If you did not enter a Name, the default name is the *<device host name>*_VPNSM_*<module number>.)*
  - **Edit** Select the check box next to the VPNSM that you want to edit and click the **Edit** button. You receive a window with the current information about this VPNSM that you can edit. Then click **OK**.
  - **Delete** Select the check box(es) next to the VPNSM(s) you want to delete and click the **Delete** button. You receive a confirmation window in which you can click **OK** to complete the deletion or you can click **Cancel** to cancel the deletion.
  - **OK** Click **OK** and you return to the Create Catalyst Device window and the created VPNSM(s) are listed.
  - **Cancel** Click **Cancel** if you decide not to create a VPNSM.

The Login and Password Information section of the Create Catalyst Device window contains the following fields:

- **Login User** (optional) Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.

- **Verify Login Password** (optional) Displayed as stars (*). Must match the Login Password field. Limited to 80 characters.
- **Enable User** (optional) Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Enable Password** (optional) Displayed as stars (*). Must match the Enable Password field. Limited to 80 characters.

The Device and Configuration Access Information section of the Create Catalyst Device window contains the following fields:

- **Terminal Session Protocol** (optional) Configures the method of communication between ISC and the device. Choices include: Telnet, Secure Shell (SSH), and CNS. In previous versions of ISC, this field was called the Transport field. Default: The default set in the DCPL properties.
- **Config Access Protocol** (optional) Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, and FTP. Default: The default set in the DCPL properties.
- **SNMP Version** (optional) Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: The default set in the DCPL properties.

The SNMP v1/v2c section of the Create Catalyst Device window contains the following fields:

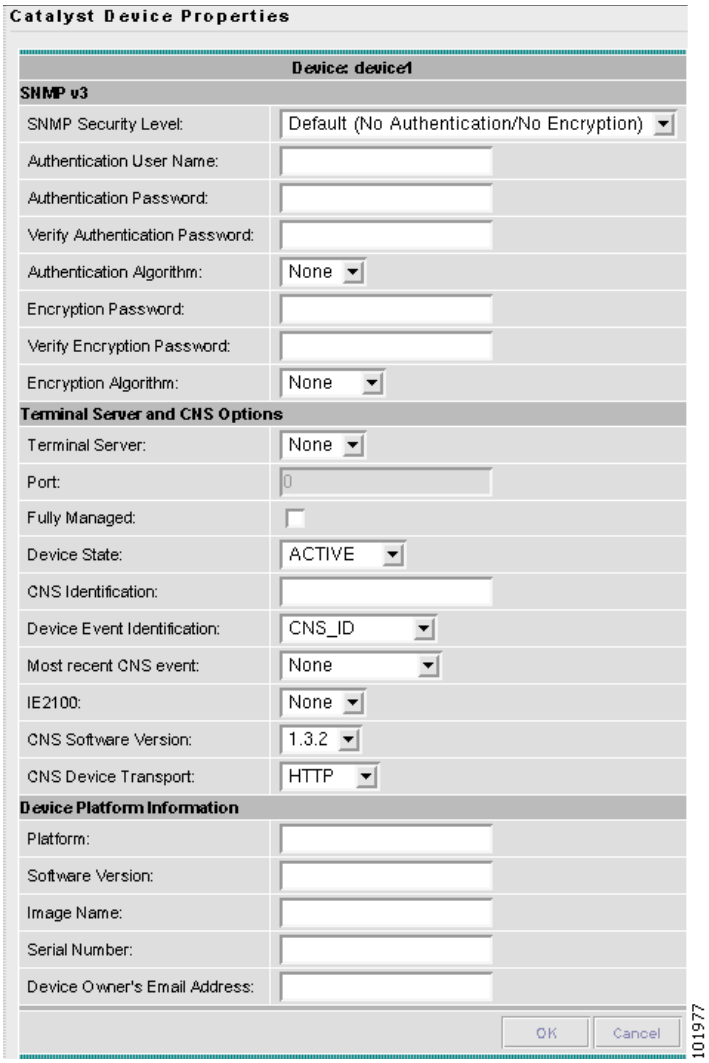
- **Community String RO** (optional) SNMP Read-Only Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW** (optional) SNMP Read-Write Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

Step 4 Enter the desired information for the Catalyst device you are creating.

Step 5 To access the Additional Properties section of the **Create Catalyst Device**, click **Edit**.

The Catalyst Device Properties window appears, as shown in Figure 3-40.

Figure 3-40 Catalyst Device Properties Window



The SNMP v3 section of the Catalyst Device Properties window contains the following fields:

- **SNMP Security Level** (optional) Choices include: Default (<*default_set_in_DCP*L>), Authentication/No Encryption, and Authentication/Encryption. Default: Default (<*default_set_in_DCP*L>). Note: When you change the DCPL property, the <*default_set_in_DCP*L> variable changes.
- **Authentication User Name** (optional) User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password** (optional) Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Authentication Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.

- **Authentication Algorithm** (optional) Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password** (optional) Displayed as stars (*). In previous versions of ISC, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Verify Encryption Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Encryption Algorithm** (optional) In previous versions of ISC, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

The Terminal Server and CNS Options section of the Catalyst Device Properties window contains the following fields:

- **Terminal Server** (optional) Choices include: None and the list of existing Terminal Server names. Default: None.
- **Port** (optional) Disabled until a Terminal Server is selected. Range: 0-65535. Default: 0.
- **Fully Managed** (optional) If the Fully Managed check box is selected, the device becomes a fully managed device. ISC performs additional management actions only for fully managed devices. These actions include e-mail notifications upon receipt of device configuration changes originated outside ISC and the scheduling of enforcement audit tasks upon detection of possible intrusion. Default: Not selected and therefore not selected.
- **Device State** (optional) Choices include: ACTIVE and INACTIVE. ACTIVE indicates that the router has been plugged on the network and can be part of ISC tasks such as collect config and provisioning. INACTIVE indicates the router has not been plugged-in. Default: ACTIVE.
- **CNS Identification** Required if the Device Event Identification field is set to CNS_ID. Only valid characters that Cisco IOS allows are alphanumeric characters and (.) (-) (_).
- **Device Event Identification** (optional) Indicates whether the CNS Identification field contains a HOST_NAME or CNS_ID. Default: HOST_NAME.
- **Most Recent CNS event** (optional) Choices include: None, CONNECT, and DISCONNECT. Changing from the default of None is not recommended. Note: The last connect or disconnect CNS TIBCO event received by ISC for each CNS-enabled IOS device is automatically recorded.
- **IE2100** (optional) Disabled unless the Device State field is INACTIVE or the Terminal Session Protocol field is CNS. A valid IE2100 must be selected if the Terminal Session Protocol is CNS. Choices include: None and the list of existing IE2100 names. Default: None.
- **CNS Software Version** (optional) Choices include: 1.3, 1.3.1, and 1.3.2. This is the release version of Cisco CNS Configuration Engine that manages the IOS device. Default: 1.3.2.
- **CNS Device Transport** (optional) Choices include: HTTP and HTTPS. This field determines what will be the transport mechanism used by ISC to create, delete, or edit devices in the IE2100 repository. If HTTPS is used, the Cisco CNS Configuration Engine must be running in secure mode. Default: HTTP.

The Device Platform Information section of the Catalyst Device Properties window contains the following fields:

- **Platform** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional) Should match what is configured on the target router device. Limited to 80 characters.

- **Image Name** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional) Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 6 Enter any desired Additional Properties information for the Catalyst device you are creating.

Step 7 Click **OK**.

Step 8 Click **Save**.

The Devices window reappears with the new Catalyst device listed.

Creating a Cisco IOS Device

To create a Cisco IOS device, do the following:

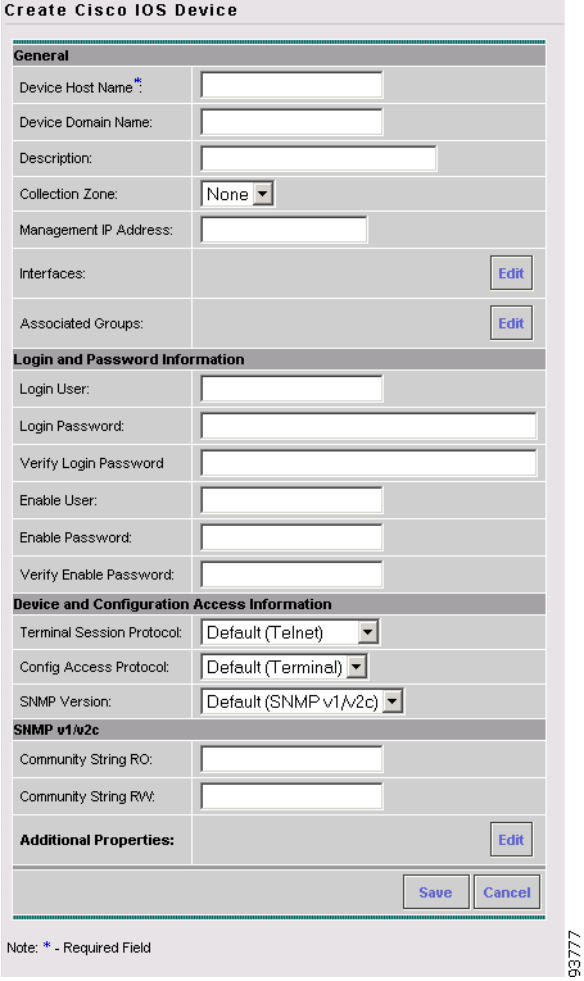
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **Cisco IOS Device**.

The Create Cisco IOS Device window appears, as shown in Figure 3-41.

Figure 3-41 Create Cisco IOS Device Window



The General section of the Create Cisco IOS Device window contains the following fields:

- **Device Host Name** Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional) Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional) Drop-down list of all collection zones within the ISC. Choices include: None and all collection zones within the ISC. Default: None.
- **Management IP Address** (optional) Valid IP address of the device that ISC uses to configure the target router device.
- **Interfaces** (optional) Click the Edit button to view, add, edit, and delete all interfaces associated with the device. See Table 3-7 for a description of the Interface fields.

Table 3-7 Create Cisco IOS Device Interface Fields

Field	Description	Additional
Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
IP Address	IP address associated with this interface.	

- **Associated Groups** (optional) Click the **Edit** button to view, add, and remove all Device Group associations.

The Login and Password Information section of the Create Cisco IOS Device window contains the following fields:

- **Login User** (optional) Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Login Password** (optional) Displayed as stars (*). Must match the Login Password field. Limited to 80 characters.
- **Enable User** (optional) Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Enable Password** (optional) Displayed as stars (*). Must match the Enable Password field. Limited to 80 characters.

The Device and Configuration Access Information section of the Create Cisco IOS Device window contains the following fields:

- **Terminal Session Protocol** (optional) Configures the method of communication between ISC and the device. Choices include: Telnet, Secure Shell (SSH), and CNS. In previous versions of ISC this
- **Config Access Protocol** (optional) Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, and FTP. Default: The default set in the DCPL properties.
- **SNMP Version** (optional) Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: The default set in the DCPL properties.

The SNMP v1/v2c section of the Create Cisco IOS Device window contains the following fields:

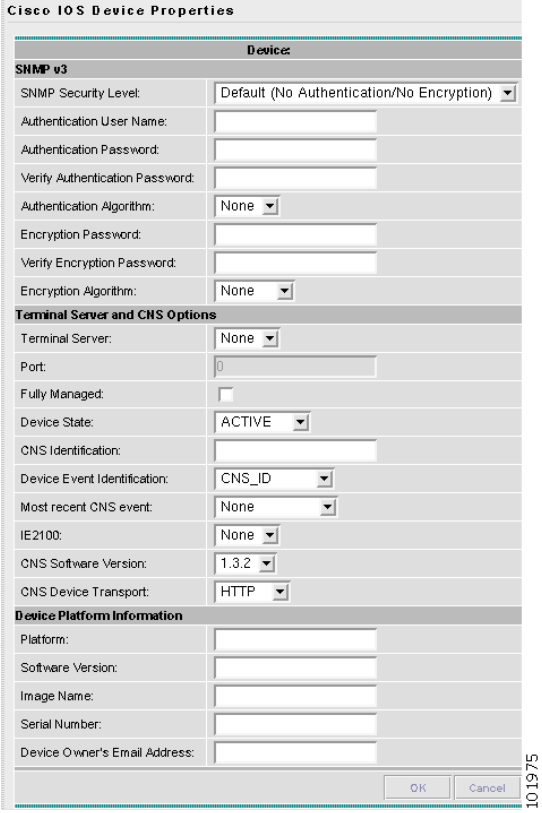
- **Community String RO** (optional) SNMP Read-Only Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW** (optional) SNMP Read-Write Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

Step 4 Enter the desired information for the Cisco IOS device you are creating.

Step 5 To access the Additional Properties section of the **Create Cisco IOS Device**, click **Edit**.

The Cisco IOS Device Properties window appears, as shown in Figure 3-42.

Figure 3-42 Cisco IOS Device Properties Window



The SNMP v3 section of the Cisco IOS Device Properties window contains the following fields:

- **SNMP Security Level** (optional) Choices include: Default (<*default_set_in_DCP*L>), Authentication/No Encryption, and Authentication/Encryption. Default: Default (<*default_set_in_DCP*L>). Note: When you change the DCPL property, the <*default_set_in_DCP*L> variable changes.
- **Authentication User Name** (optional) User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password** (optional) Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Authentication Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Authentication Algorithm** (optional) Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password** (optional) Displayed as stars (*). In previous versions of ISC, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.

- **Verify Encryption Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Encryption Algorithm** (optional) In previous versions of ISC, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

The Terminal Server and CNS Options section of the Cisco IOS Device Properties window contains the following fields:

- **Terminal Server** (optional) Choices include: None and the list of existing Terminal Server names. Default: None.
- **Port** (optional) Disabled until a Terminal Server is selected. Range: 0-65535. Default: 0.
- **Fully Managed** (optional) If the Fully Managed check box is selected, the device becomes a fully managed device. ISC performs additional management actions only for fully managed devices. These actions include e-mail notifications upon receipt of device configuration changes originated outside ISC and the scheduling of enforcement audit tasks upon detection of possible intrusion. Default: Not selected and therefore not selected.
- **Device State** (optional) Choices include: ACTIVE and INACTIVE. ACTIVE indicates that the router has been plugged on the network and can be part of ISC tasks such as collect config and provisioning. INACTIVE indicates the router has not been plugged-in. Default: ACTIVE.
- **CNS Identification** Required if the Device Event Identification field is set to CNS_ID. Only valid characters that Cisco IOS allows are alphanumeric characters and (.) (-) (_).
- **Device Event Identification** (optional) Indicates whether the CNS Identification field contains a HOST_NAME or CNS_ID. Default: HOST_NAME.
- **Most Recent CNS event** (optional) Choices include: None, CONNECT, and DISCONNECT. Changing from the default of None is not recommended. Note: The last connect or disconnect CNS TIBCO event received by ISC for each CNS-enabled IOS device is automatically recorded.
- **IE2100** (optional) Disabled unless the Device State field is INACTIVE or the Terminal Session Protocol field is CNS. A valid IE2100 must be selected if the Terminal Session Protocol is CNS. Choices include: None and the list of existing IE2100 names. Default: None.
- **CNS Software Version** (optional) Choices include: 1.3, 1.3.1, 1.3.2, and 1.4. This is the release version of Cisco CNS Configuration Engine that manages the IOS device. Default: 1.3.2.
- **CNS Device Transport** (optional) Choices include: HTTP and HTTPS. This field determines what will be the transport mechanism used by ISC to create, delete, or edit devices in the IE2100 repository. If HTTPS is used, the Cisco CNS Configuration Engine must be running in secure mode. Default: HTTP.

The Device Platform Information section of the Cisco IOS Device Properties window contains the following fields:

- **Platform** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name** (optional) Should match what is configured on the target router device. Limited to 80 characters.

- **Serial Number** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional) Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 6 Enter any desired Additional Properties information for the Cisco IOS device you are creating.

Step 7 Click **OK**.

Step 8 Click **Save**.

The Devices window reappears with the new Cisco IOS device listed.

Creating a Terminal Server

To create a Terminal Server device, do the following:

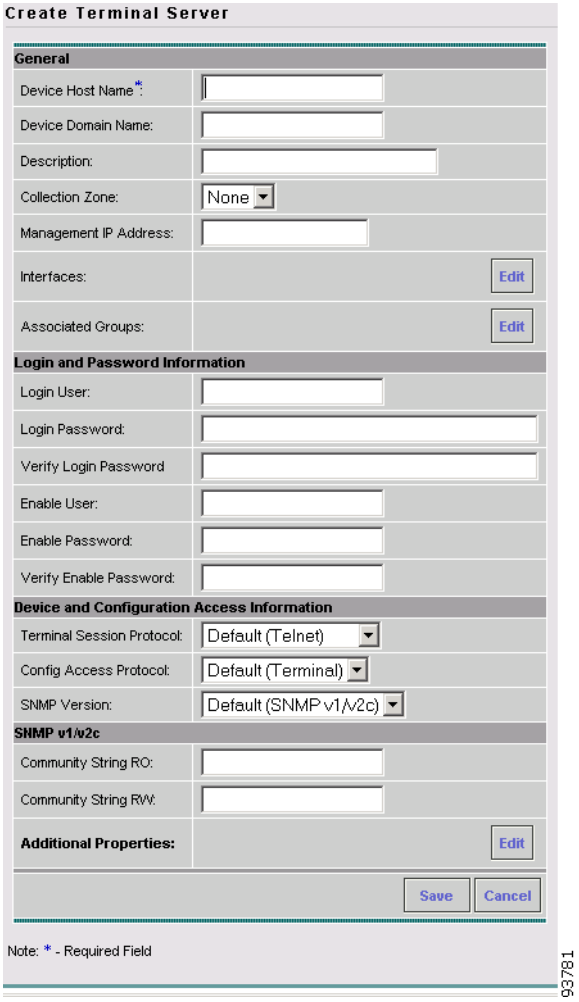
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **Terminal Server**.

The Create Terminal Server window appears, as shown in Figure 3-43.

Figure 3-43 Create Terminal Server Window



The General section of the Create Terminal Server window contains the following fields:

- **Device Host Name** (required) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional) Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional) Drop-down list of all collection zones within the ISC. Choices include: None and all collection zones within the ISC. Default: None.
- **Management IP Address** (optional) Valid IP address of the device that ISC uses to configure the target router device.

- **Interfaces** (optional) Click the **Edit** button to view, add, edit, and delete all interfaces associated with the device. See Table 3-8 for a description of the Interfaces fields.

Table 3-8 Create Terminal Server Device Interfaces Fields

Field	Description	Additional
Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
IP Address	IP address associated with this interface.	

- **Associated Groups** (optional) Click the **Edit** button to view, add, and remove all Device Group associations.

The Login and Password Information section of the Create Terminal Server window contains the following fields:

- **Login User** (optional) Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Login Password** (optional) Displayed as stars (*). Must match the Login Password field. Limited to 80 characters.

- **Enable User** (optional) Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Enable Password** (optional) Displayed as stars (*). Must match the Enable Password field. Limited to 80 characters.

The Device and Configuration Access Information section of the Create Terminal Server window contains the following fields:

- **Terminal Session Protocol** (optional) Configures the method of communication between ISC and the device. Choices include: Telnet, Secure Shell (SSH), CNS, and RSH. In previous versions of ISC, this field was called the Transport field. Default: The default set in the DCPL properties.
- **Config Access Protocol** (optional) Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, FTP, and RCP. Default: The default set in the DCPL properties.
- **SNMP Version** (optional) Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: The default set in the DCPL properties.

The SNMP v1/v2c section of the Create Terminal Server window contains the following fields:

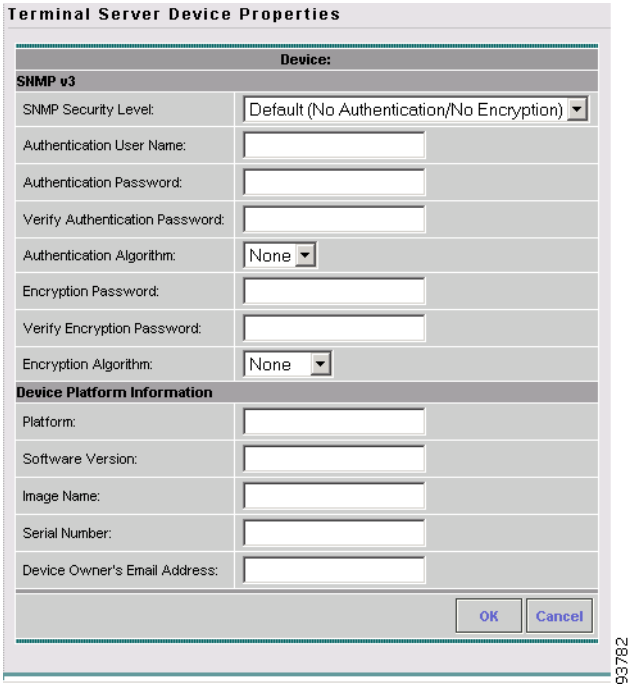
- **Community String RO** (optional) SNMP Read-Only Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW** (optional) SNMP Read-Write Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

Step 4 Enter the desired information for the Terminal Server you are creating.

Step 5 To access the Additional Properties section of the **Create Terminal Server**, click **Edit**.

The Terminal Server Device Properties window appears, as shown in Figure 3-44.

Figure 3-44 Terminal Server Device Properties Window



The SNMP v3 section of the Terminal Server Device Properties window contains the following fields:

- **SNMP Security Level** (optional) Choices include: Default (<*default_set_in_DCP*L>), Authentication/No Encryption, and Authentication/Encryption. Default: Default (<*default_set_in_DCP*L>). Note: When you change the DCPL property, the <*default_set_in_DCP*L> variable changes.
- **Authentication User Name** (optional) User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password** (optional) Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Authentication Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Authentication Algorithm** (optional) Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password** (optional) Displayed as stars (*). In previous versions of ISC, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.

- **Verify Encryption Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Encryption Algorithm** (optional) In previous versions of ISC, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

The Device Platform Information section of the Terminal Server Device Properties window contains the following fields:

- **Platform** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional) Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 6 Enter any desired Additional Properties information for the Terminal Server device you are creating.

