CHAPTER 4

Provisioning MPLS VPN Service Requests

The focus of the VPN Solutions Center product is the service provided for a customer on the link between the customer's CE and the provider's PE. This chapter describes how you create a service request in the VPN Solutions Center software, as well as how to modify and delete service requests. Finally, this chapter tells you how to check on a service request's status and find out what went wrong if the request failed.

The main topics presented in this chapter are as follows:

Service Request Summary

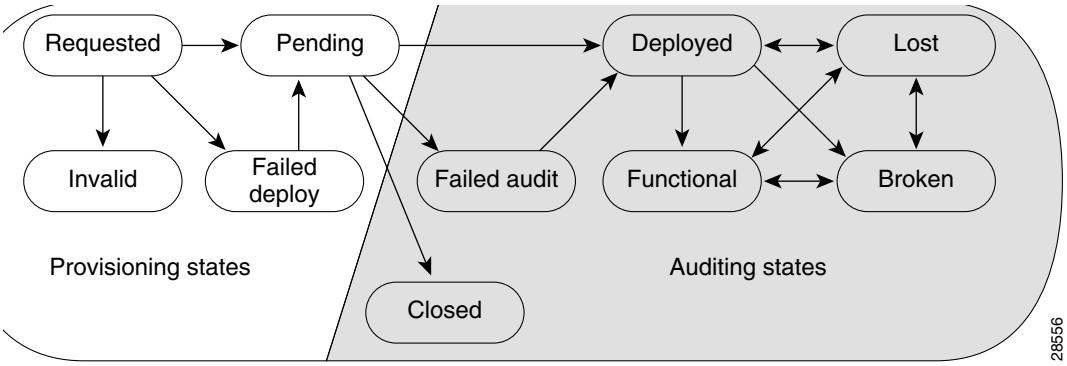
The service model is the centerpiece of service provisioning. With the service model, the VPN Solutions Center software can capture the specified VPN service provisioning request, analyze the validity of the request, and audit the provisioning results.

The service provider operators take all service request information from their customers. VPN Solutions Center can assist the operator in making entries because the product has customer information such as the VPN information, the list of the assigned PEs and CEs, and so forth.

The VPN Console steps the operator through the process and simplifies the task of provisioning the CE and PE by automating most of the tasks required to set up an MPLS VPN.

Figure 4-1 shows a high-level diagram of the relationships and movement among VPN Solutions Center service request states.

Figure 4-1 Service Request States: Movement and Relationships



The sections below describe each of the service request states and their transition sequences.

Definitions of VPN Solutions Center Service Request States

Table 4-1 describes the functions of each VPN Solutions Center service request state. They are listed in alphabetical order.

Table 4-1 Summary of VPN Solutions Center Service Request States

Service Request Type	Description
Broken	While the router is correctly configured, the service is unavailable (due to a broken cable or Layer 2 problem, for example). A 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.
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 a successful audit of a remove request. VPN Solutions Center does not remove a service request from the database to allow for extended auditing. Only a specific administrator action results in service requests being removed.
Deployed	A service request moves to Deployed if the configlet commands have been verified as 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.
Failed Audit	This state indicates that the service request has not yet successfully passed an audit, and therefore has not yet moved to either the Functional or Deployed state. The Failed Audit state is initiated from the Pending state. Once a service request is deployed successfully, it cannot reenter the Failed Audit state (except when the service request is redeployed).

Table 4-1 Summary of VPN Solutions Center Service Request States (continued)

Service Request Type	Description
Failed Deploy	After provisioning occurred, the service request failed to download the configuration updates to the router. A service request moves to Failed Deploy if the Telnet Gateway Server (TGS) detected an error during the deployment process. If TGS is not being used to download configuration updates, and VPNSC is simply exporting configuration updates to a directory, there is no way to distinguish between a service request in the Failed Deploy and Pending states. The cause for a Failed Deploy status is that TGS 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, etc.). If the configuration updates are exported to a directory, the service request cannot move into a Failed Deploy state.
Functional	A 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 configuration-level verification.
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 configlets 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 deployed, 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 or Functional.
Pending	A service request moves to Pending when the Provisioning Driver determines that the request looks consistent and was able to generate the required configlets for this request. Pending indicates that the service request has generated the configlets and the configlets 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 done 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.

Service Request State Transition Sequences

Table 4-2 on page 4-4 and Table 4-3 on page 4-5 show the state transition paths for VPN Solutions Center service requests. The beginning state of a service request is listed in the first column; the states that service requests transition to are displayed in the heading row.

For example, to use Table 4-2 to trace the state of a Pending service request to Functional, find "**Pending**" in the first column and move to your right until you find "**Functional**" in the heading. You can see that for a service request to move from Pending to Functional, a successful routing audit must take place.

Table 4-2 shows the service request transitions from *Requested* to *Lost*.