Step 7 Click **OK**.

Step 8 Click **Save**.

The Devices window reappears with the new Terminal Server device listed.

Creating a VPN 3000

- NOT SUPPORTED in this release. -

To create a VPN 3000 device, do the following:

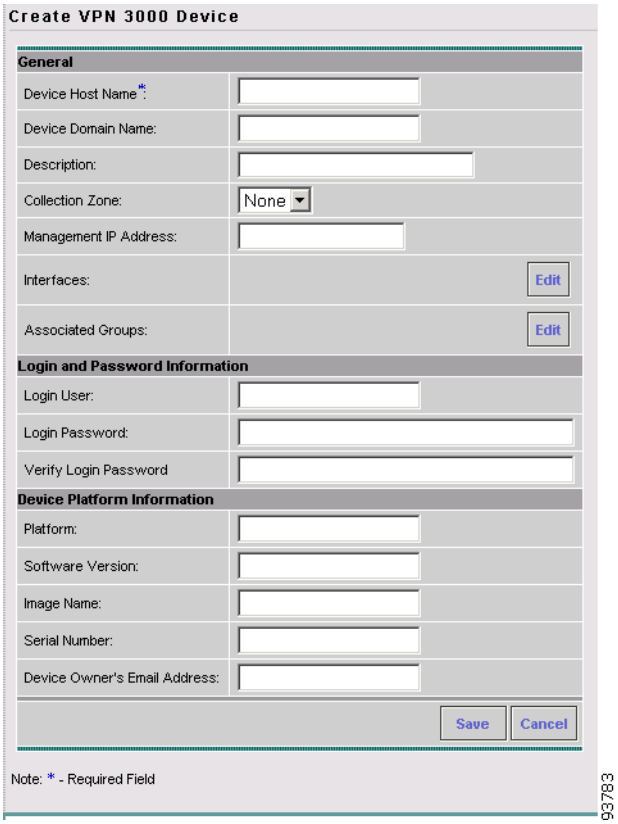
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **VPN 3000**.

The Create VPN 3000 Device window appears, as shown in Figure 3-45.

Figure 3-45 Create VPN 3000 Device Window



The General section of the Create VPN 3000 Device window contains the following fields:

- **Device Host Name** (required) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 255 characters.
- **Device Domain Name** (optional) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional) Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional) Drop- down list of all collection zones within the ISC. Choices include: None and all collection zones within the ISC. Default: None.
- **Management IP Address** (optional) Valid IP address of the device that ISC uses to configure the target router device.

- **Interfaces** (optional) Click the **Edit** button to view, add, edit, and delete all interfaces associated with the device. See Table 3-9 for a description of the Interfaces fields.

Table 3-9 Create VPN 3000 Device Interfaces Fields

Field	Description	Additional
Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
IP Address	IP address associated with this interface.	

- **Associated Groups** (optional) Click the **Edit** button to view, add, and remove all Device Group associations.

The Login and Password Information section of the Create VPN 3000 Device window contains the following fields:

- **Login User** (optional) Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Login Password** (optional) Displayed as stars (*). Must match the Login Password field. Limited to 80 characters.

The Device Platform Information section of the Create VPN 3000 Device window contains the following fields:

- **Platform** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional) Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 4 Enter the desired information for the VPN 3000 device you are creating.

Step 5 Click **Save**.

The Devices window reappears with the new VPN 3000 device listed.

Creating a Firewall

- NOT SUPPORTED in this release. -

To create a PIX Firewall, do the following:

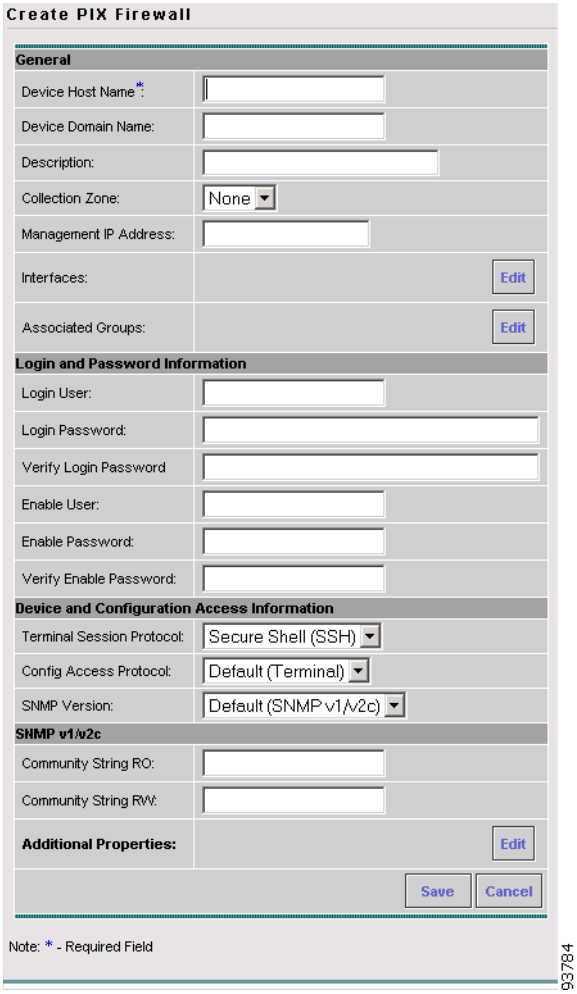
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **Firewall**.

The Create PIX Firewall window appears, as shown in Figure 3-46.

Figure 3-46 Create PIX Firewall Window



The General section of the Create PIX Firewall window contains the following fields:

- **Device Host Name** (required) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 256 characters.
- **Description** (optional) Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional) Drop-down list of all collection zones within the ISC. Choices include: None and all collection zones within the ISC. Default: None.
- **Management IP Address** (optional) Valid IP address of the device that ISC uses to configure the target router device.

- **Interfaces** (optional) Click the **Edit** button to view, add, edit, and delete all interfaces associated with the device. See Table 3-10 for a description of the Interfaces fields.

Table 3-10 Create PIX Firewall Device Interfaces Fields

Field	Description	Additional
Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
IP Address	IP address associated with this interface.	

- **Associated Groups** (optional) Click the **Edit** button to view, add, and remove all Device Group associations.

The Login and Password Information section of the Create PIX Firewall window contains the following fields:

- **Login User** (optional) Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Login Password** (optional) Displayed as stars (*). Must match the Login Password field. Limited to 80 characters.

- **Enable User** (optional) Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Enable Password** (optional) Displayed as stars (*). Must match the Enable Password field. Limited to 80 characters.

The Device and Configuration Access Information section of the Create PIX Firewall window contains the following fields:

- **Terminal Session Protocol** (optional) Configures the method of communication between ISC and the device. Choices include: Telnet, Secure Shell (SSH), and CNS. In previous versions of ISC, this field was called the Transport field. Default: The default set in the DCPL properties.
- **Config Access Protocol** (optional) Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, and FTP. Default: The default set in the DCPL properties.
- **SNMP Version** (optional) Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: The default set in the DCPL properties.

The SNMP v1/v2c section of the Create PIX Firewall window contains the following fields:

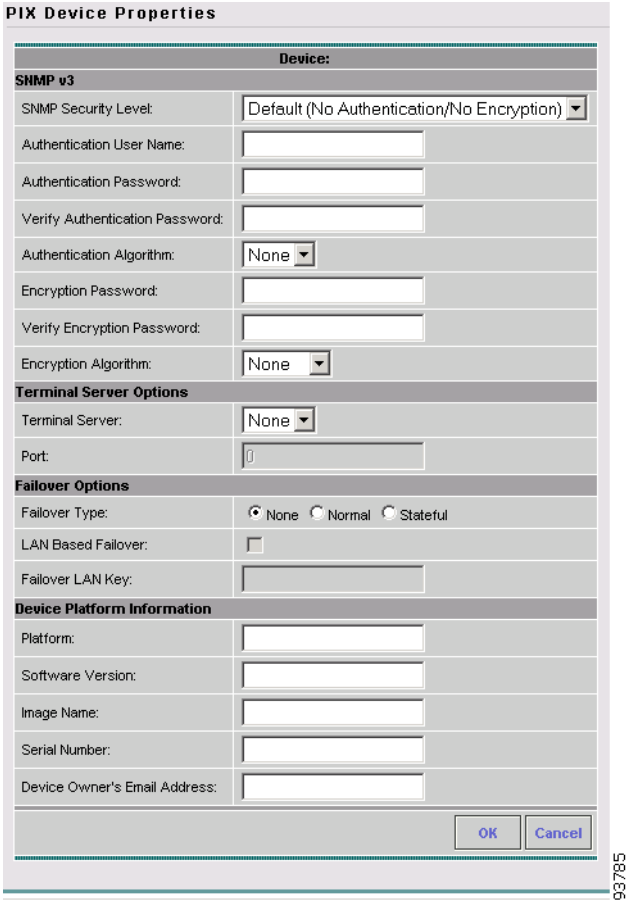
- **Community String RO** (optional) SNMP Read-Only Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW** (optional) SNMP Read-Write Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

Step 4 Enter the desired information for the PIX Firewall device you are creating.

Step 5 To access the Additional Properties section of the **Create PIX Firewall**, click **Edit**.

The PIX Device Properties window appears, as shown in Figure 3-47.

Figure 3-47 PIX Device Properties Window



The SNMP v3 section of the PIX Device Properties window contains the following fields:

- **SNMP Security Level** (optional) Choices include: Default (<*default_set_in_DCP*L>), Authentication/No Encryption, and Authentication/Encryption. Default: Default (<*default_set_in_DCP*L>). Note: When you change the DCPL property, the <*default_set_in_DCP*L> variable changes.
- **Authentication User Name** (optional) User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password** (optional) Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Authentication Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Authentication Algorithm** (optional) Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.

- **Encryption Password** (optional) Displayed as stars (*). In previous versions of ISC, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Verify Encryption Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Encryption Algorithm** (optional) In previous versions of ISC, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

The Terminal Server Options section of the PIX Device Properties window contains the following fields:

- **Terminal Server** (optional) Choices include: None and the list of existing Terminal Server names. Default: None.
- **Port** (optional) Disabled until a Terminal Server is selected. Range: 0-65535. Default: 0.

The Failover Options section of the PIX Device Properties window contains the following fields:

- **Failover Type** Determines whether failover is enabled for this PIX device. Choices: None, Normal, and Stateful. Default: None.
- **LAN Based Failover** (optional) Enabled only if the Failover Type is Normal or Stateful.
- **Failover LAN Key** (optional) The key used in LAN based Failover. Limited to 20 characters.

The Device Platform Information section of the PIX Device Properties window contains the following fields:

- **Platform** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional) Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 6 Enter any desired Additional Properties information for the PIX Firewall device you are creating.

Step 7 Click **OK**.

Step 8 Click **Save**.

The Devices window reappears with the new PIX Firewall device listed.

Creating a Cisco CNS IE2100

Note To use the Cisco CNS IE2100 functionality on ISC, you must first set up the Cisco CNS IE2100 appliance and the ISC workstation as explained in Appendix B, "Setting Up Cisco CNS IE2100 Appliances Running Cisco CNS Configuration Engine 1.3 Software with ISC" in *Cisco IP Solution Center Installation Guide*. You must also create a Cisco IOS device to communicate with the Cisco CNS IE2100 appliance. See Appendix A, "Setting Up Oracle for ISC," in *Cisco IP Solution Center Installation Guide*.

To create a Cisco CNS IE2100 appliance, do the following:

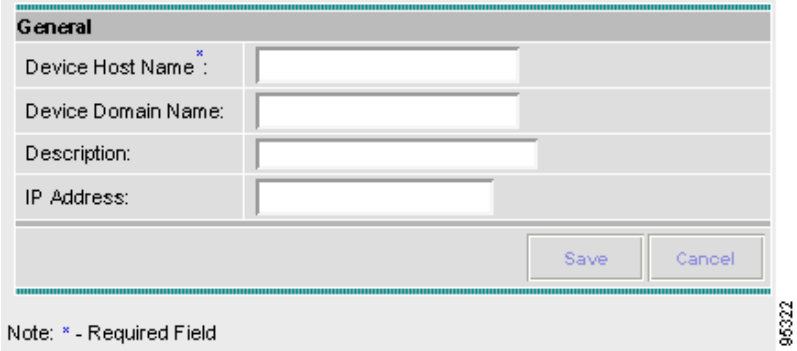
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **IE2100**.

The Create IE2100 Device window appears, as shown in Figure 3-48.

Figure 3-48 Create IE2100 Device Window



The General section of the Create IE2100 Device window contains the following fields:

- **Device Host Name** (required) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional) Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **IP Address** (optional) Valid IP address of the Cisco CNS IE2100 device that ISC uses to configure the target router device.

Step 4 Enter the desired information for the Cisco CNS IE2100 device you are creating.

Step 5 Click **Save**.

The Devices window reappears with the new Cisco CNS IE2100 device listed.

Editing a Device

From the Edit window, you can modify the fields that have been specified for a particular device.

To access the Edit window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in Figure 3-49.

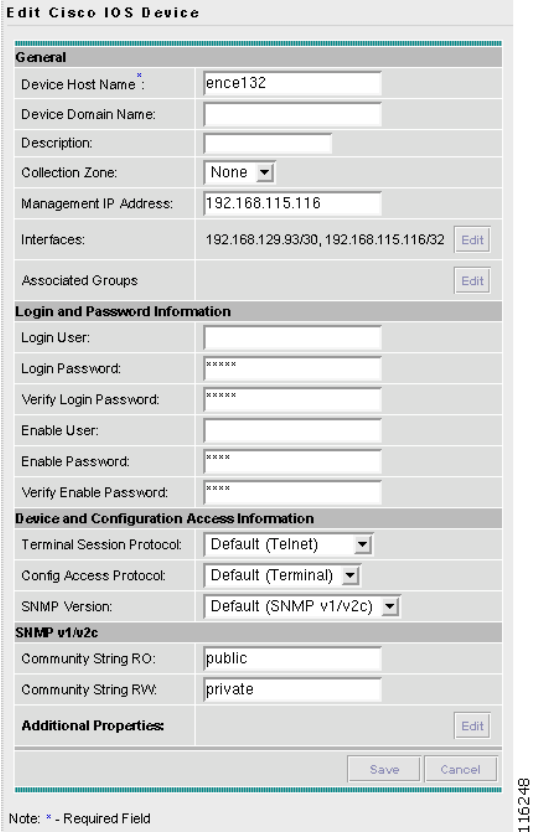
Figure 3-49 Devices List Window

Step 2 Select a single device to edit by selecting the box to the left of the Device Name. You can also select a device to edit by clicking on the hyper link of the device name.

Step 3 Click the **Edit** button. This button is only enabled if a device is selected.

The Edit window appropriate to the type of device selected appears. For example, if you selected a Cisco IOS device the Edit Cisco IOS Device window appears, as shown in Figure 3-50.

Figure 3-50 Editing a Device Window



Step 4 Enter the changes you want to make to the selected device.

Step 5 Click **Save**.

The changes are saved and the Devices window reappears.

Deleting Devices

From the Delete window, you can remove selected devices from the database.

To access the Delete window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in Figure 3-51.

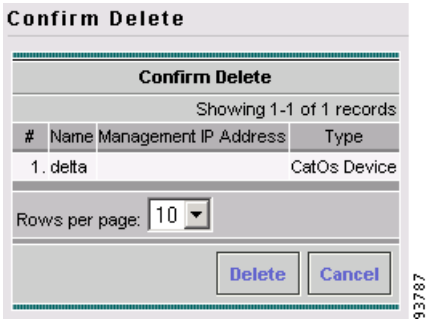
Figure 3-51 Devices List Window

Step 2 Select one or more devices to delete by selecting the check box(es) to the left of the Device Name(s).

Step 3 Click the **Delete** button. This button is only enabled if one or more devices are selected.

The Confirm Delete window appears, as shown in Figure 3-52.

Figure 3-52 Confirm Delete Window



Step 4 Click the **Delete** button to confirm that you want to delete the device(s) listed.

The Devices window reappears with the specified device(s) deleted.

Editing a Device Configuration

From the Config window, you can edit the configuration for a specified device.

To access the Config window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in Figure 3-53.

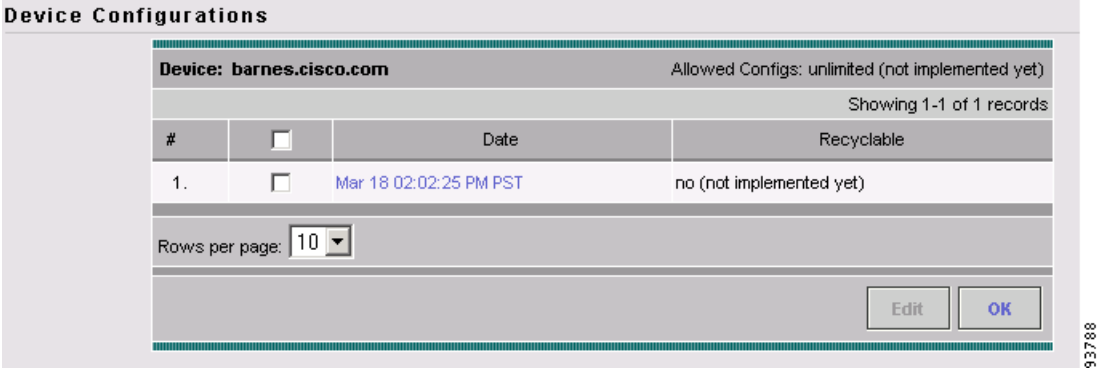
Figure 3-53 Devices List Window

Step 2 Select a single device to modify by selecting the check box to the left of the Device Name.

Step 3 Click the **Config** button.

The Device Configurations window for the selected device appears, as shown in Figure 3-54.

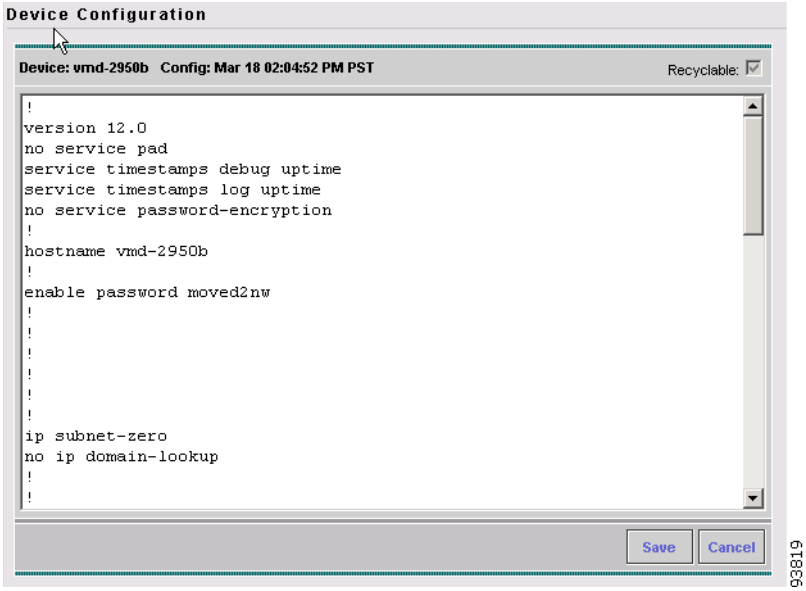
Figure 3-54 Device Configurations Window



Step 4 Select the box to the left of the Date for the configuration that you want to modify and click the **Edit** button. This button is only enabled if a device is selected.

The Device Configuration window for the selected device appears, as shown in Figure 3-55.

Figure 3-55 Device Configuration Window



Step 5 Enter the changes you want to make to the selected device configuration.

Step 6 Click **Save**.

The changes are saved and the Device Configurations window reappears.

Step 7 Click OK to return to the Devices window.

E-mailing a Device's Owner

From the E-mail window, you can send a device report via e-mail to the owners of specified devices.

To access the E-mail window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in Figure 3-56.

Figure 3-56 Devices List Window

Step 2 Select the devices for which you want to send a device report by selecting the check box(es) to the left of the Device Name(s).

Step 3 Click the **E-Mail** button. This button is only enabled if one or more devices are selected.

The Send Mail to Device Owners window appears, as shown in Figure 3-57.

Figure 3-57 Send Mail to Device Owners Window

Step 4 Compose the e-mail that you want to send to the selected device owners.

Step 5 Click **Send**.

The e-mail is sent and the Devices window reappears.

Copying a Device

From the Copy window, you receive a copy of the chosen device and can name it and change values.

To access the Copy window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in Figure 3-58.

Figure 3-58 Devices List Window

Step 2 Select a single device to copy by selecting the check box to the left of the Device Name.

Step 3 Click the **Copy** button. This button is only enabled if a device is selected.

A window appropriate to the type of device selected to copy appears. You receive an exact copy of the selected device but the Name, Management IP Address, all Interfaces, and VPNSM blades for a Catalyst Switch running Cisco IOS are blanked out and you must fill in the required information and save this new device. See the "Creating a Device" section on page 3-45 for specifics.

Device Groups

Every network element that ISC manages must be defined as a device in the system. After you have defined your network elements as devices, you can organize the devices into groups for collection and management purposes.

This section describes how to create, edit, and delete device groups and e-mail device group owners. This section includes the following:

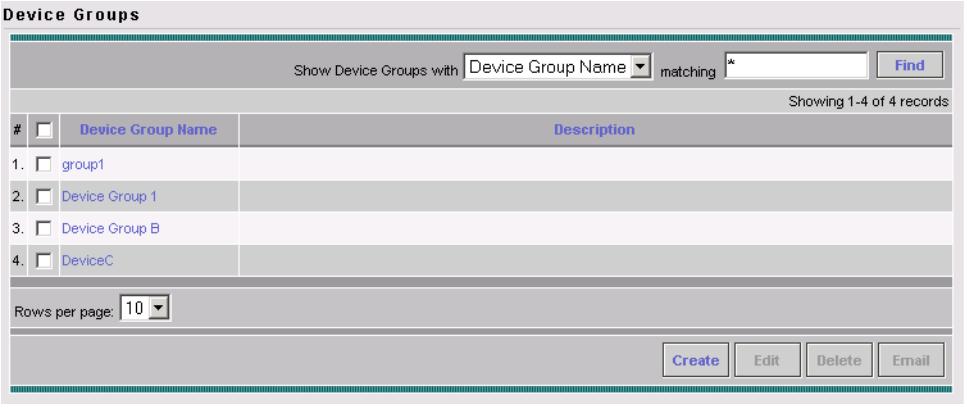
Accessing the Device Groups Window

The Device Groups feature is used to create, edit, and delete device groups and e-mail device group owners.

To access the Device Groups window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Device Groups** to access the Device Groups window shown in Figure 3-59.

Figure 3-59 Device Groups Window



The Device Groups window contains the following:

- **Device Group Name** Lists the name of the device group. You can sort the list by device group name.
- **Description** Lists the description of the device group.

From the Device Groups window, you can create, edit, or delete device groups or e-mail device group owners using the following buttons:

- **Create** Click to create new device groups. Enabled only if no device group is selected.
- **Edit** Click to edit a selected device group (select device group by clicking the corresponding box). Enabled only if a single device group is selected.
- **Delete** Click to delete selected device group(s) (select device group by clicking the corresponding box). Enabled only if one or more device groups are selected.
- **E-mail** Click to send e-mail to the owner of a selected device group (select device group by clicking the corresponding box). Enabled only if one or more device groups are selected.

Creating a Device Group

From the Create Device Group window, you can create different device groups.

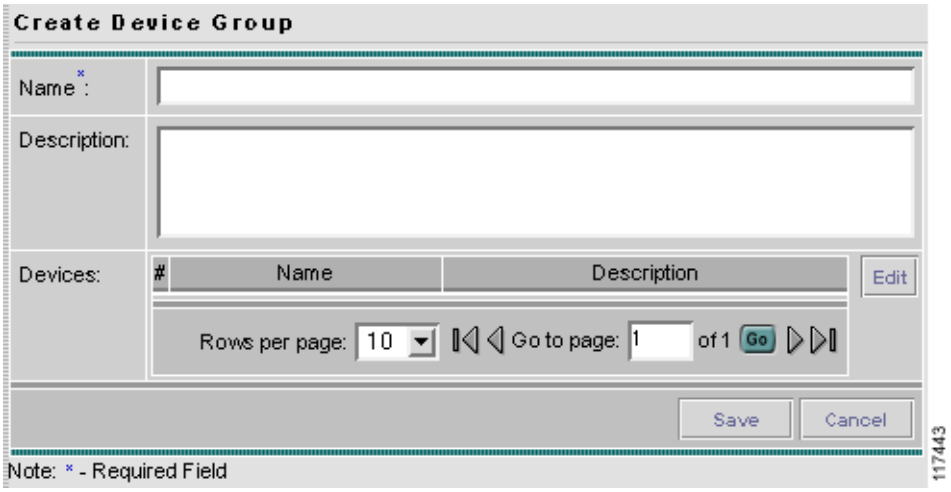
To create a device group, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Device Groups**.

Step 2 Click the **Create** button.

The Create Device Group window appears, as shown in Figure 3-60.

Figure 3-60 Create Device Group Window



The Create Device Group window contains the following fields:

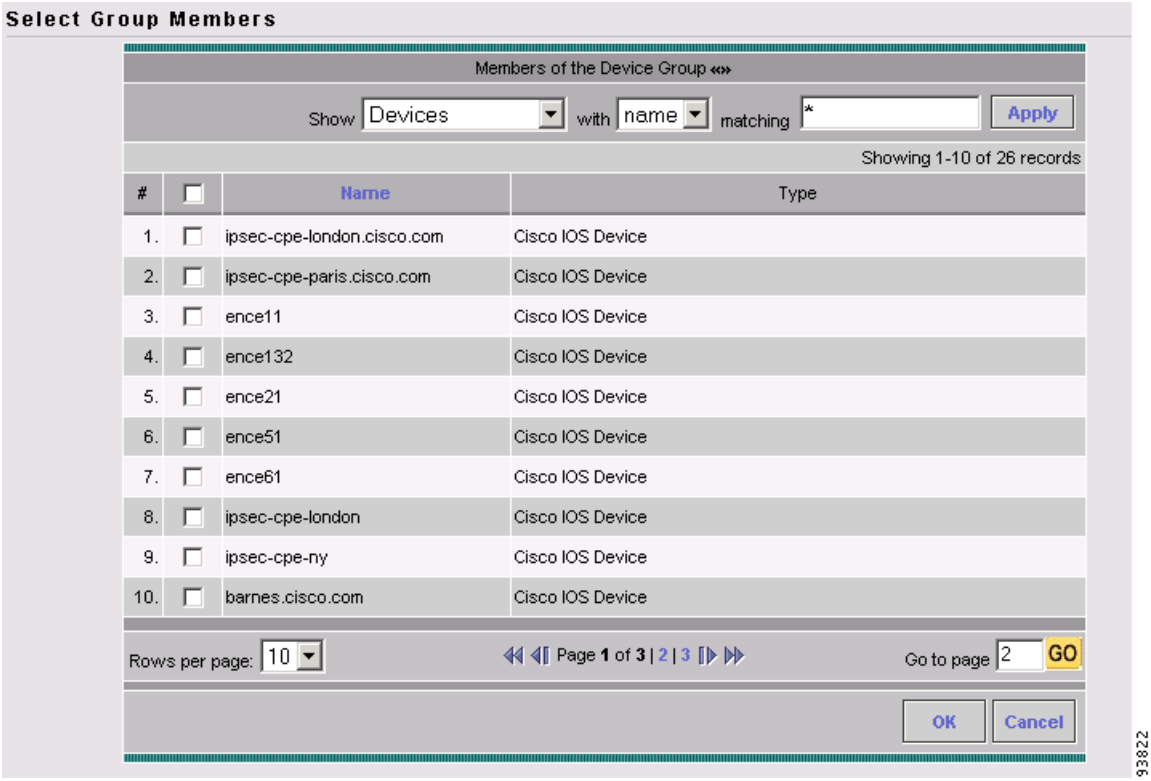
- **Name** (required) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. Limited to 80 characters.
- **Description** (optional) Any pertinent information about the device group that could be helpful to service provider operators. Limited to 512 characters.

Step 3 Enter the name and the description of the Device Group that you are creating.

Step 4 Click **Edit**.

The Select Group Members window appears, as shown in Figure 3-61.

Figure 3-61 Select Group Members Window

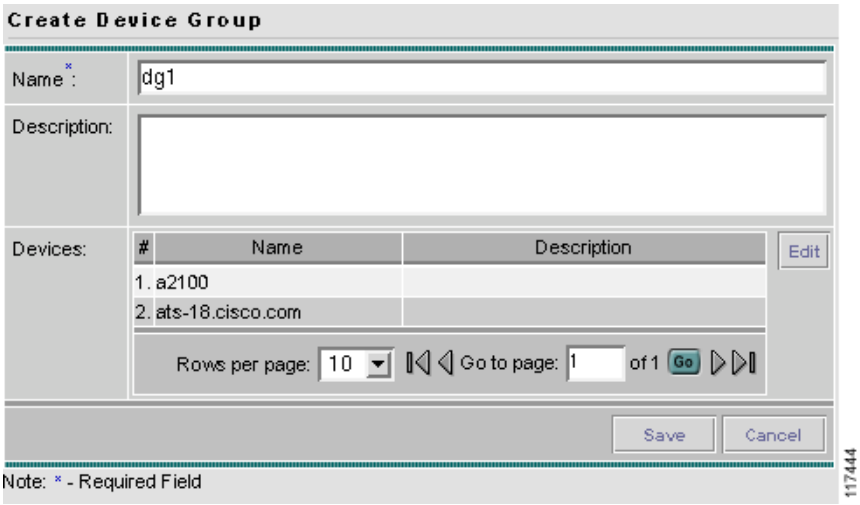


Step 5 Select the devices that you want to be group members by selecting the check box to the left of the device name.

Step 6 Click **OK**.

The Create Device Group window appears listing the selected devices, as shown in Figure 3-62.

Figure 3-62 Create Device Group Window



Step 7 Click **Save**.

The Device Groups window reappears with the new device group listed.

Editing a Device Group

From the Edit Device Group window, you can modify the fields that have been specified for a particular device group.

To access the Edit Device Group window, do the following:

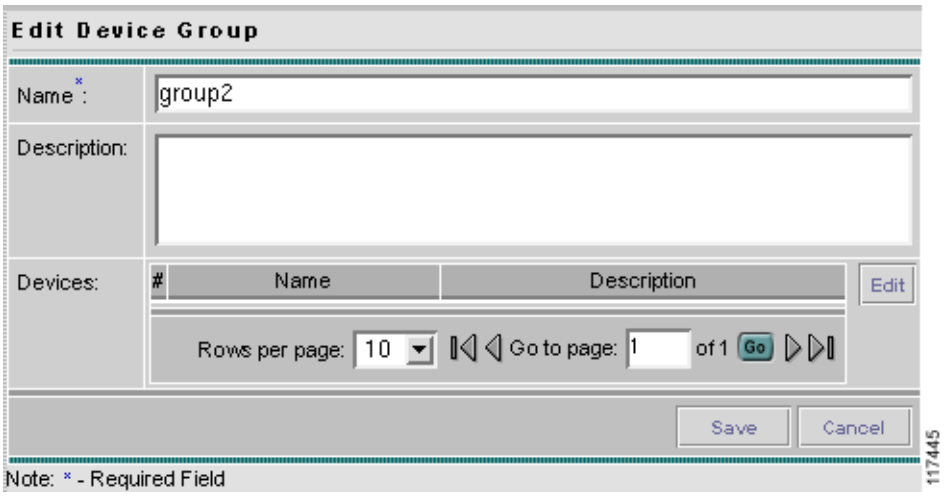
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Device Groups**.

Step 2 Select a single device group to modify by selecting the check box to the left of the Device Group Name.

Step 3 Click the **Edit** button. This button is only enabled if a device group is selected.

The Edit Device Group window appears, as shown in Figure 3-63.

Figure 3-63 Edit Device Group Window



Step 4 Enter the changes you want to make to the selected device group.

Step 5 Click **Save**.

The changes are saved and the Device Groups window reappears.

Deleting Device Groups

From the Delete window, you can remove selected device groups from the database.

To access the Delete window, do the following:

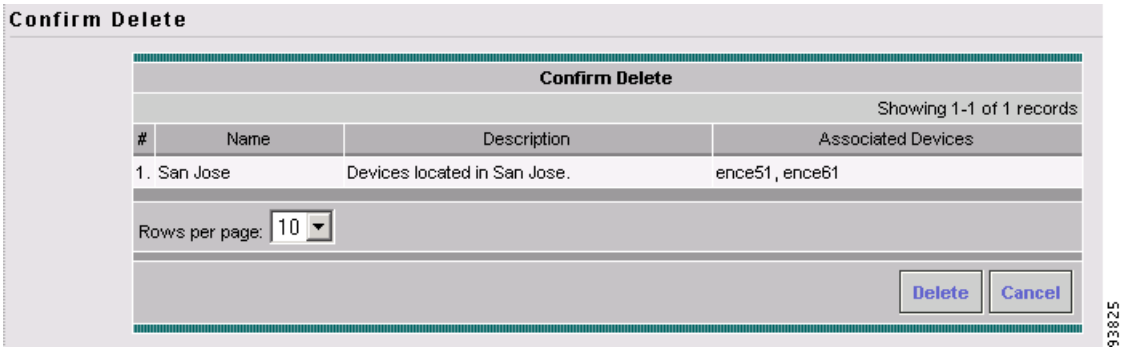
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Device Groups.**

Step 2 Select one or more device groups to delete by selecting the check box(es) to the left of the Device Group Names.

Step 3 Click the **Delete** button. This button is only enabled if one or more device groups are selected.

The Confirm Delete window appears, as shown in Figure 3-64.

Figure 3-64 Confirm Delete Window



Step 4 Click the **Delete** button to confirm that you want to delete the device group(s) listed.

The Device Groups window reappears with the specified device group(s) deleted.

E-mailing a Device Group

From the E-mail window, you can send a device report via e-mail to the owners of specified device groups.

To access the E-mail window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Device Groups**.

Step 2 Select the device groups for which you want to send a device report by selecting the check box to the left of the Device Group Name.

Step 3 Click the **E-Mail** button. This button is only enabled if one or more device groups are selected.

The Send Mail to Device owners of selected groups window appears, as shown in Figure 3-65.

Figure 3-65 Send Mail to Device Owners of Selected Groups Window

Step 4 Compose the e-mail that you want to send to the selected device group owners.

Step 5 Click **Send**.

The e-mail is sent and the Device Groups window reappears.

Customers

A customer site is a set of IP systems with mutual IP connectivity between them without the use of a VPN. Each customer site belongs to exactly one customer. A customer site can contain one or more (for load balancing) edge device routers. This section describes how to create, edit, and delete customers. This section includes the following:

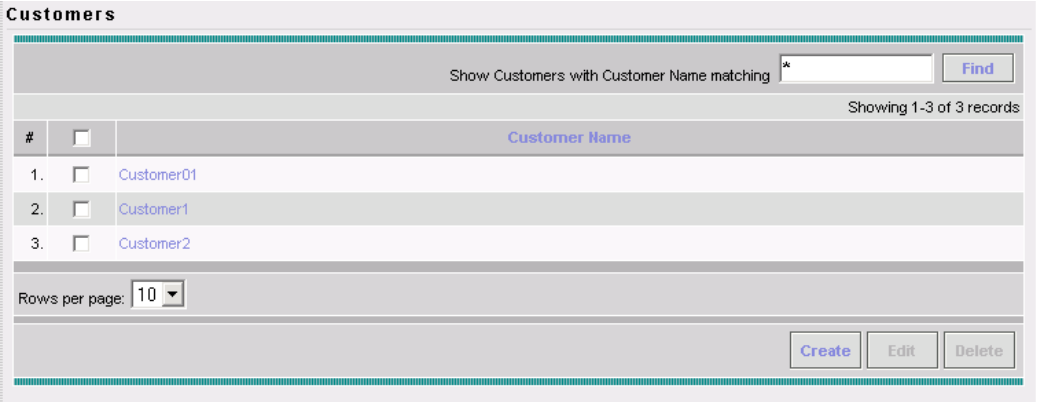
Accessing the Customers Window

The Customers feature is used to create, edit, and delete customers.

To access the Customers window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Customers** to access the Customers window shown in Figure 3-66.

Figure 3-66 Customers Window



The Customers window contains the following:

- **Customer Name** Lists the names of customers. You can sort the list by customer name.

From the Customers window, you can create, edit, or delete customers using the following buttons:

- **Create** Click to create new customers.
- **Edit** Click to edit selected customer (select by clicking the corresponding box). Enabled only if a single customer is selected.
- **Delete** Click to delete selected customer (select customer by clicking the corresponding box). Enabled only if one or more customers are selected.

Creating a Customer

From the Create Customer window, you can create different customers.

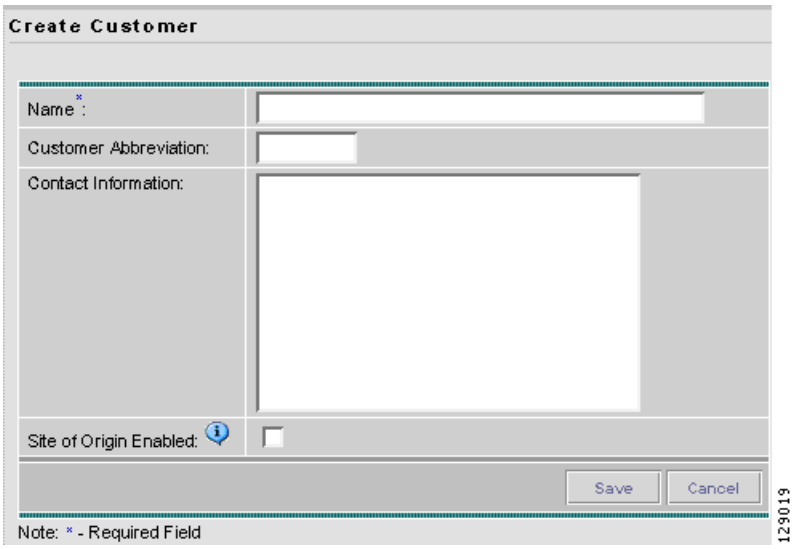
To create a customer, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Customers**.

Step 2 Click the **Create** button.

The Create Customer window appears, as shown in Figure 3-67.

Figure 3-67 Create Customer Window



The Create Customer window contains the following fields:

- **Name** (required) Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters.
- **Customer Abbreviation** This field in used only for L2VPN and L2TPv3 Frame Relay service requests. The entry in this field is used to construct a connect name. When this field is left blank, DLCI switching is the transport mode used. Limited to 10 characters.
- **Customer Information** (optional) Any pertinent information about the customer that could be helpful to service provider operators. Limited to 5256 characters.
- **Site of Origin Enabled** (optional) This check box appears only when you have MPLS permissions. Select this check box to enable the site of origin.

Step 3 Enter the name and information for the Customer that you are creating. Select the **Site of Origin Enabled** check box if you want this enabled.

Step 4 Click **Save**.

The Customers window reappears with the new customer listed.

Editing a Customer

From the Edit Customer window, you can modify the fields that have been specified for a particular customer.

To access the Edit Customer window, do the following:

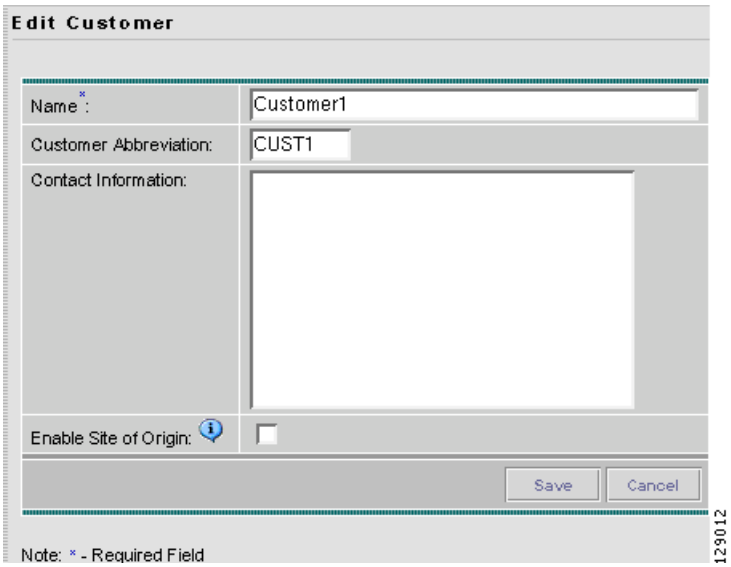
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Customers**.

Step 2 Select a single customer to modify by selecting the check box to the left of the Customer Name.

Step 3 Click the **Edit** button. This button is only enabled if a customer is selected.

The Edit Customer window appears, as shown in Figure 3-68.

Figure 3-68 Edit Customer Window



Step 4 Enter the changes you want to make to the selected customer.

Step 5 Click **Save**.

The changes are saved and the Customers window reappears.

Deleting Customers

From the Delete window, you can remove selected customers from the database.

To access the Delete window, do the following:

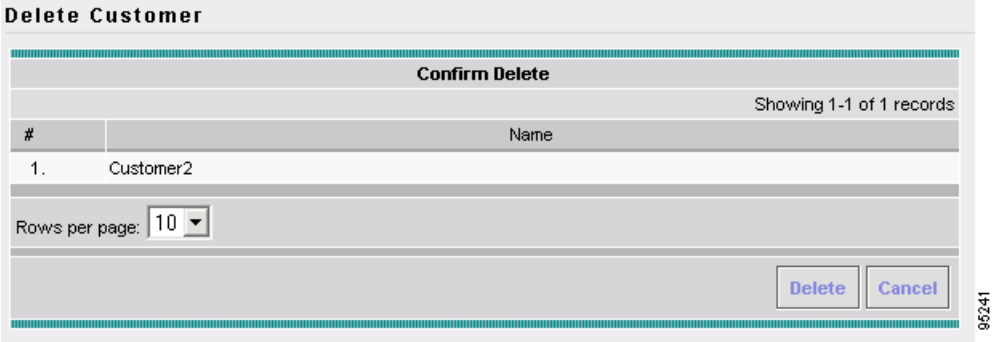
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Customers.**

Step 2 Select one or more customers to delete by selecting the check box to the left of the Customer Name.

Step 3 Click the **Delete** button. This button is only enabled if one or more customers are selected.

The Confirm Delete window appears, as shown in Figure 3-69.

Figure 3-69 Confirm Delete Window



Step 4 Click the **Delete** button to confirm that you want to delete the customer(s) listed.

The Customers window reappears with the specified customer(s) deleted.

Creating Customer Sites

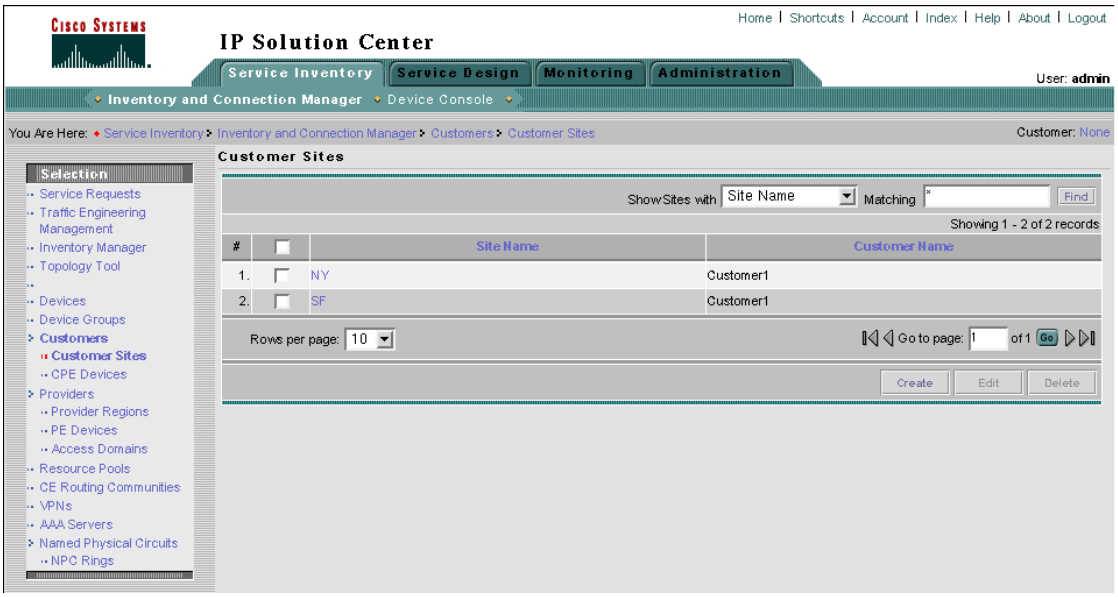
To access the Customer Sites window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager.**

Step 2 Click on **Customer Sites** listed in the Inventory and Connection Manager tree in the left column as shown in Figure 3-70.