Table 4-2 State Transition Paths for VPN Solutions Center Service Requests (Part 1)

Service Request States	Requested	Pending	Failed Audit	Deployed	Functional	Lost
Requested	No transition to Requested	Successful service request deployment	No transition to Failed Audit	No transition to Deployed	No transition to Functional	No transition to Lost
Pending	No transition to Requested	—Successful service request deployment —Audit with error	Audit is not successful	Audit is successful	Routing audit is successful	No transition to Lost
Failed Audit	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	Audit is successful	Routing audit is successful	No transition to Lost
Deployed	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	Audit is successful	Routing audit is successful	Audit found error
Functional	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	No transition to Deployed	Routing audit is successful	Audit found error
Lost	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	Audit is successful	Routing audit is successful	Audit found error
Broken	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	No transition to Deployed	Routing audit is successful	Audit found error
Invalid	No transition to Requested	Successful service request redeployment	Redeployment caused service request error	No transition to Deployed	No transition to Functional	No transition to Lost

Table 4-2 State Transition Paths for VPN Solutions Center Service Requests (Part 1) (continued)

Service Request States	Requested	Pending	Failed Audit	Deployed	Functional	Lost
Failed Deploy	No transition to Requested	Successful service request redeployment	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Deployed	No transition to Functional	No transition to Lost
Closed	No transition to Requested	No transition to Pending	No transition to Failed Audit	No transition to Deployed	No transition to Functional	No transition to Lost

Table 4-3 shows the service request transitions from *Broken* to *Closed*.

Table 4-3 State Transition Paths for VPN Solutions Center Service Requests (Part 2)

Service Request States	Broken	Invalid	Failed Deploy	Closed
Requested	No transition to Broken	Deploy Service Request error	Deployment failed	No transition to Closed
Pending	Route audit is not successful. Configlet is correct.	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	Removal of the service request is successful
Failed Audit	Route audit is not successful. Configlet is correct.	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
Deployed	Route audit is not successful. Configlet is correct.	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
Functional	Route audit is not successful. Configlet is correct.	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
Lost	Route audit is not successful. Configlet is correct.	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
Broken	Route audit is not successful. Configlet is correct.	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
Invalid	No transition to Broken	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
Failed Deploy	No transition to Broken	Redeploy service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
Closed	No transition to Broken	No transition to Invalid	No transition to Failed Deploy	No transition to Closed

Overview of Service Request Definition Process

Provisioning a VPN provides a method to build a service for site-to-site connectivity between a provider edge router and a customer edge router. It includes the following steps:

1. From the VPN Console, define a service request to add VPN service between a CE and PE.
2. Schedule to download the new configuration to the CE and PE pairs.
3. Use the reports available from the Provisioning menu to verify the service requests and view configlets.

The first step in provisioning a VPN is to define a *service request*. A service request defines through whom (the provider edge router) and to whom (the customer edge router) the service is provided. In this procedure, you determine the specifics of the link between the PE and CE.

The important elements of the process are as follows:

1. When defining a service request, you define the VPN's membership in a *CE Routing Community* (CERC).

   A CE Routing Community describes how CEs in a VPN communicate with each other. The most common examples are hub-and-spoke and full mesh topologies.

   For more information on CERCs, see the "CE Routing Communities" section on page 1-18.
2. Define the routing protocol for the PE-CE link.
3. Define the IP addressing scheme for the PE-CE link.

   Within a VPN (or extranet), all IP addresses must be unique. Customer IP addresses are not allowed to overlap with provider IP addresses. Overlap is possible only when two devices cannot see each other; that is, they are in isolated, non-extranet VPNs.

   The VPN Solutions Center software assumes that it has an IP address pool to draw addresses from. The only way to guarantee that the product can use these addresses freely is if they are provider IP addresses.

   Predefining a unique section (or sections) of IP address space for the PE-CE links is the only way to ensure stable security. Thus, because of the security and maintenance issues, Cisco does not recommend using customer IP addresses on the PE-CE link.

Adding a Service for a PE-CE Link

A service request is an instance of service contract between a customer edge router (CE) and a provider edge router (PE). The service request wizard asks you to enter several parameters, including the specific interfaces on the CE and PE routers, routing protocol information, and IP addressing information.

You can also integrate a VPN Solutions Center template with a service request. You can associate one or more templates to the CE and the PE.

To add VPN service between a PE and CE, follow these steps:

Step 1 From the VPN Console, choose **Provisioning > Add VPN Service to CE**.

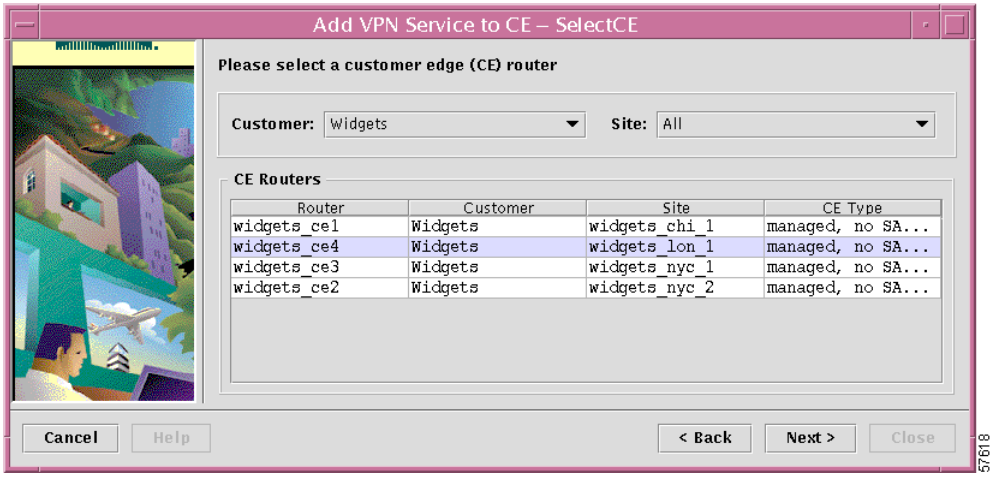
The introductory panel in the Add VPN Service to CE wizard appears. It is informational only.