The Customer Sites window appears.

Figure 3-70 Customer Sites Window



The Customer Sites window contains the following:

- **Site Name** Lists the names of sites. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by site name.
- **Customer Name** Lists the names of customer. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by customer name.

From the Customer Sites window, you can create, edit, or delete customer sites using the following buttons:

- **Create** Click to create new customer sites. Enabled only if no customer site is selected.
- **Edit** Click to edit selected customer sites (select by clicking the corresponding box). Enabled only if a single customer site is selected.
- **Delete** Click to delete selected customer site(s) (select by clicking the corresponding box). Enabled only if one or more customer sites are selected.

CPE Devices

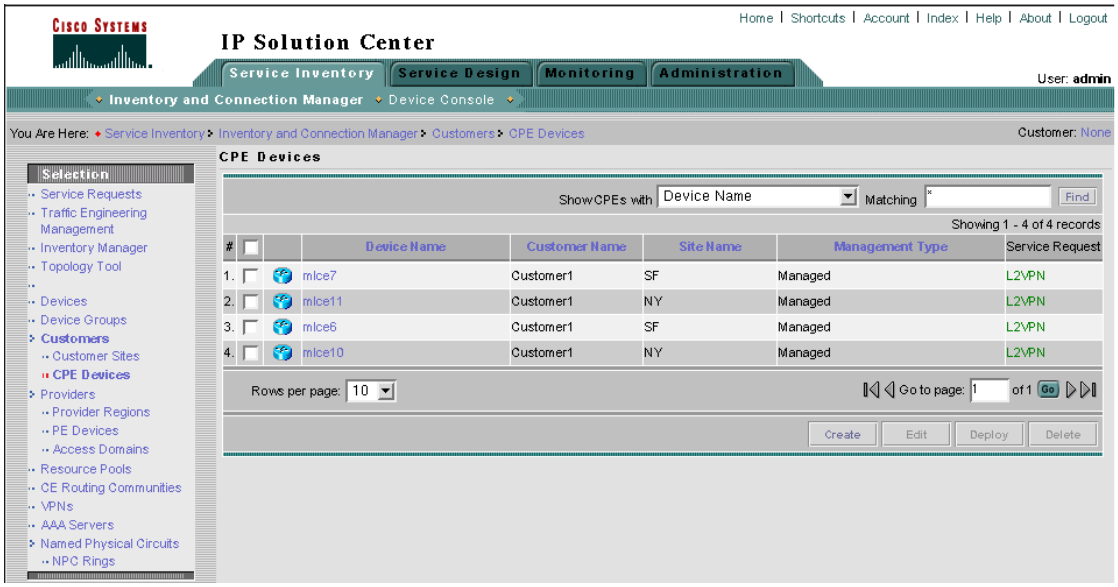
The CPE feature provides a list of CPEs that have been associated with a site through the CPE editor or Inventory Manager. To access the CPE Devices window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager**.

Step 2 Click on **CPE Devices** listed in the Inventory and Connection Manager tree in the left column, as shown in Figure 3-71.

The CPE Devices window appears.

Figure 3-71 CPE Devices Window



The CPE Devices window contains the following:

- **Device Name** Lists the names of devices. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by device name.
- **Customer Name** Lists the names of customer. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by customer name.
- **Site Name** Lists the names of sites. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by site name.
- **Management Type** When associating a CE with a customer site, you can select Managed or Unmanaged. Other choices are available (see below), but they should not be confused with this primary choice.
  - Managed—A managed CE can be provisioned directly by the provider using ISC. The CE must be reachable from an ISC server.
  - Unmanaged —An unmanaged CE cannot be provisioned directly by the provider. If Unmanaged is selected, the provider can use ISC to generate a configuration, and then send the configuration to the customer for placement on the CE.
  - Managed - Management LAN —A managed Management LAN or Management CE (MCE) is configured like a managed CE router, but it resides in the provider space. Normally, an MCE acts as the network operations center (NOC) gateway router.
  - Unmanaged - Management LAN —An unmanaged Management LAN or MCE is configured like an unmanaged CE router, but it resides in the provider space. Normally, an MCE acts as the network operations center (NOC) gateway router.
  - Directly Connected —In most cases, the CE is connected to a PE router. In this case, the CE is connected to a workstation or other device.
  - Directly Connected Management Host —In most cases, the CE is connected to a PE router. In this case, the CE is connected to a workstation or other device, on which ISC resides.
  - Multi-VRF —A multi-VRF CE (MVRFCE) is owned by the customer, but resides in the provider space. It is used to off load traffic from the PE.
  - Unmanaged Multi-VRF—An unmanaged multi-VRF CE is provisioned like an unmanaged CE (configurations are not uploaded or downloaded to the device by the provider). It is owned by the customer and resides in the provider space.

Create CPE Device

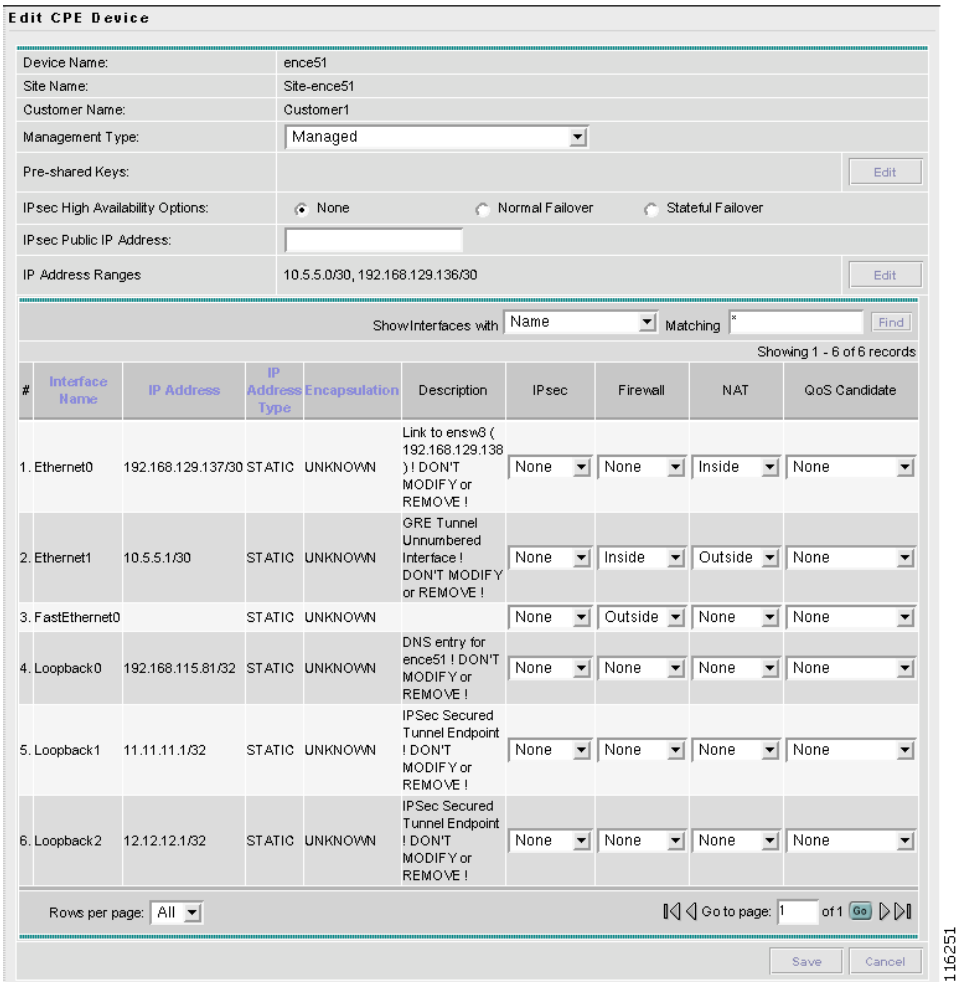
Click **Create** to create new CPE devices. Enabled only if no customer site is selected. The resulting window is shown in Figure 3-72, "Create CPE Device."

Figure 3-72 Create CPE Device

Edit CPE Device

Click **Edit** to edit a single CPE device selected in Figure 3-71. The result is a window as shown in the example in Figure 3-73, "Edit CPE Device."

Figure 3-73 Edit CPE Device



Deploy CPE Device

- NOT SUPPORTED in this release. -

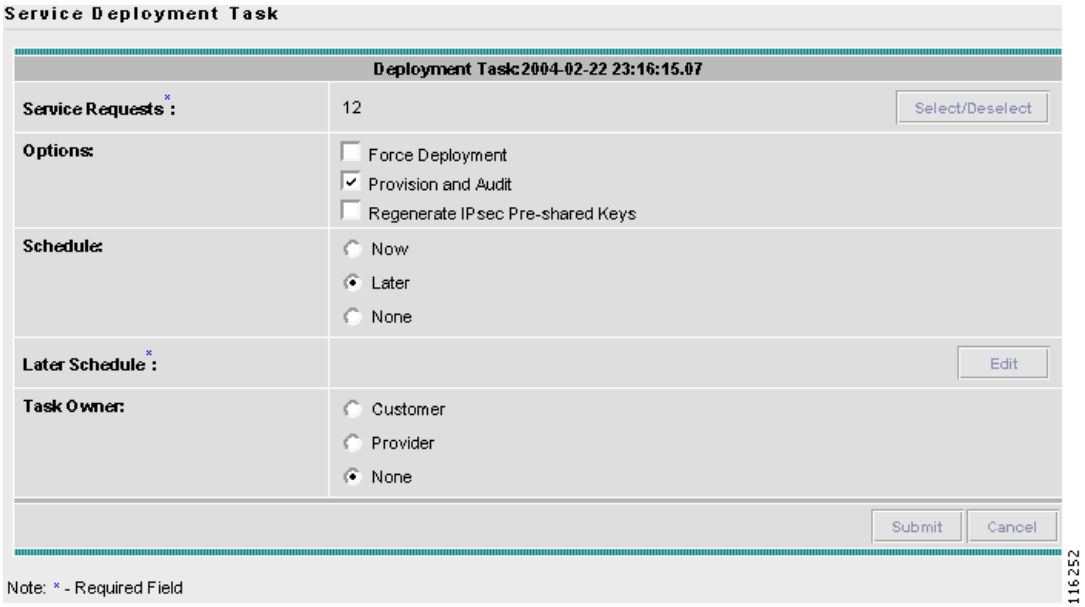
To deploy CPE Device(s), follow these steps:

Note This **Deploy** button is supported for Site-to-Site VPN, Remote Access VPN, NAT, and Firewall services *only*. The only way to use this **Deploy** button with other services is to find the available Service Requests for the CPE, as explained in Step 3.

Step 1 In Figure 3-71, select one or more check boxes for the CPE(s) you want to Deploy.

Step 2 Click the **Deploy** button and you receive a window, as shown in Figure 3-74, "Service Deployment Task."

Figure 3-74 Service Deployment Task



Step 3 In **Service Requests** in Figure 3-74, click the **Select/Deselect** button and you will receive a window from which you can select and deselect Service Requests you want to deploy.

Caution *Be sure* to only select IPsec, IPsec Remote Access, NAT, or Firewall Service Requests. If you are using a service other than these, go no further.

Step 4 Click **Select**.

Step 5 In **Options**, choose: **Force Deployment**; **Provision and Audit**; or **Regenerate IPsec Pre-shared Keys**

Step 6 In **Schedule**, choose **Now**; **Later**; or **None**. If you choose **Later**, a **Later Schedule** category appears. Click that **Edit** button and you will receive a Task Schedule window from which you can choose how often to deploy the chosen Service Requests and when to start and stop this process. Make your choices and click **OK**.

Step 7 For Task Owner, choose **Customer**; **Provider**; or **None**.

Step 8 Click **Submit**.

Delete CPE Device

Click to delete selected CPE device(s) (select by clicking the corresponding box). Enabled only if one or more CPE devices are selected.

Providers

This section describes how to create and manage providers. This section includes the following:

- Accessing the Providers Window, page 3-96

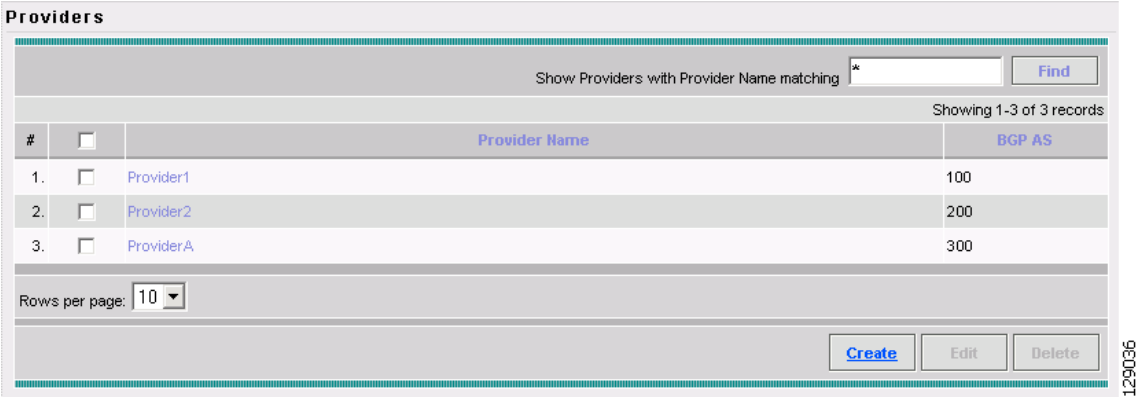
Accessing the Providers Window

The Providers feature is used to create and manage providers.

To access the Providers window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Providers** to access the Providers window shown in Figure 3-75.

Figure 3-75 Providers Window



The Providers window contains the following:

- **Provider Name** Lists the names of providers. You can sort the list by provider name.
- **BGP AS** The Unique number assigned to each BGP autonomous system.

From the Providers window, you can create, edit, or delete providers using the following buttons:

- **Create** Click to create new providers. Enabled only if no customer is selected.
- **Edit** Click to edit selected provider (select the corresponding box). Enabled only if a single provider is selected.
- **Delete** Click to delete a selected provider (select the corresponding box). Enabled only if one or more providers are selected.

Creating a Provider

From the Create Provider window, you can create different providers.

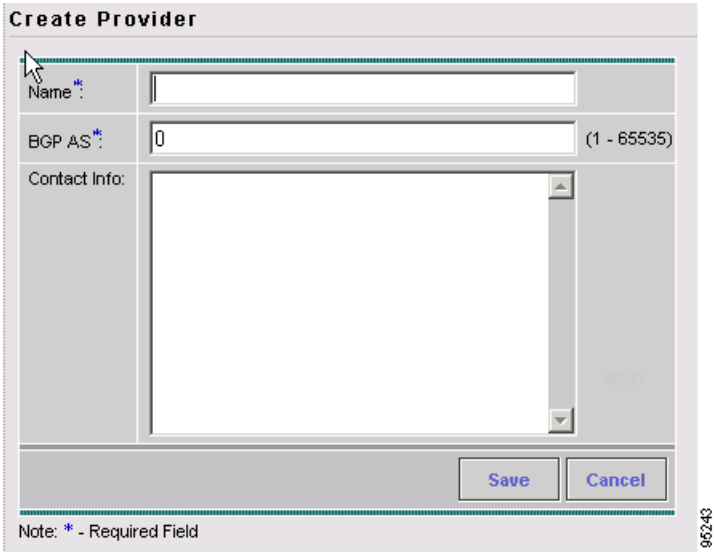
To create a provider, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Providers**.

Step 2 Click the **Create** button.

The Create Provider window appears, as shown in Figure 3-76.

Figure 3-76 Create Provider Window



The Create Provider window contains the following fields:

- **Name** (required) Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters.
- **BGP AS** (required) Each BGP autonomous system is assigned a unique 16-bit number by the same central authority that assigns IP network numbers. Range: 1 to 65535.
- **Contact Information** (optional) Any pertinent information about the provider that could be helpful to service provider operators. Limited to 256 characters.

Step 3 Enter the name, BGP AS, and any contact information for the Provider that you are creating.

Step 4 Click **Save**.

The Providers window reappears with the new provider listed.

Editing a Provider

From the Edit Provider window, you can modify the fields that have been specified for a particular provider.

To access the Edit Provider window, do the following:

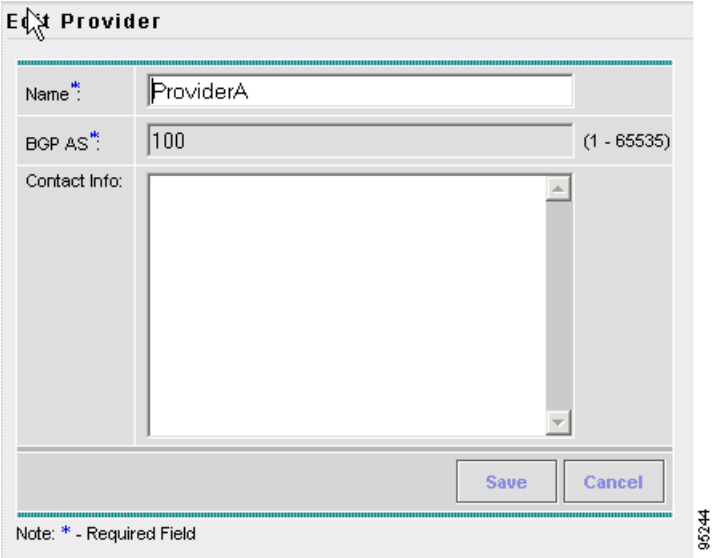
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Providers**.

Step 2 Select a single provider to modify by selecting the check box to the left of the Provider Name.

Step 3 Click the **Edit** button. This button is only enabled if a customer is selected.

The Edit Provider window appears, as shown in Figure 3-77.

Figure 3-77 Edit Provider Window



Step 4 Enter the changes you want to make to the selected provider.

Step 5 Click **Save**.

The changes are saved and the Providers window reappears.

Deleting Providers

From the Delete window, you can remove selected providers from the database.

To access the Delete window, do the following:

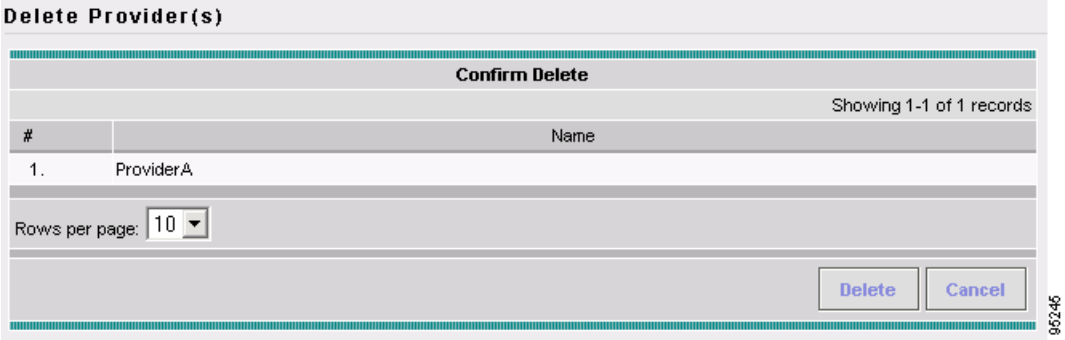
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Providers.**

Step 2 Select provider(s) to delete by selecting the check box to the left of the Provider Name.

Step 3 Click the **Delete** button. This button is only enabled if one or more Providers are selected.

The Confirm Delete window appears, as shown in Figure 3-78.

Figure 3-78 Confirm Delete Window



Step 4 Click the **Delete** button to confirm that you want to delete the provider(s) listed.

The Providers window reappears with the specified provider(s) deleted.

Creating Provider Regions

A Provider Region is considered to be a group of provider edge routers (PEs) within a single BGP autonomous system. The primary objective for defining Provider Regions is to allow a provider to employ unique IP address pools in large Regions, such as Europe, Asia Pacific, and so forth.

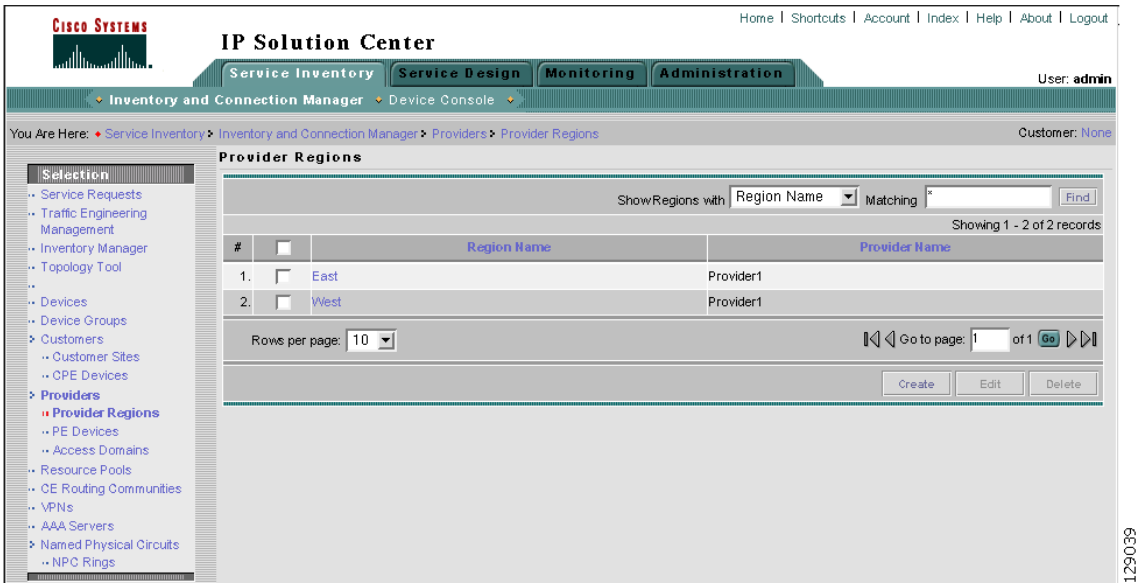
To access the Provider Regions window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager.**

Step 2 Click on **Provider Regions** listed in the Inventory and Connection Manager tree in the left column, as shown in Figure 3-79.