Step 2 Click **Next**. The Select CE dialog box appears (see Figure 4-2).

Selecting a Customer Edge Router (CE)

Step 1 From the Select CE dialog box, select the customer edge router for this link (see Figure 4-2).

Figure 4-2 The Select CE Dialog Box



Step 2 From the Customer drop-down list, select the appropriate customer.

Step 3 From the Site drop-down list, select the appropriate site.

Step 4 From the CE Routers list, select the appropriate CE for this link, then click **Next**.

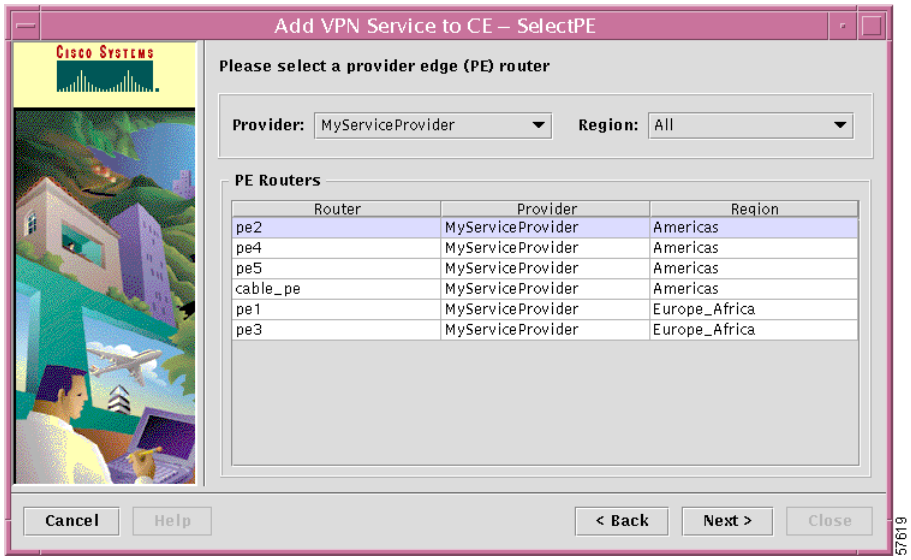
Note If you are configuring a service for a cable link, the specified CE should be an unmanaged CE.

The Select PE dialog box appears (see Figure 4-3).

Selecting the Provider Edge Router (PE)

Step 1 From the Select PE dialog box, select the provider edge router for this link.

Figure 4-3 Select PE Dialog Box



Step 2 From the Provider drop-down list, select the appropriate service provider name.

Step 3 From the Region drop-down list, select the appropriate region.

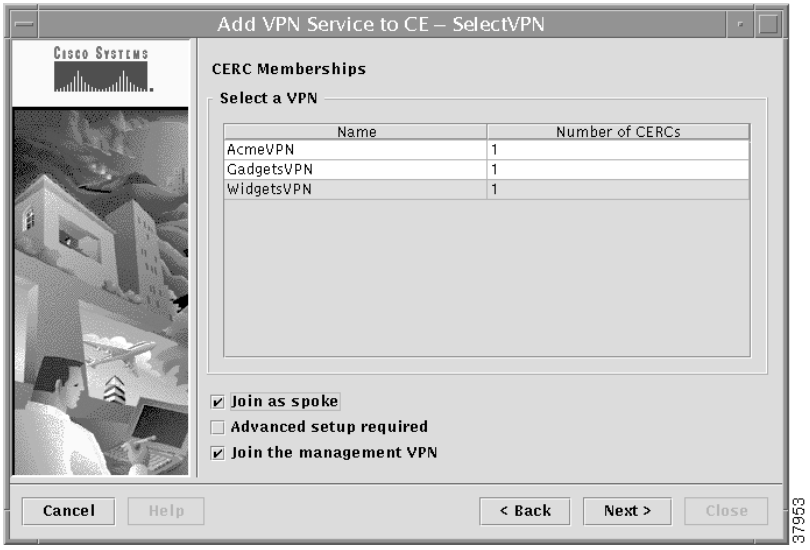
Step 4 From the PE Routers list, select the provider edge router for this link, then click **Next**.

The Select VPN: CERC Memberships dialog box appears (see Figure 4-4).

Defining CERC Membership and Joining the Management VPN

Step 1 From the Select VPN: CERC Memberships dialog box, select the appropriate VPN from the list and specify the VPN topology.

Figure 4-4 Select VPN: CERC Memberships Dialog Box



The most common types of VPNs are *hub-and-spoke* and *full mesh*. These two basic types of VPNs—full mesh and hub and spoke—can be represented with a single CERC.

For additional information on CE routing communities, see the "CE Routing Communities" section on page 1-18 and the "Defining CE Routing Communities" section on page 3-15.

Step 2 If you are building a VPN with a hub-and-spoke topology, check the **Join as Spoke** check box.

- 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.

Step 3 If you are building a VPN with CEs that are members of multiple VPNs (extranets), check the **Advanced setup required** check box.