The Provider Regions window appears.

Figure 3-79 Provider Regions Window



The Provider Regions window contains the following:

- **Region Name** Lists the names of regions. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by region name.
- **Provider Name** Lists the names of providers. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by provider name.

From the Provider Regions window, you can create, edit, or delete provider regions using the following buttons:

- **Create** Click to create new provider regions. Enabled only if no customer is selected.
- **Edit** Click to edit selected provider regions (select the corresponding box). Enabled only if a single provider region is selected.
- **Delete** Click to delete selected provider regions (select the corresponding box). Enabled only if one or more provider regions are selected.

Creating PE Devices

The PE Devices feature provides a list of provider edge routers (PEs) that have been associated with the region, either through the PE editor or Inventory Manager.

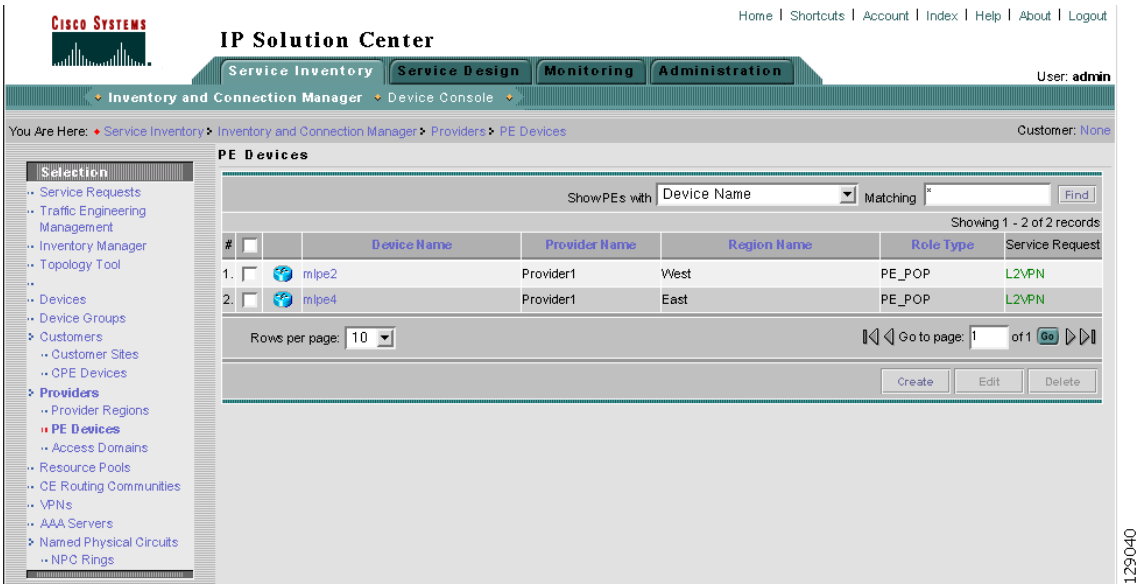
To access the PE Devices window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager.**

Step 2 Click on **PE Devices** listed in the Inventory and Connection Manager tree in the left column, as shown in Figure 3-80.

The PE Devices window appears.

Figure 3-80 PE Devices Window



The PE Devices window contains the following:

- **Device Name** Lists the names of devices. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by device name.
- **Provider Name** Lists the names of providers. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by provider name.
- **Region Name** Lists the names of regions. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by region name.
- **Role Type** Choices include: PE_POP, PE_CLE, PE_CORE, PE_MVRF.

From the PE Devices window, you can create, edit, or delete providers using the following buttons:

- **Create** Click to create new PE device. Enabled only if no PE device is selected.
- **Edit** Click to edit selected PE device (select the corresponding box). Enabled only if a single PE device is selected.
- **Delete** Click to delete selected PE device(s) (select the corresponding box). Enabled only if one or more PE devices are selected.

Creating Access Domains

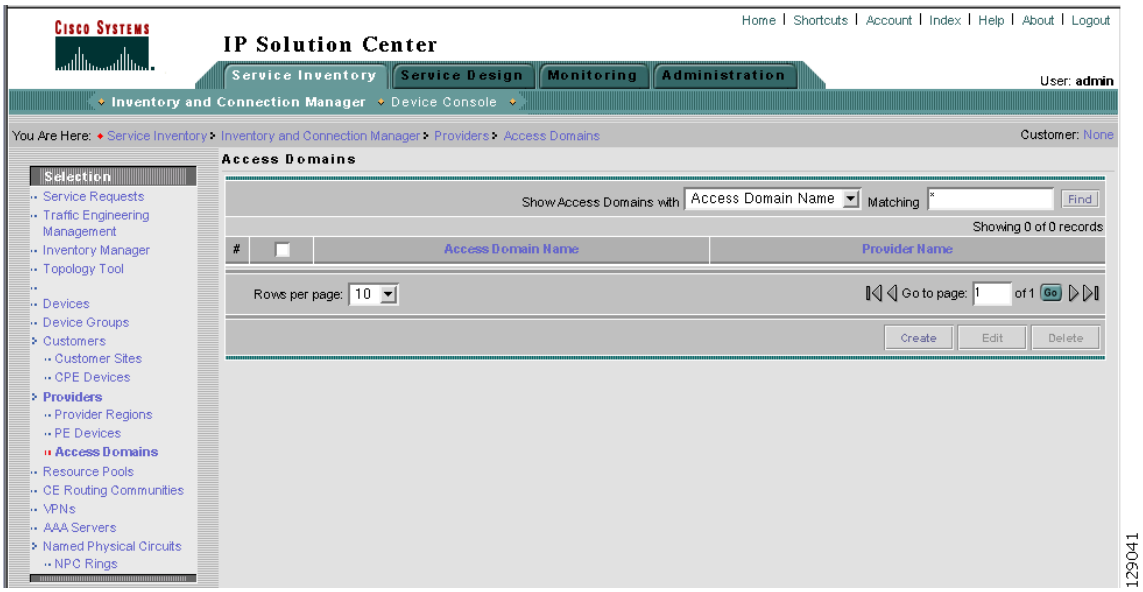
To access the Access Domains window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager**.

Step 2 Click on **Access Domains** listed in the Inventory and Connection Manager tree in the left column, as shown in Figure 3-81.

The Access Domains window appears.

Figure 3-81 Access Domains Window



The Access Domains window contains the following:

- **Access Domain Name** Lists the names of access domain. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by access domain name.
- **Provider Name** Lists the names of providers. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by provider name.

From the Access Domains window, you can create, edit, or delete access domains using the following buttons:

- **Create** Click to create new access domain. Enabled only if no access domain is selected.
- **Edit** Click to edit selected access domain (select the corresponding box). Enabled only if a single access domain is selected.
- **Delete** Click to delete selected access domain(s) (select the corresponding box). Enabled only if one or more access domains are selected.

Resource Pools

Cisco IP Solution Center enables multiple pools to be defined and used during operations. The following resource pools are available:

- *IP address pool*: The IP address pool can be defined and assigned to regions or VPNs. This feature gives the service operator the flexibility to manage the allocation of all IP addresses in the network.
- *Multicast pool*: The Multicast pool is used for Multicast MPLS VPNs.

- *Route Target (RT) pool*: A route target is the MPLS mechanism that informs PEs as to which routes should be inserted into the appropriate VRFs. Every VPN route is tagged with one or more route targets when it is exported from a VRF and offered to other VRFs. The route target can be considered a VPN identifier in MPLS VPN architecture. RTs are a 64-bit number.
- *Route Distinguisher (RD) pool*: The IP subnets advertised by the CE routers to the PE routers are augmented with a 64-bit prefix called a route distinguisher (RD) to make them unique. The resulting 96-bit addresses are then exchanged between the PEs, using a special address family of Multiprotocol BGP (referred to as MP-BGP). The RD pool is a pool of 64-bit RD values that Cisco IP Solution Center uses to make sure the IP addresses in the network are unique.
- *Site of origin pool*: The pool of values for the site-of-origin (SOO) attribute. The site-of-origin attribute prevents routing loops when a site is multihomed to the MPLS VPN backbone. This is achieved by identifying the site from which the route was learned, based on its SOO value, so that it is not readvertised back to that site from a PE in the MPLS VPN network.
- *VC ID poo*l: VC ID pools are defined with a starting value and a size of the VC ID pool. (VC ID is a 32-bit unique identifier that identifies a circuit/port.) A given VC ID pool is not attached to any Inventory object. During the deployment of an Ethernet Service (EWS, ERS for example), VC ID is auto-allocated from the VC ID pool.
- *VLAN ID pool*: VLAN ID pools are defined with a starting value and a size of the VLAN pool. A given VLAN ID pool can be attached to an Access Domain. During the deployment an Ethernet Service (EWS, ERS for example), VLAN ID can be auto-allocated from the Access Domain's VLAN pools. This gives the Service Provider a tighter control of VLAN ID allocation.

All these resources, that are made available to the service provider, enable the automation of service deployment.

This section describes how you can create and manage pools for various types of resources. This section includes the following:

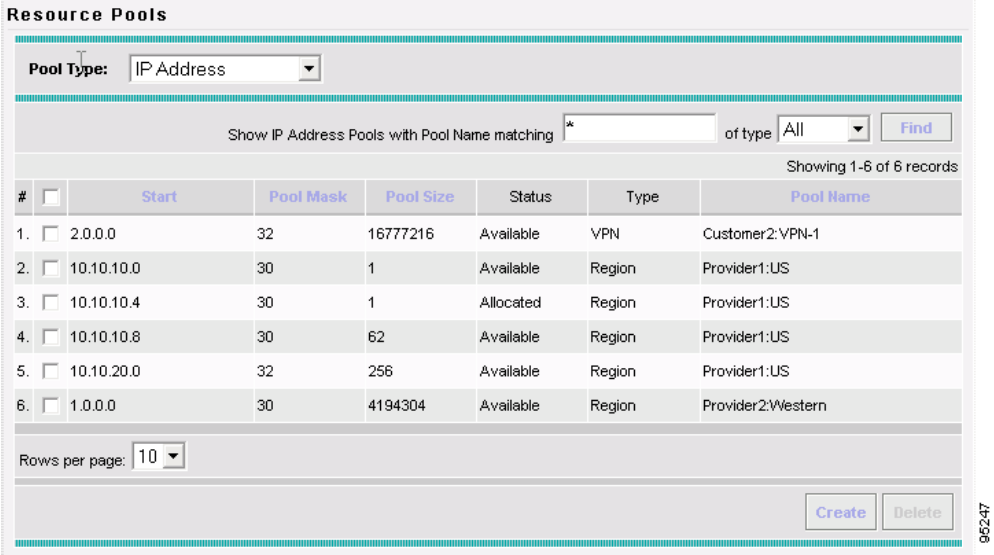
Accessing the Resource Pools Window

The Resource Pools feature is used to create and manage various types of resource pools.

To access the Resource Pools window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource Pools** to access the Resource Pools window shown in Figure 3-82.

Figure 3-82 Resource Pools Window



From the Resource Pools window, you have access to the following buttons:

- **Pool Type** Choices include: IP Address, Multicast Address, Route Distinguisher, Route Target, Site of Origin, VC ID, and VLAN. The fields displayed in the Resource Pools window vary depending on the pool type selected.
- **Create** Click to create new resource pools. Enabled only if no resource pool is selected.
- **Delete** Click to delete selected resource pools (select by clicking the corresponding box). Enabled only if one or more resource pools are selected.

Creating an IP Address Pool

ISC uses IP address pools to automatically assign IP addresses to PEs and CEs. Each Region has an IP address pool to use for IP numbered addresses (/30 pools) and a separate IP address pool for IP unnumbered addresses (/32 loopback address pools).

Within a VPN or extranet, all IP addresses must be unique. Customer IP addresses must not overlap with the provider's IP addresses. Overlapping IP addresses are only possible when two devices cannot see each other—that is, when they are in isolated VPNs.

From the Create IP Address Pool window, you can create IP address pools.

To create an IP address pool, do the following:

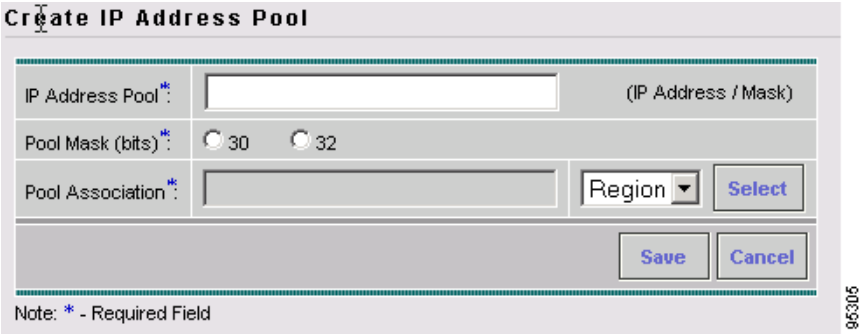
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource Pools**.

Step 2 Select **IP address** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create IP Address Pool window appears, as shown in Figure 3-83.

Figure 3-83 Create IP Address Pool Window



The Create IP Address Pool window contains the following fields:

- **IP Address Pool** (required) Text field in the format a.b.c.d/mask, for example 172.0.0.0/8.
- **Pool Mask (bits)** (required) Choices include: **30** and **32**

  where:

  30 is used for IP numbered address pools (/30)

  32 is used for IP unnumbered loopback address pools (/32).
- **Pool Association** (required) Choices include: Region and VPN.

Note If you choose **VPN**, an additional optional field appears, **Pool Name Suffix**, when you return to Figure 3-83. This field allows the creation of multiple address pools within the same VPN. If you are creating this address pool for DMVPN usage, the recommendation is to use this field to specify a suffix.

Step 4 Enter the required information for the IP address pool you are creating.

Step 5 Click **Save**.

The Resource Pools window reappears with the new IP address pool listed.

Creating a Multicast Pool

From the Create Multicast Pool window, you can create multicast pools. These pools are global and are not associated with any provider or customer.

To create a multicast pool, do the following:

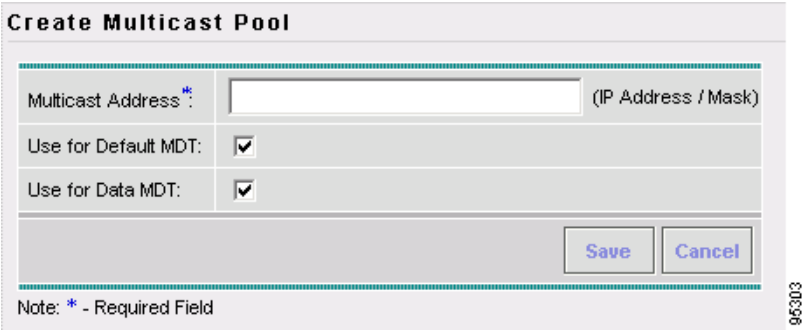
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource Pools**.

Step 2 Select **Multicast** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create Multicast Pool window appears, as shown in Figure 3-84.

Figure 3-84 Create Multicast Pool Window



The Create Multicast Pool window contains the following fields:

- **Multicast Address** (required) Text field in the format a.b.c.d/mask, for example 239.0.0.0/8. Range: 224.0.1.0/8 to 239.255.255.255/32.
- **Use for default MDT** (optional) This is a check box. Default: selected.
- **Use for Data MDT** (optional) This is a check box. The *data MDT* contains a range of multicast group addresses and a bandwidth threshold. Thus, whenever a CE behind a multicast-VRF exceeds that bandwidth threshold while sending multicast traffic, the PE sets up a new data MDT for the multicast traffic from that source. The PE informs the other PEs about this data MDT and, if they have receivers for the corresponding group, the other PEs join this data MDT. Default: selected.

Step 4 Enter the required information for the multicast pool you are creating.

Step 5 Click **Save**.

The Resource Pools window reappears with the new multicast pool listed.

Creating a Route Distinguisher and Route Target Pool

MPLS-based VPNs employ Border Gateway Protocol (BGP) to communicate between PEs to facilitate customer routes. This is made possible through extensions to BGP that carry addresses other than IPv4 addresses. A notable extension is called the route distinguisher (RD).

The purpose of the route distinguisher (RD) is to make the prefix value unique across the network backbone. Prefixes should use the same RD if they are associated with the same set of route targets (RTs) and anything else that is used to select routing policy. The community of interest association is based on the route target (RT) extended community attributes distributed with the Network Layer Reachability Information (NLRI). The RD value must be a globally unique value to avoid conflict with other prefixes.

The MPLS label is part of a BGP routing update. The routing update also carries the addressing and reachability information. When the RD is unique across the MPLS VPN network, proper connectivity is established even if different customers use non-unique IP addresses.

For the RD, every CE that has the same overall role should use a VRF with the same name, same RD, and same RT values. The RDs and RTs are only for route exchange between the PEs running BGP. That is, for the PEs to do MPLS VPN work, they have to exchange routing information with more fields than usual for IPv4 routes; that extra information includes (but is not limited to) the RDs and RTs.

From the Create Route Distinguisher Pool window, you can create route distinguisher pools.

To create a route distinguisher pool, do the following:

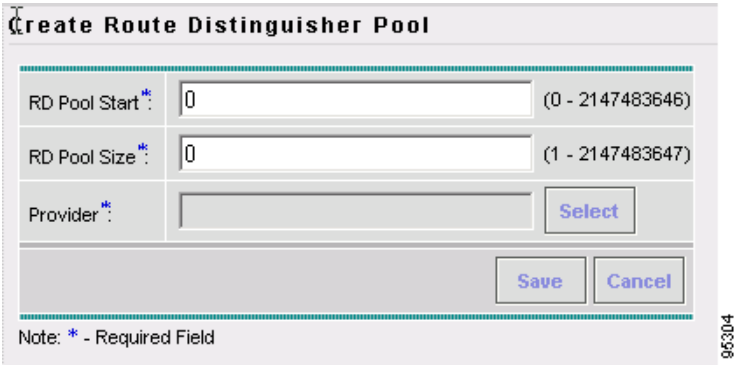
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource pools**.

Step 2 Select **Route Distinguisher** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create Route Distinguisher Pool window appears, as shown in Figure 3-85.

Figure 3-85 Create Route Distinguisher Pool Window



The Create Route Distinguisher Pool window contains the following fields:

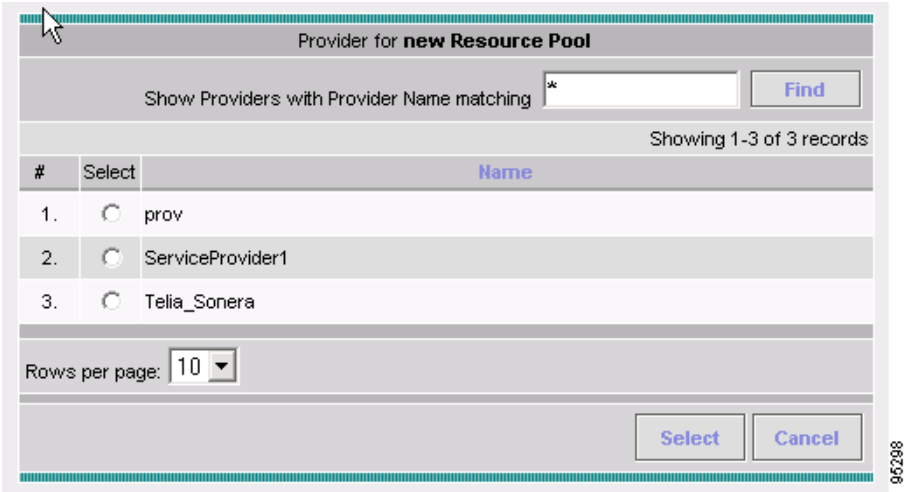
- **RD Pool Start** (required) Range: 0 to 2147483646.
- **RD Pool Size** (required) Range: 1 to 2147483647.
- **Provider** (required)

Step 4 Enter the **RD Pool Start** and **Size** information for the route distinguisher pool you are creating.

Step 5 Click the **Select** button.

The Provider for new Resource Pool window appears, as shown in Figure 3-86.

Figure 3-86 Provider for New Resource Pool Window



Step 6 Select one of the providers listed and click **Select**.

Step 7 Click **Save**.

The Resource Pools window reappears with the new route distinguisher pool listed.

To create a Route Target Pool, do the following:

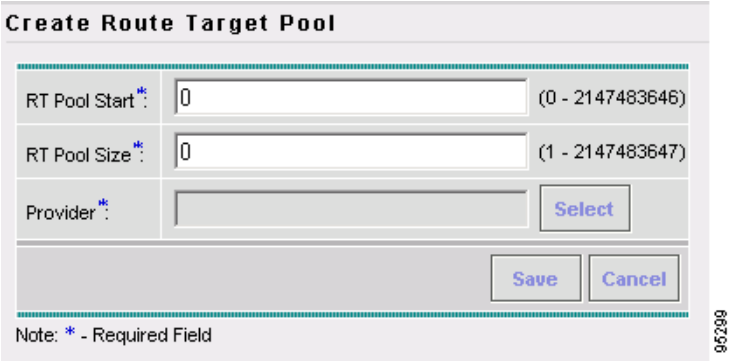
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource pools**.

Step 2 Select **Route Target** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create Route Target Pool window appears, as shown in Figure 3-87.

Figure 3-87 Create Route Target Pool Window



The Create Route Target Pool window contains the following fields:

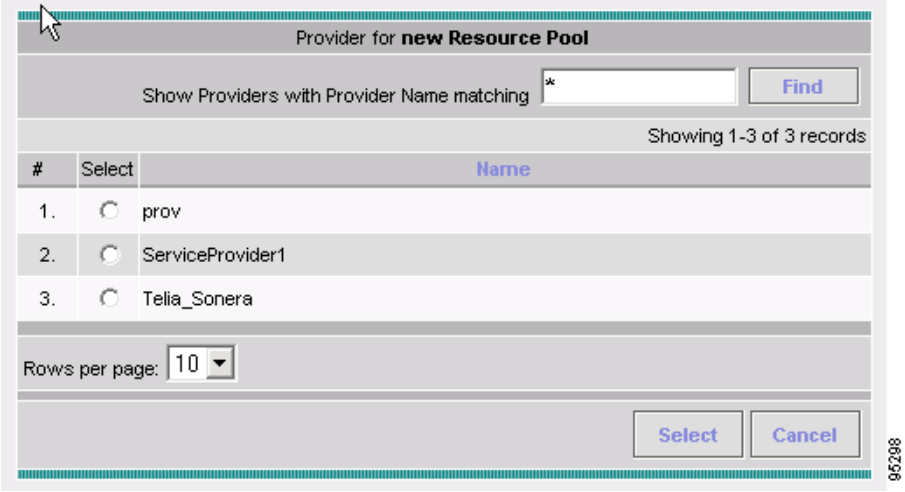
- **RT Pool Start** (required) Range: 0 to 2147483646.
- **RT Pool Size** (required) Range: 1 to 2147483647.
- **Provider** (required)

Step 4 Enter the **RT Pool Start** and **Size** information for the route target pool you are creating.

Step 5 Click the **Select** button.

The Provider for new Resource Pool window appears, as shown in Figure 3-88.

Figure 3-88 Provider for New Resource Pool Window



Step 6 Select one of the providers listed and click **Select**.

Step 7 Click **Save**.

The Resource Pools window reappears with the new route target pool listed.

Creating a Site of Origin Pool

In MPLS VPN, CE sites use private/public AS numbers and when one AS number is used for each VPN, all sites belonging to the same VPN share the same private/public AS number. The default BGP behavior is to drop any prefix if its own AS number is already in the AS path. As a result, a customer site does not learn prefixes of a remote site in this situation. AS-OVERRIDE must be configured (if there are hub sites involved, ALLOWAS-IN must be configured) to allow those prefixes to be sent by PE routers but a routing loop can occur.

For example, CE1 and CE2 belong to the same customer VPN and have the same AS number 65001. The AS path between two customer sites is 65001 - 1234 - 65001 and prefixes cannot be exchanged between customer sites because AS 65001 is already in the path. To solve this problem, AS-OVERRIDE options are configured on PE routers; but it introduces a routing loop into the network without using extended community site of origin attributes.

Site of origin is a concept in MPLS VPN architecture that prevents routing loops in sites that are multi-homed to the MPLS VPN backbone and in sites using AS-OVERRIDE in conjunction. Site of origin is a type of BGP extended community attribute used to identify a prefix that originated from a site so that the re-advertisement of that prefix back to the site can be prevented. This attribute uniquely identifies the site from which the PE router learned the route. Site of origin is tagged at PE in peering with BGP neighbors using an inbound route-map and works in conjunction with BGP CE-PE routing protocol.

Site of origin must be unique per customer site per VPN/customer (when these sites are multi-homed). Therefore, the same value of site of origin must be used on PE routers connected to the same CE router or to the same customer site.

Note Each time a customer site is created, ISC generates a unique site of origin value from the selected site of origin provider pool if Site of Origin is enabled. This site of origin value must be unique per customer site per customer/VPN.

From the Create Site of Origin Pool window, you can create site of origin pools.

To create a site of origin pool, do the following:

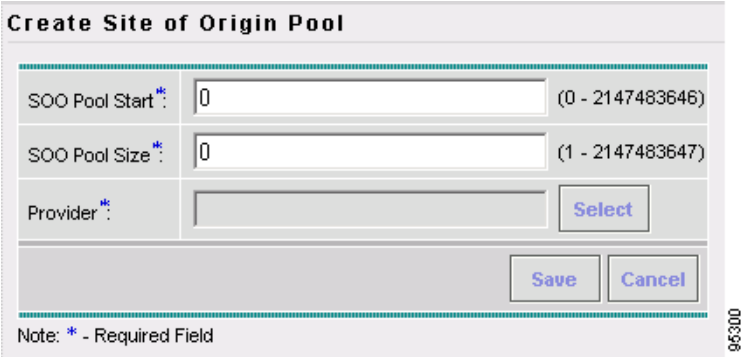
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource pools**.

Step 2 Select **Site of Origin** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create Site of Origin Pool window appears, as shown in Figure 3-89.

Figure 3-89 Create Site of Origin Pool Window



The Create Site of Origin Pool window contains the following fields:

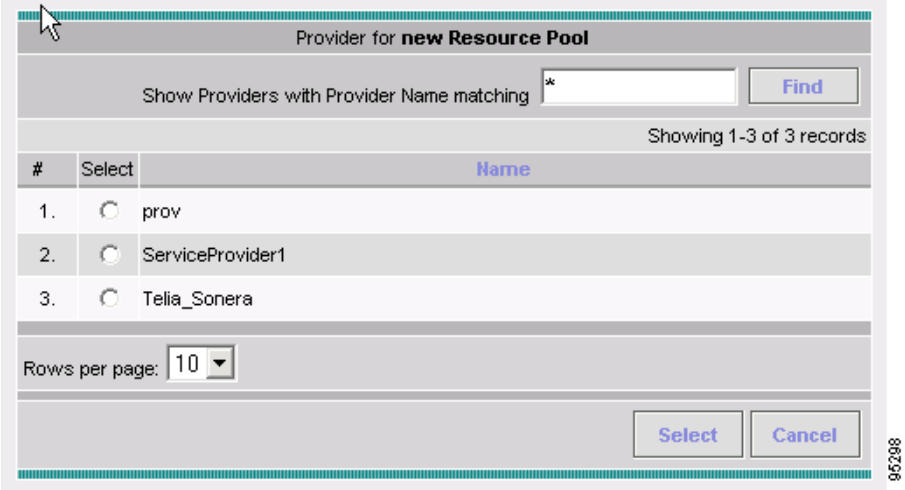
- **SOO Pool Start** (required) Range: 0 to 2147483646.
- **SOO Pool Size** (required) Range: 1 to 2147483647.
- **Provider** (required)

Step 4 Enter the **SOO Pool Start** and **Size** information for the site of origin pool you are creating.

Step 5 Click the **Select** button.

The Provider for new Resource Pool window appears, as shown in Figure 3-90.

Figure 3-90 Provider for New Resource Pool Window



Step 6 Select one of the providers listed and click **Select**.

Step 7 Click **Save**.

The Site of Origin pools window reappears with the new route target pool listed.

Creating a VC ID Pool

From the Create VC ID Pool window, you can create VC ID pools. These pools are global and are not associated with any provider or customer

To create a VC ID pool, do the following:

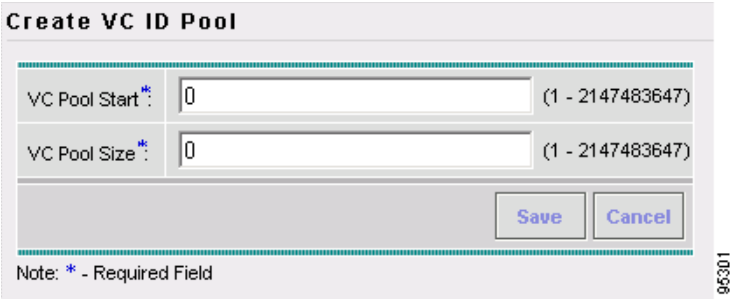
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource pools**.

Step 2 Select **VC ID** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create VC ID Pool window appears, as shown in Figure 3-91.

Figure 3-91 Create VC ID Pool Window



The Create VC ID Pool window contains the following fields:

- **VC Pool Start** (required) Range: 1 to 2147483646.
- **VC Pool Size** (required) Range: 1 to 2147483647.

Step 4 Enter the required information for the site of origin pool you are creating.

Step 5 Click **Save**.

The VC ID Pools window reappears with the new VC ID pool listed.

Creating a VLAN Pool

From the Create VLAN Pool window, you can create VLAN pools.

To create a VLAN pool, do the following:

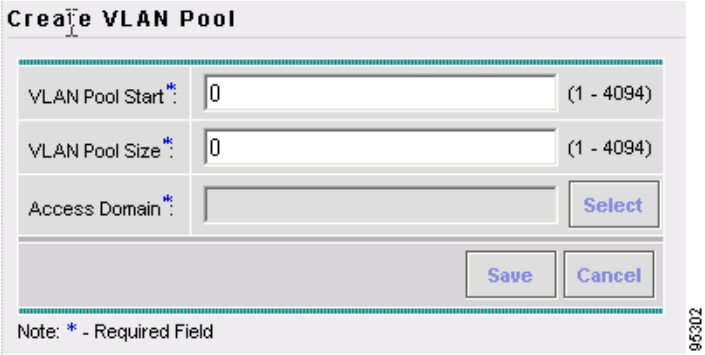
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource pools**.

Step 2 Select **VLAN** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create VLAN Pool window appears, as shown in Figure 3-92.

Figure 3-92 Create VLAN Pool Window



The Create VLAN Pool window contains the following fields:

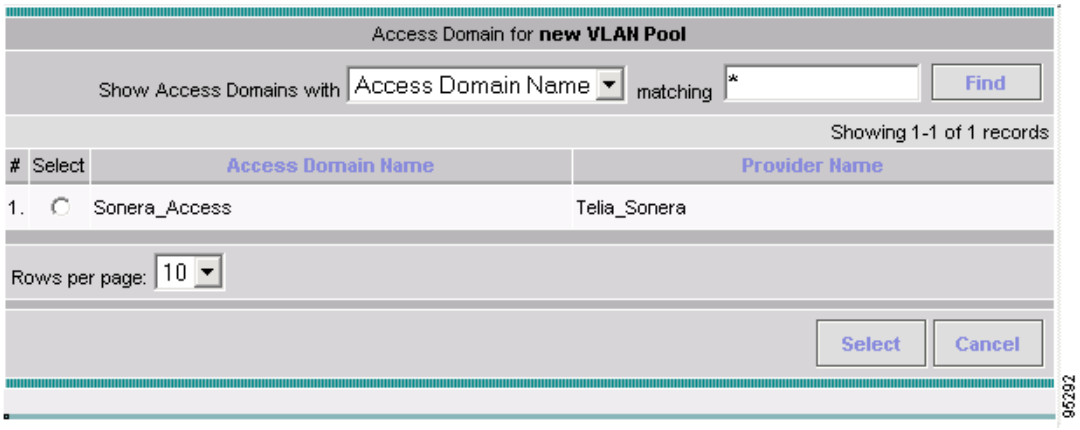
- **VLAN Pool Start** (required) Range: 1 to 4094.
- **VLAN Pool Size** (required) Range: 1 to 4094.
- **Access Domain** (required)

Step 4 Enter the **VLAN Pool Start** and **Size** information for the VLAN pool you are creating.

Step 5 Click the **Select** button.

The Access Domain for new VLAN Pool window appears, as shown in Figure 3-93.

Figure 3-93 Access Domain for new VLAN Pool Window



Step 6 Select one of the access domains listed and click **Select**.

Step 7 Click **Save**.

The VLAN Pools window reappears with the new VLAN pool listed.

Deleting Resource Pools

From the Resource Pool window, you can delete specific resource pools.

To delete resource pools, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource pools**.

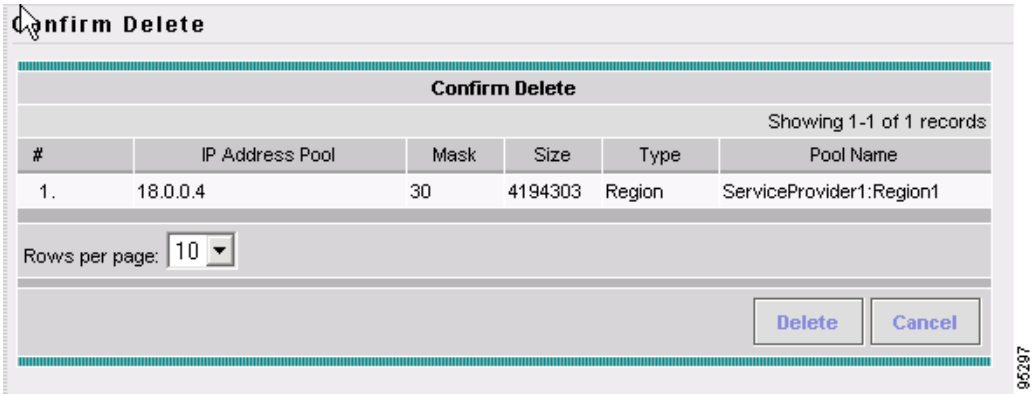
Step 2 Select a pool type from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Select one or more resource pools to delete by selecting the check box to the left of the resource pool(s).

Step 4 Click the **Delete** button.

The Confirm Delete window appears, as shown in Figure 3-94.

Figure 3-94 Confirm Delete Window



Step 5 Click the **Delete** button to confirm that you want to delete the resource pool(s) listed.

The Resource Pools window reappears with the specified pool(s) deleted.

CE Routing Communities

A VPN can be organized into subsets called *CE routing communities*, or CERCs. A CERC describes how the CEs in a VPN communicate with each other. Thus, CERCs describe the logical topology of the VPN. Cisco IP Solution Center can be employed to form a variety of VPN topologies between CEs by building hub and spoke or full mesh CE routing communities. CERCs are building blocks that allow you to form complex VPN topologies and CE connectivity.

The most common types of VPNs are *hub-and-spoke* and *full mesh*.

- A hub-and-spoke CERC is one in which one or a few CEs act as hubs, and all spoke CEs talk only to or through the hubs, never directly to each other.
- A full mesh CERC is one in which every CE connects to every other CE.

These two basic types of VPNs—full mesh and hub and spoke—can be represented with a single CERC. Whenever you create a VPN, the Cisco IP Solution Center software creates one default CERC for you. This means that until you need advanced customer layout methods, you will not need to define new CERCs. Up to that point, you can think of a CERC as standing for the VPN itself—they are one and the same. If, for any reason, you must override the software's choice of route target values, you can do so only at the time you create a CERC in the Cisco IP Solution Center software.

To build very complex topologies, it is necessary to break down the required connectivity between CEs into groups, where each group is either fully meshed, or has a hub and spoke pattern. (Note that a CE can be in more than one group at a time, if each group has one of the two basic patterns.) Each subgroup in the VPN wants its own CERC. Any CE that is only in one group just joins the corresponding CERC (as a spoke if necessary). If a CE is in more than one group, then you can use the Advanced Setup choice during provisioning to add the CE to all the relevant groups in one service request. Given this information, the provisioning software does the rest, assigning route target values and VRF tables to arrange exactly the connectivity the customer requires. You can use the Topology tool to double-check the CERC memberships and resultant VPN connectedness.

Cisco IP Solution Center supports multiple CEs per site and multiple sites connected to the same PE. Each CERC has unique route targets (RT), route distinguisher (RD), and VPN Routing and Forwarding instance (VRF) naming. After provisioning a CERC, it is a good idea to run the audit reports to verify the CERC deployment and view the topologies created by the service requests. The product supports linking two or more CE routing communities in the same VPN.

This section describes how you can create and manage CE routing communities. This section includes the following:

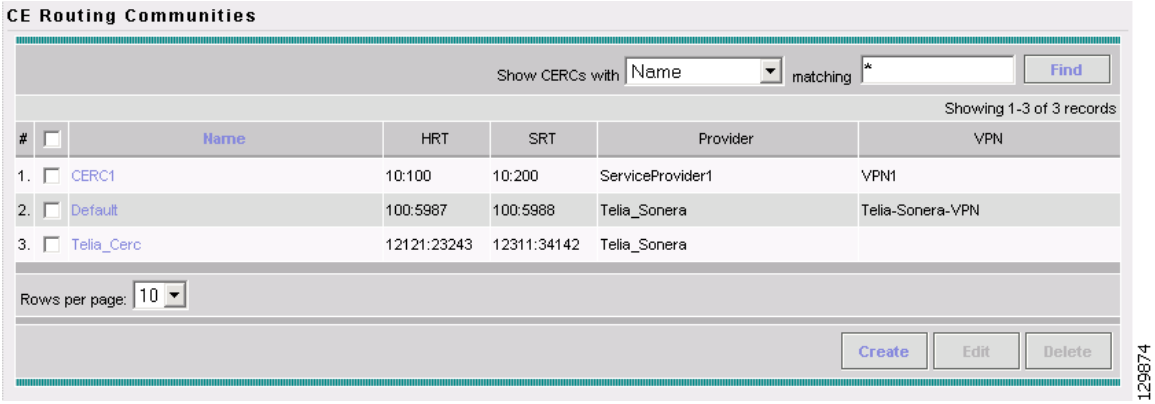
Accessing the CE Routing Communities Window

The CE Routing Communities feature is used to create and manage CERCs.

To access the CE Routing Communities window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > CE Routing Communities** to access the CE Routing Communities window shown in Figure 3-95.

Figure 3-95 CE Routing Communities Window



From the CE Routing Communities window, you can create, edit, or delete CE routing communities using the following buttons:

- **Create** Click to create new CE routing communities. Enabled only if no CE routing community is selected.
- **Edit** Click to edit selected CE routing communities (select by clicking the corresponding box). Enabled only if one CE routing community is selected.
- **Delete** Click to delete selected CE routing communities (select by clicking the corresponding box(es)). Enabled only if one or more CE routing communities are selected.

Creating CE Routing Communities

When you create a VPN, the Cisco IP Solution Center software creates one default CE routing community (CERC) for you. But if your network topology and configuration require customized CERC definitions, you can define CERCs customized for your network.

Tip Customized CERCs should be defined only in consultation with the VPN network administrator. To build complex topologies, it is necessary to break down the required connectivity between CEs into groups, where each group is either fully meshed or has a hub-and-spoke pattern. A CE can be in more than one group at a time, as long as each group has one of the two basic configuration patterns.

Each subgroup in the VPN wants its own CERC. Any CE that is only in one group just joins the corresponding CERC (as a spoke if necessary). If a CE is in more than one group, then you can use the Advanced Setup choice during provisioning to add the CE to all the relevant groups in one service request. Given this information, Cisco IP Solution Center does the rest, assigning route target values and VRF tables to arrange the precise connectivity the customer requires.

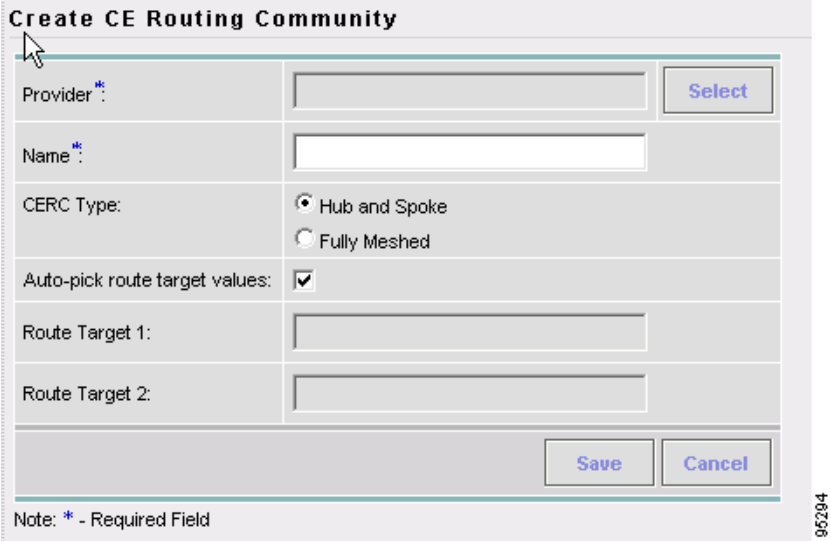
To create a CE routing community, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > CE Routing Communities**.

Step 2 Click **Create**.

The Create CE Routing Community window appears, as shown in Figure 3-96.

Figure 3-96 Create CE Routing Community Window



Step 3 Complete the CERC fields as required for the CE Routing Community:

a. **Provider** (required) To specify the service provider associated with this CERC, click **Select**.

   The Select Provider dialog box is displayed.

b. Choose the name of the service provider, then click **Select**.

c. **Name** (required) Enter the name of the CERC.

d. **CERC Type** Specify the CERC type: Hub and Spoke or Fully Meshed.

e. **Auto-Pick Route Target Values** Choose to either let Cisco IP Solution Center automatically set the route target (RT) values or set the RT values manually.

   By default, the **Auto-pick route target values** check box is selected. If you deselect the check box, you can enter the Route Target values manually.

Caution If you choose to bypass the **Auto-pick route target values** option and set the route target (RT) values manually, note that the RT values cannot be edited after they have been defined in the ISC software.

Step 4 When you have finished entering the information in the Create CE Routing Community dialog box, click **Save**.

After creating the CERC, you can add it to the VPN.

Deleting CE Routing Communities

From the CE Routing Community window, you can delete specific CERCs.

To delete CERC(s), do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > CE Routing Communities**

Step 2 Select CERC(s) to delete by selecting the check box(es) to the left of the CERC name.

Step 3 Click the **Delete** button.

The Confirm Delete window appears.

Step 4 Click **OK** to confirm that you want to delete the CERC(s) listed.

The CE Routing Communities window reappears with the specified CERC(s) deleted.