Extranet provisioning provides a way to create multiple VPN connectivity to a single VRF.

Step 4 If you are adding a CE to the *management VPN*, check the **Join the management VPN** check box. For more information, see the "Implementing the Management VPN Technique" section on page 3-23.

When you use the VPN Solutions Center software to define a management VPN, the software automatically generates an *export route map* for the management VPN.

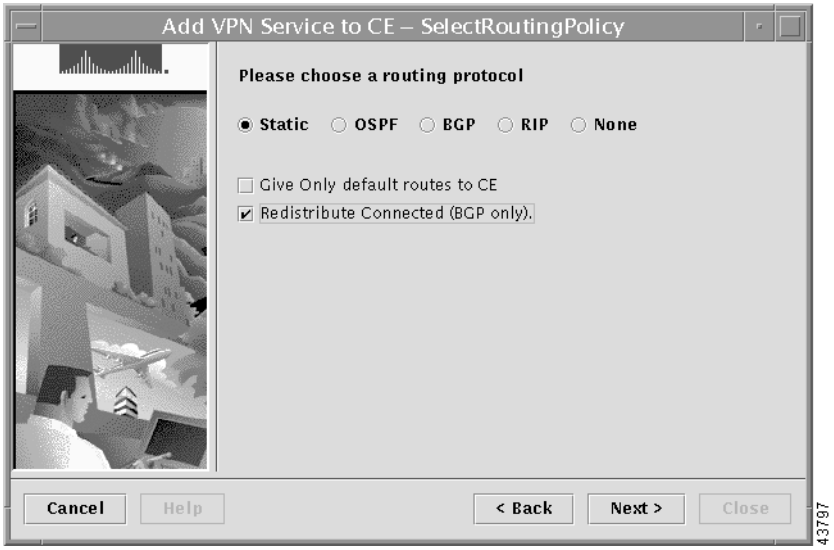
Step 5 Click **Next**.

The Select Routing Policy dialog box appears (see Figure 4-5).

Choosing the Routing Protocol for the Link

The Select Routing Policy dialog box appears. The first routing protocol option is Static routing. Figure 4-5 shows the options available when you choose to use a Static protocol.

Figure 4-5 The Static Protocol Routing Policy Options



Step 1 Choose the routing protocol for the PE-CE link.

The routing protocol you choose must run on both the PE and the CE.

- You can choose *Static* (for specifying a static route), *OSPF* (Open Shortest Path First), *BGP* (Border Gateway Protocol), *RIP* (Routing Information Protocol), or *None* (to specify parameters for cable service).
- The wizard presents a different sequence of screens and requires different information depending on which protocol you choose.

Step 2 Complete the necessary fields and other information required for the selected routing protocol as described below, then click **Next**.

Proceed to "Specifying Redistributed Protocols on the Link" section on page 4-17.

Static Routes Options

Step 1 To define static routes on the PE-CE link, choose the **Static** radio button. VPN Solutions Center displays the dialog box shown in Figure 4-5.

The Static Routes dialog box provides the following options:

- *Give Only Default Routes to CE*

  When using the **Give only default routes to CE** option with static route provisioning on the PE-CE link, the product creates a default route on the CE that points to the PE. The VRF static route to the CE's site is redistributed into BGP to other sites in the VPN.

When you select the **Give only default routes to CE** option, the default route (0.0.0.0/32) is filled in for you; the site contains no Internet feed or any other requirement for a default route. When it encounters a packet that does not route locally, it can send the packet to the VPN.

- *Redistribute Connected (BGP only)*

  When you check **Redistribute Connected**, the connected routes (that is, the routes to the directly connected PEs or CEs) are distributed to all the other CEs in that particular VPN.

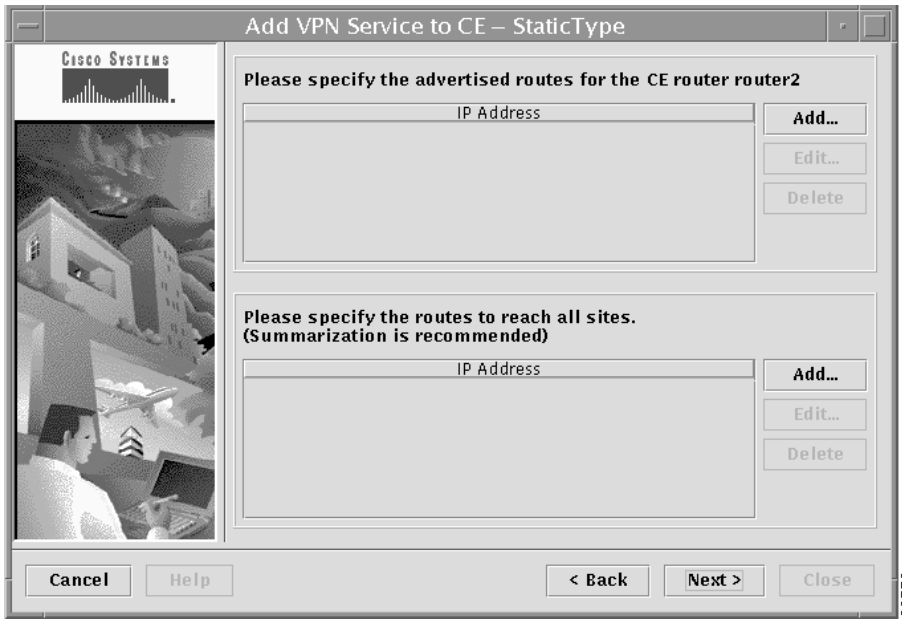
Note When joining the management VPN and you are using IP numbered addresses on the link, you must enable the **Redistribute Connected** option.

Step 2 When you click **Next**, VPN Solutions Center software asks for two lists of static routes (see Figure 4-6):

- Those static routes to put on the PE, which describe all of the address space in the CE's site.
- Those static routes to put on the CE, which describe all of the address space throughout the VPN.

  That is, the product informs the PE what the CE needs to know, and informs the CE what the VPN (via the PE) needs to know.

Figure 4-6 Specifying the Static Routes on the PE-CE Link



Step 3 To specify the advertised routes for the specified CE, click the **Add** button in the upper right corner of the dialog box. The Advertised Routes dialog box appears (see Figure 4-7).

Figure 4-7 Specifying the Advertised Routes to Put on the PE

Step 4 Enter the IP address of the advertised static route to be placed on the PE to define the CE's address space, then click **Add**.

The specified advertised route is displayed in the field.

Step 5 Click **OK**. You return to the Static Type dialog box (see Figure 4-6).

Step 6 To specify the static routes to put on the CE (which describes all of the address space throughout the VPN), click the **Add** button in the lower right corner of the dialog box. The Routes to Reach All Sites dialog box appears (see Figure 4-8).

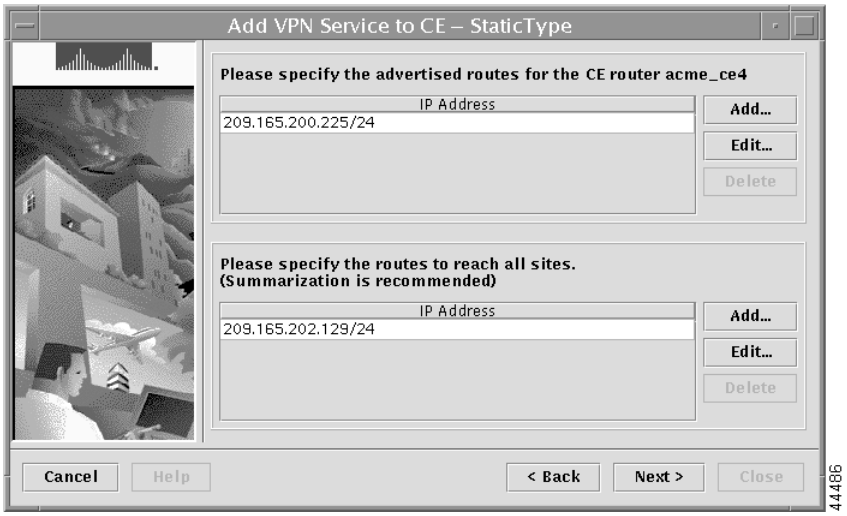
Figure 4-8 Specifying the Static Routes to Reach All Sites in the VPN

Step 7 Enter the IP address of the static route to reach all sites in the VPN, then click **Add**.

The specified static route is displayed in the field.

Step 8 Click **OK**. You return to the Static Type dialog box, which now displays the specified routes (see Figure 4-9).

Figure 4-9 Static Routes Displayed



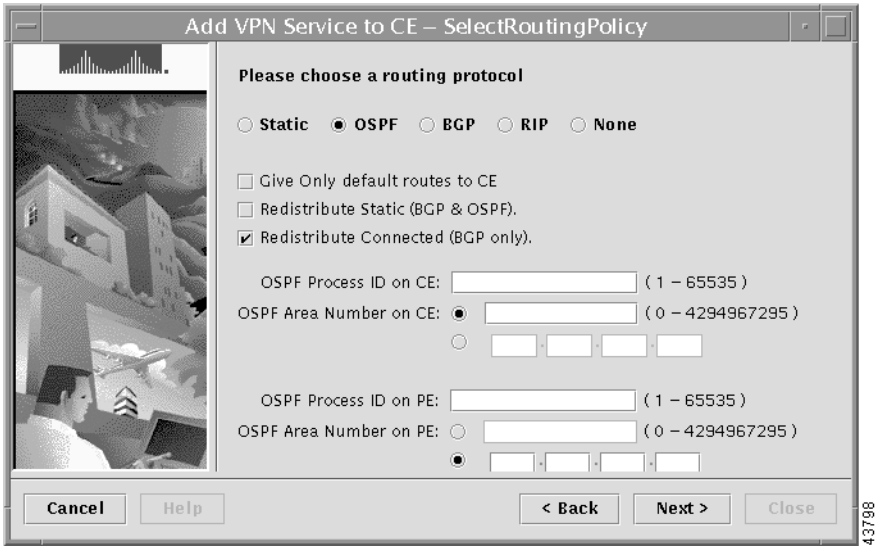
Step 9 When finished specifying the static routes for the PE-CE link, click **Next**.

The Redistribution dialog box appears, which specifies the protocols to be redistributed on the link (see the "Specifying Redistributed Protocols on the Link" section on page 4-17).