VPNs

At its simplest, a virtual private network (VPN) is a collection of sites that share the same routing table. A VPN is also a framework that provides private IP networking over a public infrastructure such as the Internet. In Cisco IP Solution Center: MPLS VPN Management, a VPN is a set of customer sites that are configured to communicate through a VPN service. A VPN is defined by a set of administrative policies.

A VPN is a network in which two sites can communicate over the provider's network in a private manner; that is, no site outside the VPN can intercept their packets or inject new packets. The provider network is configured such that only one VPN's packets can be transmitted through that VPN—that is, no data can come in or out of the VPN unless it is specifically configured to allow it. There is a physical connection from the provider edge network to the customer edge network, so authentication in the conventional sense is not required.

This section describes how you can create and manage pools for various types of resources. This section includes the following:

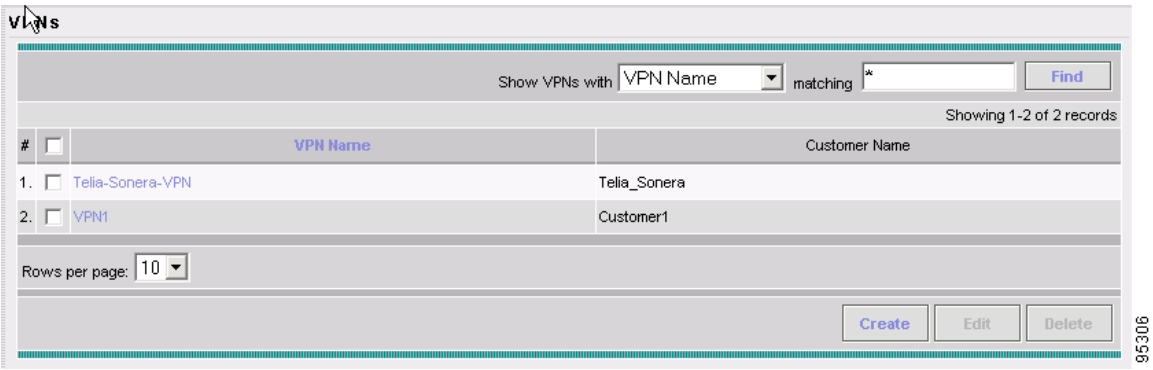
Accessing the VPNs Window

The VPN feature is used to create and manage various types of VPNs.

To access the VPN window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > VPN** to access the VPN window shown in Figure 3-97.

Figure 3-97 VPNs Window



From the VPNs window, you can create, edit, or delete VPNs using the following buttons:

- **Create** Click to create new VPNs. Enabled only if no VPN is selected.
- **Edit** Click to edit selected VPNs (select the corresponding box). Enabled only if one VPN is selected.
- **Delete** Click to delete selected VPNs (select the corresponding box). Enabled only if one or more VPNs is selected.

Creating a VPN

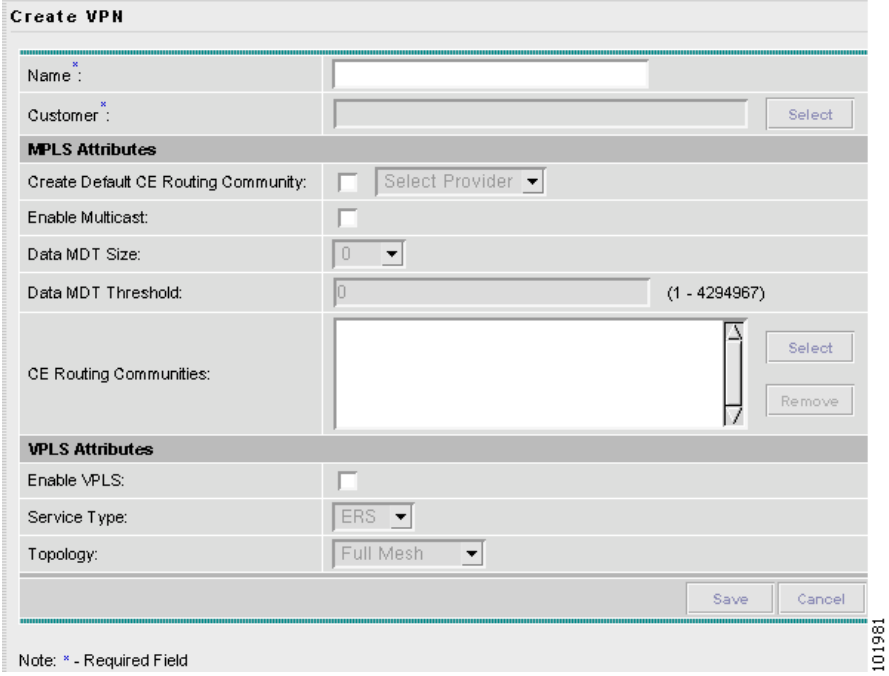
To create a VPN, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > VPN**.

Step 2 Click **Create**.

The Create VPN window appears, as shown in Figure 3-98.

Figure 3-98 Create VPN Window



Step 3 Complete the fields as required for the VPN:

a. **Name** (required) Enter the name of the VPN.

b. **Customer** (required) To select the customer associated with this VPN, choose **Select**.

c. From the list of customers, select the appropriate customer, then click **Select**.

d. If you want MPLS attributes, the optional fields for that are in e. to j.

e. **Create Default CE Routing Community** (optional) To create a default CE routing community, select the **Create Default CE Routing Community** check box and select a provider.

f. **Enable Multicast** To enable multicast VPN routing, select the **Enable Multicast** check box.

An IP address that starts with the binary prefix *1110* is identified as a *multicast group address*. There can be more than one sender and receiver at any time for a given multicast group address. The senders send their data by setting the group address as the destination IP address. It is the responsibility of the network to deliver this data to all the receivers in the network who are listening to that group address.

Note Before you can create a VPN with multicast enabled, you must define one or more multicast resource pools.

g. **Data MDT Size** (optional) If **Enable Multicast** is set on, **Data MDT Size** is required. From the drop-down list, select the data MDT size.

MDT refers to a *multicast distribution tree* (MDT). The MDT defined here carries multicast traffic from customer sites associated with the multicast domain.

h. **Data MDT Threshold** (optional) If **Enable Multicast** is set on, **Data MDT Threshold** is required. Enter the bandwidth threshold for the data multicast distribution tree.

   The *data MDT* contains a range of multicast group addresses and a bandwidth threshold. Thus, whenever a CE behind a multicast-VRF exceeds that bandwidth threshold while sending multicast traffic, the PE sets up a new data MDT for the multicast traffic from that source. The PE informs the other PEs about this data MDT and, if they have receivers for the corresponding group, the other PEs join this data MDT.

i. **CE Routing Communities** (optional) If **Enable Multicast** is set on, **CE Routing Communities** is required. If you do not choose to enable the default CERC, you can select a customized CERC that you have already created in ISC. From the CE Routing Communities pane, click **Select**.

   The Select CE Routing Communities dialog box is displayed.

j. Select the check box for the CERC you want used for this service policy, then click **Select**.

   You return to the Create VPN dialog box, where the new CERC selection is displayed, along with its *hub route target* (*HRT*) and *spoke route target* (SRT) values.

k. If you want VPLS attributes, the optional fields for that are in l. to m.

l. **Enable VPLS** (optional) Select this check box to enable VPLS.

m. **Service Type** (optional) Click the drop-down menu and choose from ERS (Ethernet Relay Service) or EWS (Ethernet Wire Service).

n. **Topology** (optional) Select the VPLS topology from the drop-down menu: Full Mesh (each CE will have direct connections to every other CE) or Hub and Spoke (only the Hub CE has connection to each Spoke CE and the Spoke CEs do not have direct connection to each other).

Step 4 When satisfied with the settings for this VPN, click **Save**.

You have successfully created a VPN, as shown in the **Status** display in the lower left corner of the VPNs dialog box.

Deleting VPNs

From the VPNs window, you can delete specific VPNs.

To delete VPN(s), do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > VPN**.

Step 2 Select VPN(s) to delete by selecting the check box to the left of the VPN name.

Step 3 Click the **Delete** button.

The Confirm Delete window appears.

Step 4 Click **OK** to confirm that you want to delete the VPN(s) listed.

The VPNs window reappears with the specified VPN(s) deleted.

AAA Servers

This section describes how you can create and manage AAA servers. An AAA server is only required when you want remote access VPN service and Easy VPN service and the user authentication or authorization is not done internally but by an external AAA server, such as RADIUS, TACACS+, NT Domain, or SDI. In this case, ISC sets up aspects of AAA on CPE devices for the remote access services, based on the external AAA server information in the repository. When the Service Request is scheduled to be deployed, the configlet of AAA is generated and downloaded to the CPE devices.

This section includes the following:

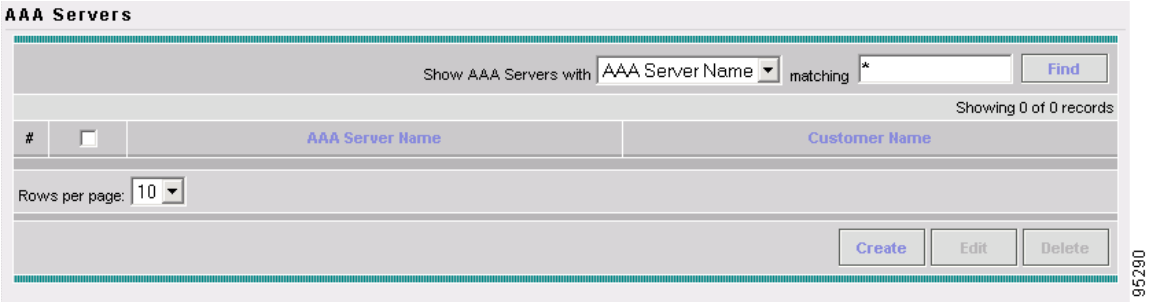
Accessing the AAA Servers Window

The AAA Servers feature is used to create or delete AAA servers that communicate with CPE devices and edit their parameters.

To access the AAA Servers window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > AAA Servers** to access the AAA Servers window shown in Figure 3-99.

Figure 3-99 AAA Servers Window



From the AAA Servers window, you can create, edit, or delete AAA servers using the following buttons:

- **Create** Click to define new AAA servers. Enabled only if no AAA server is selected.
- **Edit** Click to edit selected AAA servers (select by clicking the corresponding box). Enabled only if one AAA server is selected.
- **Delete** Click to delete selected AAA servers (select by clicking the corresponding box). Enabled only if one or more AAA servers are selected.

Defining an AAA Server

From the Create AAA Server window, you can define AAA servers.

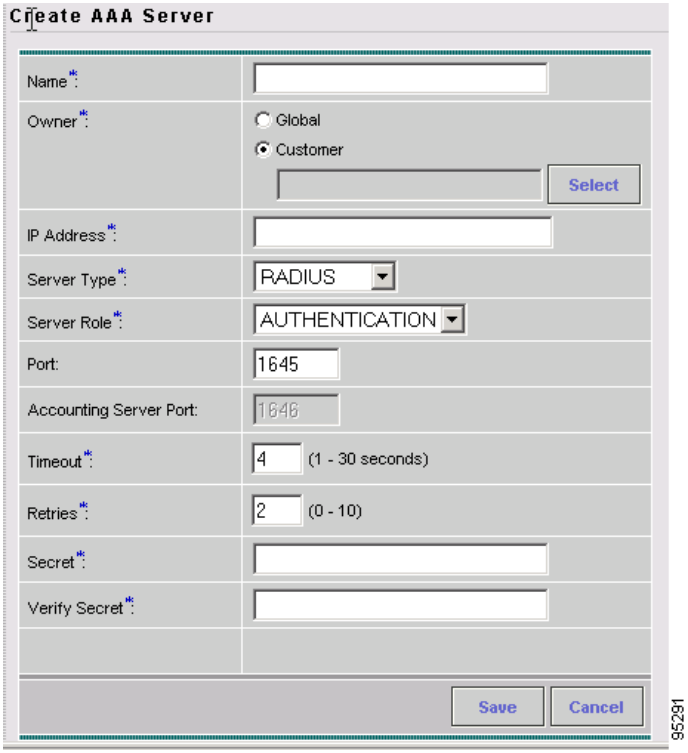
To define such a device, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > AAA Servers**.

Step 2 Click the **Create** button.

The Create AAA Servers window appears, as shown in Figure 3-100.

Figure 3-100 Create AAA Servers Window



The Create AAA Servers window contains the following fields:

- **Name** (required) Name given to the AAA Server that this record represents.
- **Owner** (required) This record can belong to a customer or it can be global to the system.
- **IP Address** (required) IP address of the AAA Server.
- **Server Type** (required) Choices: **RADIUS**, **NT DOMAIN**, **SDI,** or **TACACS+**. Default: RADIUS.
- **Server Role** (required) Specifies the role of the server, that is what it does. Choices: Authentication, Accounting, or Both. Default: Authentication.
- **Port** (optional) The Authentication Server port.
- **Accounting Server Port** (optional) Enabled when **Accounting** or **Both** is selected for the Server Type.
- **Timeout** (required) The timeout in seconds. Range: 1 to 30. Default: 4.
- **Retries** (required) The number of retries. Range: 0 to 10. Default: 2.
- **Secret** (required) Only enabled when **Radius** or **TACACS+** is selected for Server Type.

- **Verify Secret** (required) A verification field so that you confirm what you typed into the Secret field. Only enabled when **Radius** or **TACACS+** is selected for Server Type.
- **NT Domain Controller Name** (required) Only enabled when NT Domain is selected as the Server Type.

Step 3 Enter the desired information for the AAA server you are defining.

Step 4 Click **Save**.

The AAA Servers window reappears with the new AAA server listed.

Deleting AAA Servers

From the AAA Servers window, you can delete specific AAA servers.

To delete a AAA server, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > AAA Servers**.

Step 2 Select one or more AAA servers to delete by selecting the check box to the left of the AAA server name.

Step 3 Click the **Delete** button.

The Delete AAA Server(s) window appears.

Step 4 Click the **Delete** button to confirm that you want to delete the AAA servers listed.

The AAA Servers window reappears with the specified AAA servers deleted.

Named Physical Circuits

Named physical circuits (NPCs) are named circuits that describe a physical connection between a CPE or PE-CLE and a PE-POP. The intermediate nodes of the NPCs can either be CPE or PE. They can be connected in a circular fashion forming a ring of devices, which is represented by an entity known as NPC Rings. NPC Rings represent the circular topology between devices (CPE or PE) to the Named Physical Circuits. To create an NPC, you must specify how the source CPE/PE-CLE and the destination PE-POP are connected and specify the intermediate nodes.

The connectivity of the NPCs is defined by specifying a set of devices serving as physical links; each device has two interfaces that are part of the NPC connections. The Incoming Interface defines the interface from the CE direction. The Outgoing Interface defines the interface toward the PE direction.

You can also add (meaning after the chosen device) or insert (meaning before the chosen device) an NPC Ring in the link.

Keep in mind the following when you are creating an NPC:

- In the ISC software, the device you select can be any node in the link. The ISC software only shows the appropriate devices. The first device *must* be a CPE or PE-CLE and the last device *must* be a PE-POP.
- NPCs should be created before the MPLS multi-device, VPLS, or L2VPN service request is created with cpe1 and pe1. So when you create the SR, you would select the policy, cpe1, pe1, and the NPC that defines the link between cpe1 and pe1.

This section describes how you can create and delete NPCs and create, edit, and delete NPC Rings. This section includes the following:

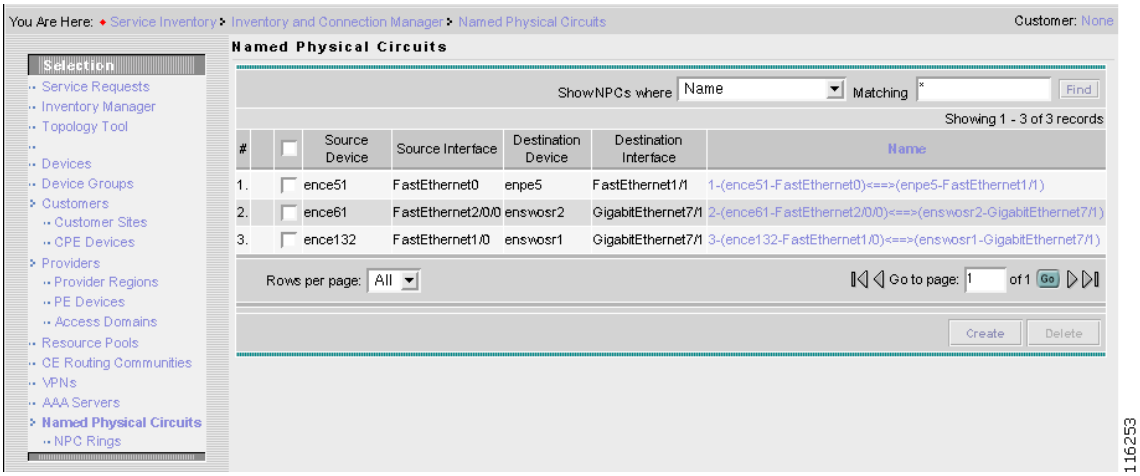
Accessing the Named Physical Circuits Window

The Named Physical Circuits feature is used to create and delete NPCs. You cannot edit or modify.

To access the Named Physical Circuits window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Named Physical Circuits** to access the window shown in Figure 3-101, "Named Physical Circuits Window."

Figure 3-101 Named Physical Circuits Window



From the Named Physical Circuits window, you can create or delete NPCs using the following buttons:

- **Create** Click to create new NPCs. Enabled only if no NPC is selected.
- **Delete** Click to delete selected NPCs (select by clicking the corresponding box(es)). Enabled only if one or more NPCs are selected.

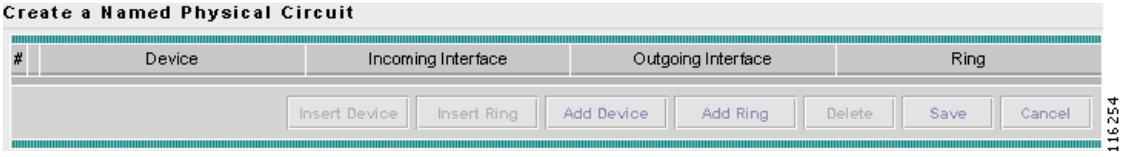
Creating a Named Physical Circuit

To add an NPC physical link, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Named Physical Circuit**.

Step 2 Click the **Create** button in Figure 3-101, "Named Physical Circuits Window," and a window, as shown in Figure 3-102, "Create a Named Physical Circuit," appears.

Figure 3-102 Create a Named Physical Circuit



Each line represents a physical link and each physical link contains the following attributes:

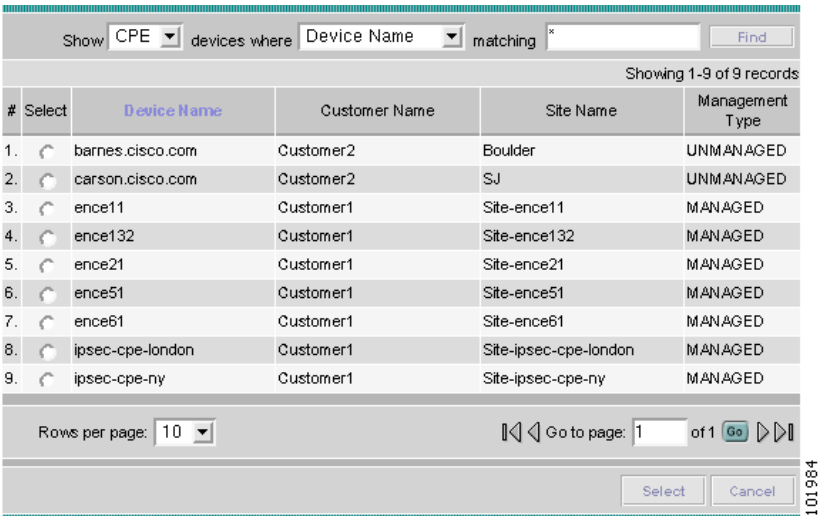
- **Device**
- **Incoming Interface**
- **Outgoing Interface**
- **Ring** (optional)

Note Before adding a ring in an NPC, create a ring and save it in the repository, as explained in the "Creating NPC Rings" section on page 3-129.

Note An NPC must have at least one link defined. The link must have two Devices, an Incoming Interface, and an Outgoing Interface.

Step 3 Click **Add Device** or **Insert Device** and a window as shown in Figure 3-103, "Select Device," appears.

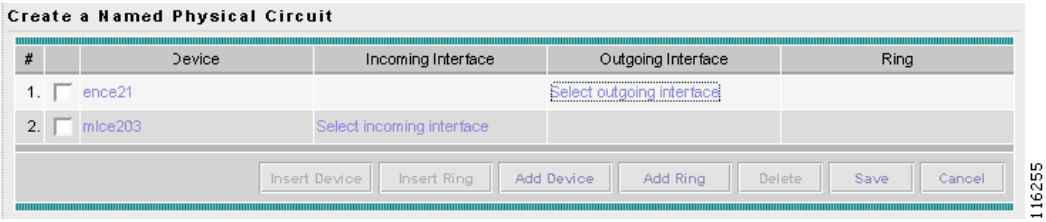
Figure 3-103 Select Device



Step 4 Be sure that the drop-down in **Show** is **CPE** or **PE**. Click a radio button next to a device and then click **Select**.

Step 5 Figure 3-102, "Create a Named Physical Circuit," reappears with the chosen **Device**.