OSPF Protocol Options

When you choose the **OSPF** radio button, VPN Solutions Center displays the dialog box shown in Figure 4-10:

Figure 4-10 The OSPF Protocol Routing Policy Options



- *Give Only Default Routes to the CE*

  When you enable the **Give only default routes to CE** option, you indicate whether the site needs *full routing* or *default routing*. Full routing is when the site must know specifically which other routes are present in the VPN. Default routing is when it is sufficient to send all packets that are not specifically for your site to the VPN.

  A device can only have one default route. Therefore, the VPN can use a default route, but only on condition that the customer site does not already have a different one. The most common reason to already have a default route is that the site has an Internet feed that is independent of the VPN.

  If the CE site already has Internet service, the CE can either 1) route all packets to unknown destinations to the Internet, or 2) learn all the routes in the Internet. The obvious choice is to route all packets to unknown destinations to the Internet. If a site has an Internet feed, it may already have a default route. Under such conditions, setting the VPN as the default route is incorrect; the VPN should only route packets meant for other VPN sites.

- *Redistribute Static (BGP and OSPF)*

  When you enable the **Redistribute Static** option for OSPF, the software redistributes the static routes into the core network (running BGP) and to the CE (running OSPF).

- *Redistribute Connected (BGP only)*

  When you enable the **Redistribute Connected** option for OSPF, the software redistributes the connected routes (that is, the routes to the directly connected PEs or CEs) to all the other CEs in that particular VPN.

- *OSPF Process ID on CE*

  The OSPF process ID is a unique value assigned for each OSPF routing process within a single router—this ID is internal to the CE only. You can enter this number either as any decimal number from 1 to 65535 or a number in dotted decimal notation.

- *OSPF Area Number on CE*

  An *area* in OSPF terms is a grouping of contiguous OSPF networks and hosts. OSPF areas are logical subdivisions of OSPF autonomous systems. The topology of each area is invisible to entities in other areas, and each maintains its own topological database.

  You can enter the OSPF area number for the CE either as any decimal number in the range specified or a number in dotted decimal notation.

- *OSPF Process ID on PE*

  The OSPF process ID is a unique value assigned for each OSPF routing process within a single router—this ID is internal to the PE only.

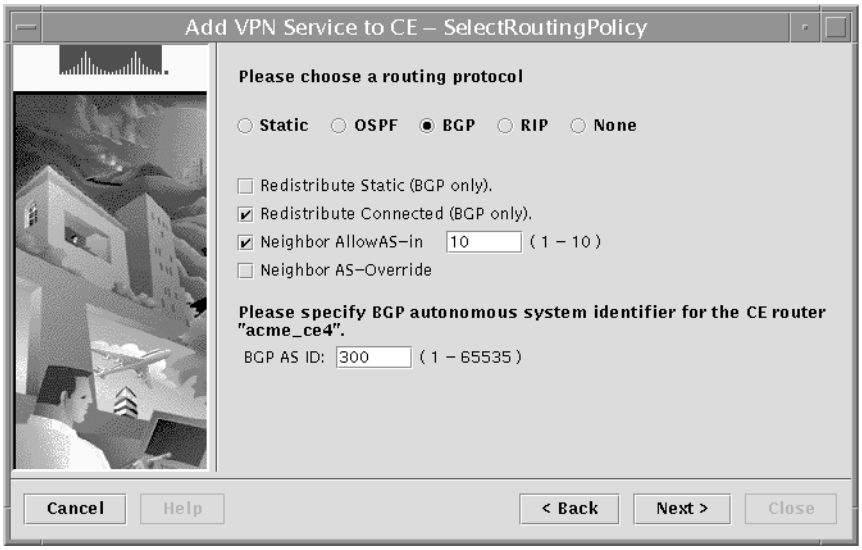
- *OSPF Area Number on PE*

  You can enter the OSPF area number for the PE either as any decimal number in the range specified or a number in dotted decimal notation.

BGP Protocol Options

When you choose the **BGP** radio button, VPN Solutions Center displays the dialog box shown in Figure 4-11:

Figure 4-11 The BGP Protocol Routing Policy Options



- *Redistribute Static (BGP only)*

  When you enable the **Redistribute Static** option for BGP, the software redistributes the static routes into the core network and to the CE, both of which are running BGP in this configuration.

- *Redistribute Connected (BGP only)*

  When you enable the **Redistribute Connected** option for BGP, the software redistributes the connected routes (that is, the routes to the directly connected PEs or CEs) to all the other CEs in that particular VPN.

- *Neighbor AllowAS-in*

  When you check the **Neighbor AllowAs-in** option, you can specify a maximum number of times (up to 10) that the service provider autonomous system (AS) number can occur in the autonomous system path.

- *Neighbor AS-Override*

  When you check the **Neighbor AS-Override** option, you configure VPN Solutions Center to reuse the same AS number on all the VPN's sites.

- *BGP Autonomous System (AS) ID for the CE*

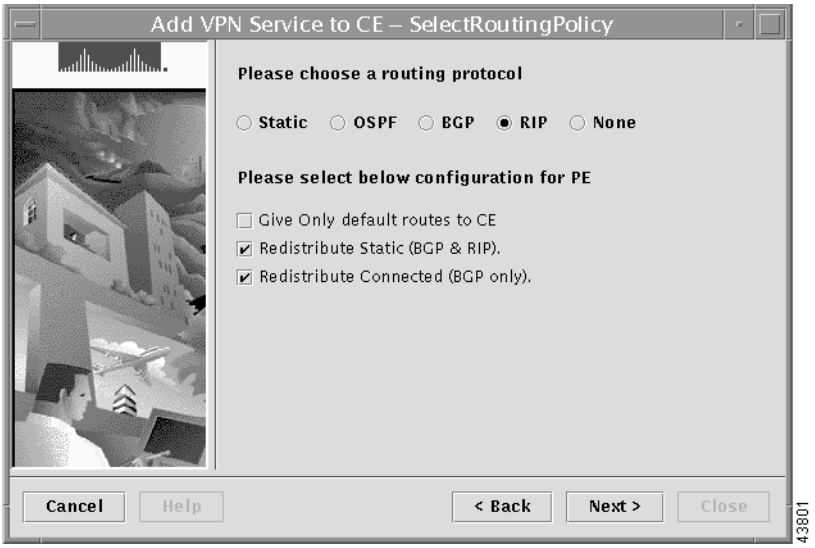
  Enter the BGP autonomous system number for the CE (that is, the customer's BGP network). The number assigned here is different from the BGP AS number for the service provider's core network.

  Proceed to "Specifying Redistributed Protocols on the Link" section on page 4-17.

RIP Protocol Options

When you choose the **RIP** radio button, VPN Solutions Center displays the dialog box shown in Figure 4-12:

Figure 4-12 The RIP Protocol Routing Policy Options



- *Give Only Default Routes to CE*

  When you enable the **Give only default route to CE** option for RIP, the product creates a default RIP route on the PE; the default RIP route points to the PE and is sent to the CE. The provisioning request gives you the option of redistributing any other routing protocols in the customer network into the CE's RIP routing protocol. The RIP routes on the PE to the CE's site are redistributed into BGP to other VPN sites.

  When you choose the **Give only default route to CE** option for RIP routing, the PE instructs the CE to send any traffic it cannot route any other way to the PE. This option should *not* be used if the CE's site needs a default route for any reason, such as having a separate Internet feed.

- *Redistribute Static (BGP and RIP)*

  When you enable the **Redistribute Static** option for RIP, the software redistributes the static routes into the core network (running BGP) and to the CE (running RIP).

- *Redistribute Connected (BGP only)*

  When you enable the **Redistribute Connected** option for BGP, the software redistributes the connected routes (that is, the routes to the directly connected PEs or CEs) to all the other CEs in that particular VPN.

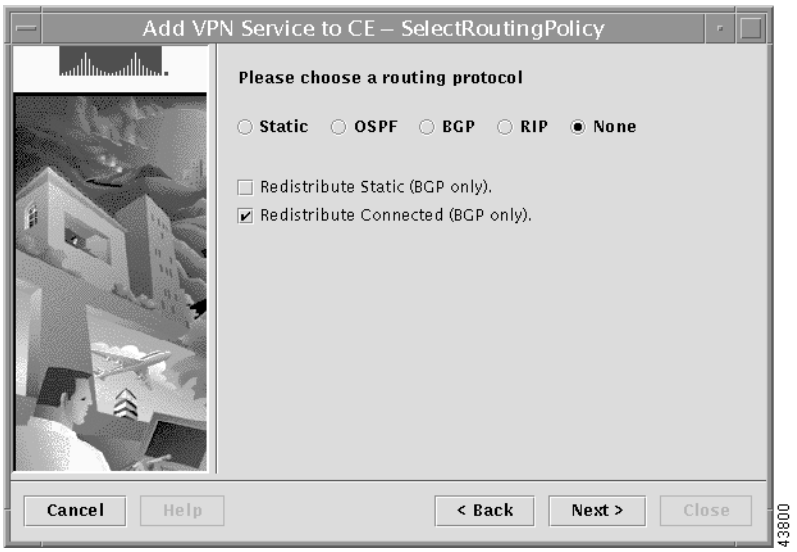
  Proceed to "Specifying Redistributed Protocols on the Link" section on page 4-17.

The None Protocol Options (for Cable Service)

The **None** option in the Routing Policy dialog box indicates that you do not want to run a routing protocol on the selected PE-CE link. *This option is provided to allow for configuring service over a cable link.* For details, see "Provisioning the Cable Maintenance Subinterface" section on page 7-9.

When you choose the **None** radio button, VPN Solutions Center displays the dialog box shown in Figure 4-13:

Figure 4-13 The Routing Policy Options for None (Cable Services)



- *Redistribute Static (BGP)*

  When you enable the **Redistribute Static** option for None, the software redistributes the static routes into the core network (running BGP).

- *Redistribute Connected (BGP only)*

  When you enable the **Redistribute Connected** option for None, the software redistributes the connected routes (that is, the routes to the directly connected PEs or CEs) to all the other CEs in that particular VPN.

Note Because there is no routing protocol on this PE-CE link, enabling the **Redistribute Connected** option for this topology is highly recommended.

Specifying Redistributed Protocols on the Link

When you complete the Routing Policy wizard and click **Next**, the Redistribution dialog box appears (see Figure 4-14).