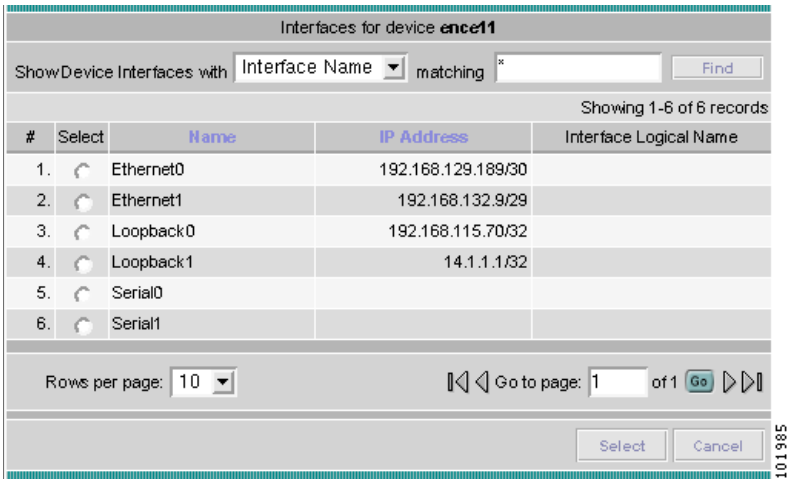
Figure 3-104 Select Device



Step 6 If you want to add a device to your NPC as the last item or after the item selected in the check box, click the **Add Device** button in Figure 3-102 on page 3-125 and then add device and interface information as explained in the previous steps. If you want to insert a device to your NPC as the first item or before the item selected in the check box, click the **Insert Device** button in Figure 3-102 on page 3-125 and then add device and interface information as explained in the previous steps.

Step 7 In the **Outgoing Interface** column in this new version of Figure 3-102, "Create a Named Physical Circuit," click **Select outgoing interface** and a window as shown in Figure 3-105, "Select Outgoing Interface," appears with a list of interfaces.

Figure 3-105 Select Outgoing Interface

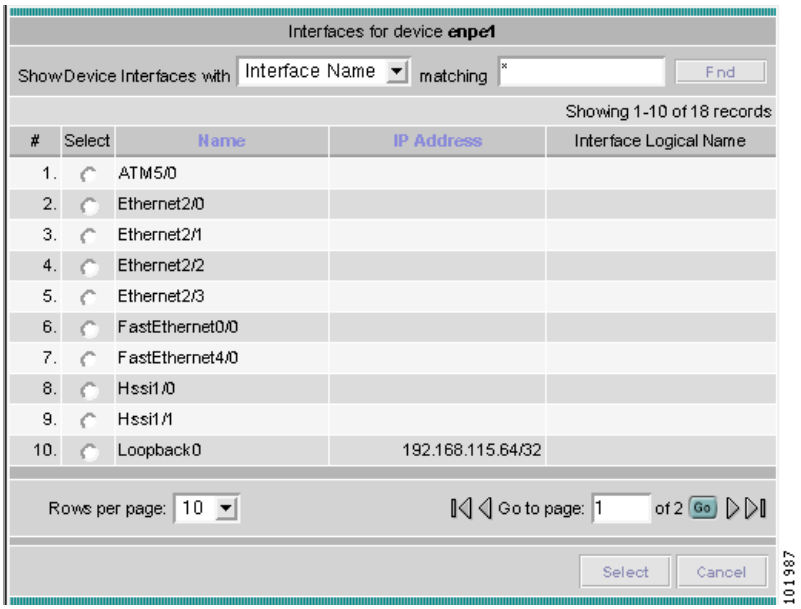


Step 8 Click a radio button next to the interface to be the source interface for this NPC and then click **Select**.

Step 9 Figure 3-102, "Create a Named Physical Circuit," reappears with the chosen **Interface**.

Step 10 In the **Incoming Interface** column in this new version of Figure 3-102, "Create a Named Physical Circuit," click **Select incoming interface** and a window as shown in Figure 3-106, "Select Incoming Interface," appears with a list of interfaces.

Figure 3-106 Select Incoming Interface



Step 11 Click a radio button next to the interface to be the incoming interface for this NPC and then click **Select**.

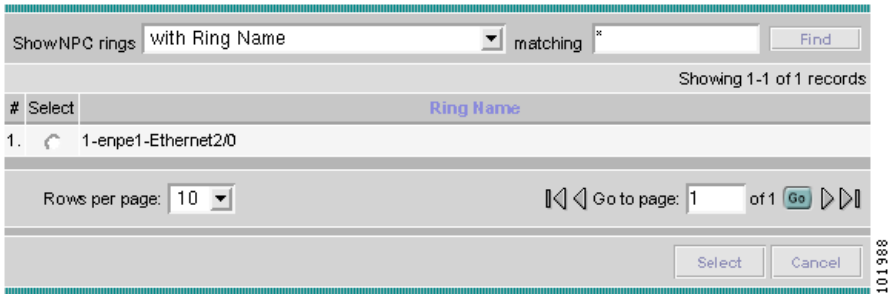
Step 12 Figure 3-102, "Create a Named Physical Circuit," reappears with the chosen **Incoming Interface**.

Step 13 If you created an NPC ring that you want to insert or add into this NPC, as explained in the "Creating NPC Rings" section on page 3-129, you can click **Insert Ring** or **Add Ring** and the ring appears at the beginning or before the item selected in the check box for **Insert Ring** or the ring appears at then end or after the item selected in the check box for **Add Ring**, as shown in Figure 3-107, "Select NPC Ring."

Note When inserting a ring, select the source device of the ring that connects to a source device or an NPC and the destination device of the ring that connects to the destination device of the NPC.

If you have not created an NPC ring that you want to insert into this NPC, proceed to Step 17.

Figure 3-107 Select NPC Ring



Step 14 Click a radio button next to the ring you choose and then click **Select**.

Step 15 Figure 3-102, "Create a Named Physical Circuit," reappears with the chosen **Ring**.

Step 16 Select the missing devices and interfaces as explained in the "Creating NPC Rings" section on page 3-129.

Step 17 Click **Save**.

Step 18 Figure 3-102, "Create a Named Physical Circuit," reappears with the new NPC listed.

Deleting Named Physical Circuits

To delete NPC(s), do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Named Physical Circuits** to access the window shown in Figure 3-101, "Named Physical Circuits Window."

Step 2 Select one or more NPCs to delete by selecting the check box(es) on the left.

Step 3 Click the **Delete** button.

The Delete NPC window appears.

Note If the specified NPC is being used by any of the Service Requests, you will not be allowed to delete it. An error message appears explaining this.

Step 4 Click the **Delete** button to confirm that you want to delete the NPCs listed.

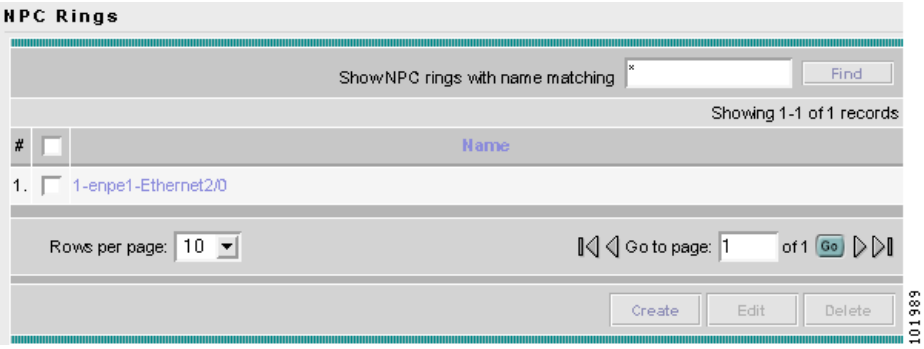
Figure 3-101, "Named Physical Circuits Window," reappears with the specified NPCs deleted.

Creating NPC Rings

Create NPC rings as follows:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > NPC Rings** and a window as shown in Figure 3-108, "NPC Rings," appears.

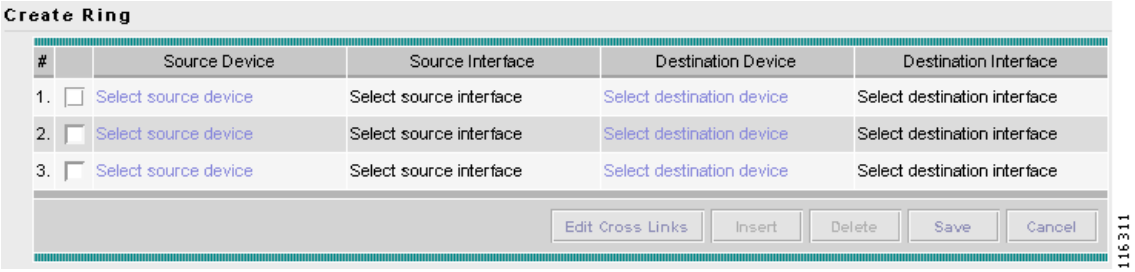
Figure 3-108 NPC Rings



Step 2 Click the **Create** button and a window as shown in Figure 3-109, "Create Ring," appears.

A ring has a minimum of three physical links that form of a ring.

Figure 3-109 Create Ring



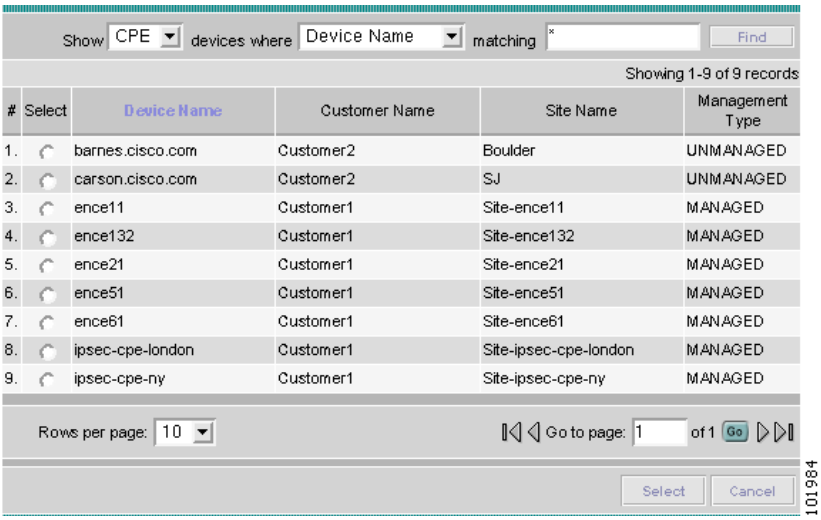
Note At any time, if you click **Cancel**, everything you have chosen disappears.

Step 3 Start with the first line, which represents the first physical link.

Step 4 In the **Source Device** column, click **Select source device** and a window as shown in Figure 3-110, "Select Source Device —CPE/PE," appears.

Note The CPE you choose *must* be a Multi-VRF CE.

Figure 3-110 Select Source Device —CPE/PE



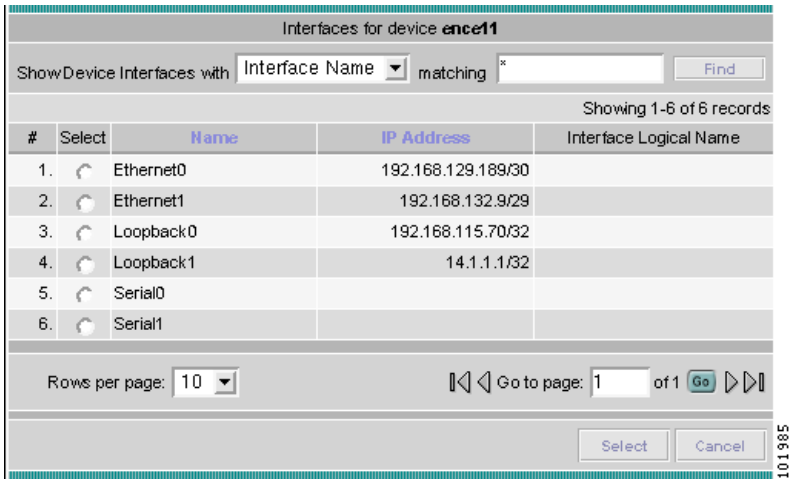
Step 5 Click a radio button next to the device to be the source device for this physical link and then click **Select**.

Step 6 Figure 3-109, "Create Ring," reappears with the chosen **Source Device**.

Note When choosing the **Source Device** for a physical link, this same choice is made for the **Destination Device** for the previous physical link (or the last physical link if you are choosing for the first physical link). For a selected device, do not select the same interface for the source and destination interface.

Step 7 In the **Source Interface** column in this new version of Figure 3-109, "Create Ring," click **Select source interface** and a window as shown in Figure 3-111, "Select Source Interface," appears with a list of interfaces.

Figure 3-111 Select Source Interface

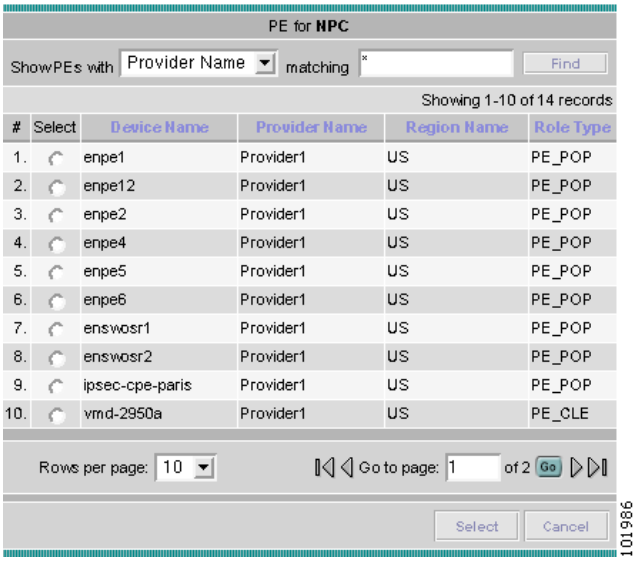


Step 8 Click a radio button next to the interface to be the source interface for this physical link and then click **Select**.

Step 9 Figure 3-109, "Create Ring," reappears with the chosen **Source Interface**.

Step 10 In the **Destination Device** column in this new version of Figure 3-109, "Create Ring,", click **Select destination device** and a window as shown in Figure 3-112, "Select Destination Device —CPE/PE," appears.

Figure 3-112 Select Destination Device —CPE/PE



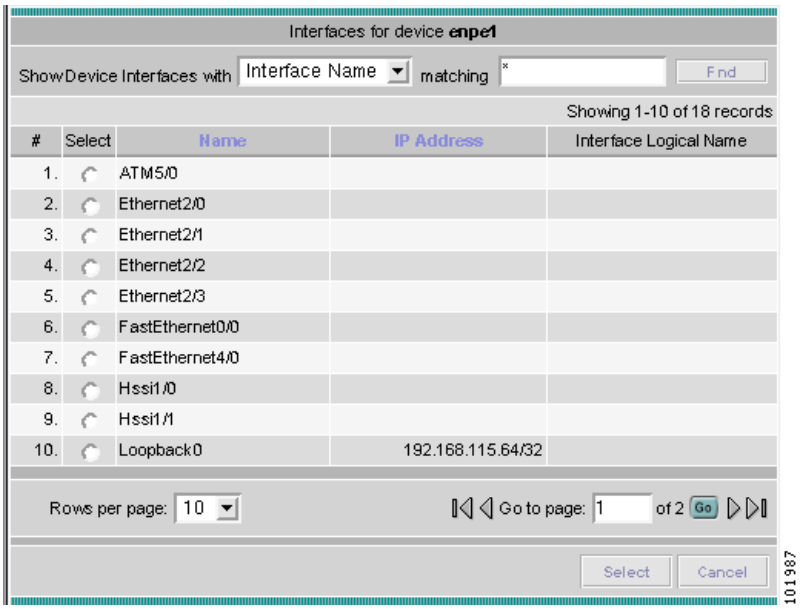
Step 11 Click a radio button next to the device to be the destination device for this physical link and then click **Select**.

Step 12 Figure 3-109, "Create Ring," reappears with the chosen **Destination Device**.

Note When choosing the **Destination Device** for the a physical link, this same choice is made for the next **Source Device**. Do not choose the same Interface for these devices.

Step 13 In the **Destination Interface** column in this new version of Figure 3-109, "Create Ring," click **Select destination interface** and a window as shown in Figure 3-113, "Select Destination Interface," appears with a list of interfaces.

Figure 3-113 Select Destination Interface



Step 14 Click a radio button next to the interface to be the destination interface for this NPC and then click **Select**.

Step 15 Figure 3-109, "Create Ring," reappears with the chosen **Destination Interface**.

Step 16 Repeat Step 4 to Step 15 for the middle physical links and Step 4 to Step 9 for the last physical link.

Step 17 If you want to insert an extra physical link in the ring, select the check box for the line that represents the physical link you want the new physical link to follow and click **Insert**. Implement Step 4 to Step 15 to fill in the remaining entries in this new physical link.

Step 18 If you want to delete a physical link in the ring but a minimum of three physical links will remain, select the check box for the line that represents the physical link you want to delete and click **Delete**.

Step 19 If you want to establish additional cross links between non-adjacent devices in this ring, you can click **Edit Cross Links** in Figure 3-109, "Create Ring," and you then view a new window like Figure 3-109 with no entry. Click the **Add** button and you can choose from the devices already in your ring. The result is a new entry in Figure 3-109 with this device as the **Source Device**. Establish the Destination Device and Source and Destination Interfaces as you did when creating the ring. The choices of devices and interfaces is limited to those already established in your ring.

Step 20 When you are completed setting up your ring, click **Save**.

Step 21 The new ring is added in Figure 3-108, "NPC Rings," and a green check for Succeeded appears. The new ring is identified by the source device-source interface.

Step 22 To create a ring with more than three physical links, select the check box for the link in Figure 3-109 on page 3-129 to which you want to insert and the **Insert** button is then enabled. Proceed in adding links as explained in this section.

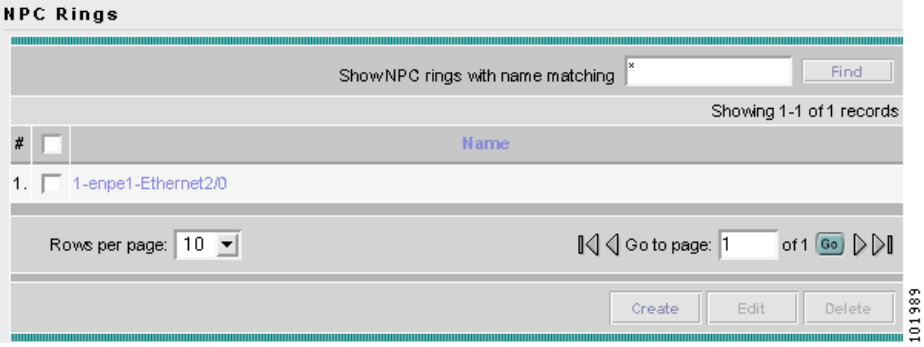
Editing NPC Rings

To edit NPC rings, do the following:

Note If the specified NPC Ring is participating in any of the Named Physical Circuits, then you can not edit the ring. An error message appears containing IDs of the NPCs that contain the NPC Ring.

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > NPC Rings** and a window as shown in Figure 3-114, "NPC Rings," appears.

Figure 3-114 NPC Rings



Step 2 Select the check box next to the line that represents an NPC ring and then click **Edit.** A window as shown in Figure 3-109, "Create Ring," appears with all the data for this ring. Proceed as in the "Creating NPC Rings" section on page 3-129 to make any changes you want.

Step 3 When you have the ring as you want it, click **Save**.

Step 4 Figure 3-108, "NPC Rings," appears with the appropriate name (source device-source interface) and a green check for Succeeded appears.

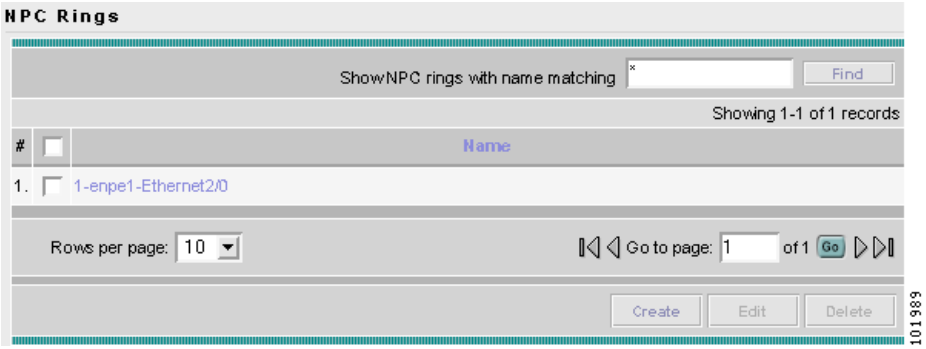
Deleting NPC Rings

To delete NPC rings, do the following.

Note If the specified NPC Ring is participating in any of the Named Physical Circuits, then you can not delete the ring. An error message appears containing IDs of the NPCs that contain the NPC Ring.

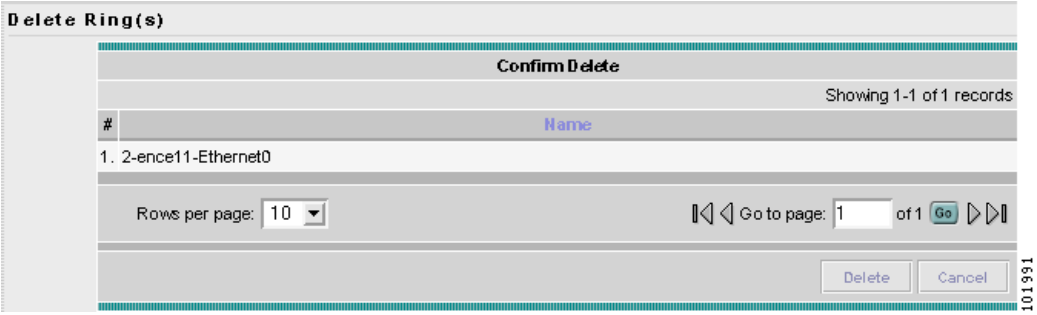
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > NPC Rings** and a window as shown in Figure 3-115, "NPC Rings," appears.

Figure 3-115 NPC Rings



Step 2 Select the check box(es) next to the line(s) that represent(s) NPC ring(s) that you want to delete and then click **Delete**. A window as shown in Figure 3-116, "Delete Rings," appears with the chosen ring(s) for deletion.

Figure 3-116 Delete Rings



Step 3 Click **Cancel** if you change your mind about deleting the chosen ring(s) or click **Delete** to actually delete the ring.

Step 4 Figure 3-115, "NPC Rings," appears with the remaining ring names and a green check for Succeeded appears.