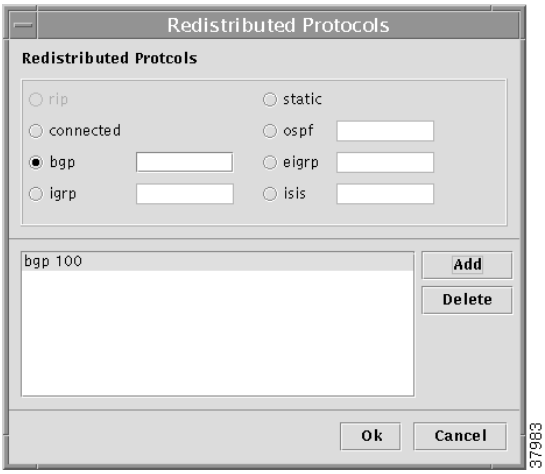
Step 1 If protocol redistribution is not required on this link, click **Next**.

Step 2 If necessary, specify the routing protocols that must be redistributed from the CE.

Step 3 Click **Add**.

The Redistributed Protocols dialog box appears (see Figure 4-14).

Figure 4-14 Redistributing Routing Protocols



Step 4 Select the protocol to be redistributed.

Step 5 Enter the appropriate AS number (BGP, IGRP, and EIGRP), process number (OSPF), or tag number (ISIS) corresponding to your protocol selection.

Step 6 Click **Add**.

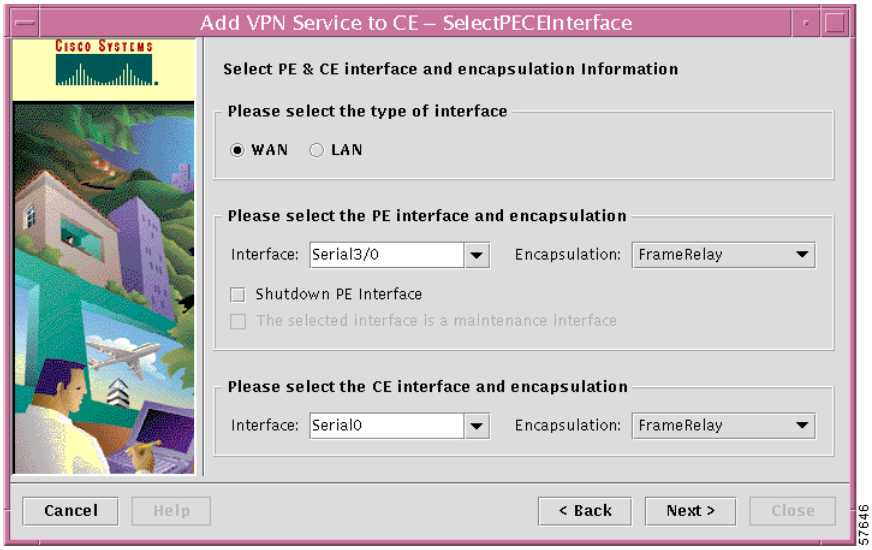
Step 7 The redistributed protocol information is displayed in the dialog box.

Step 8 Click **OK**, then click **Next**.

Defining the Interfaces on the PE-CE Link

Step 1 Define the interfaces for the PE-CE link.

Figure 4-15 The Select PE-CE Interfaces Dialog Box



Step 2 Specify the type of interfaces for the PE-CE link:

a. Wide Area Network (WAN)

b. Local Area Network (LAN)

Step 3 Select the PE interface and its encapsulation method from the drop-down lists.

- The interfaces available are determined by the PE's configuration file.
- The encapsulation methods are determined by which interface you select.

Step 4 Enable the **Shutdown** and **Maintenance Interface** options if appropriate:

- When you check the **Shutdown PE Interface** checkbox, the specified PE interface will be configured in a shut down state.
- When you select **Cable** for the PE interface, the **Selected interface is a maintenance interface** option is enabled.

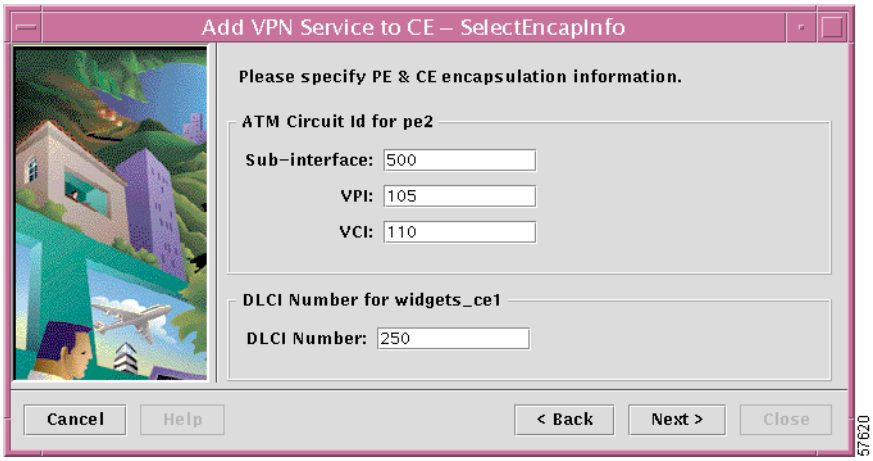
  Checking this option provisions the cable maintenance interface; this interface is always configured as subinterface 1 (for example, if the selected cable interface is *3/0*, the maintenance subinterface is *3/0.1*). For details, see the "Provisioning the Cable Maintenance Subinterface" section on page 7-9.

Step 5 Specify the CE interface and its protocol encapsulation from the drop-down lists, then click **Next**.

a. If you specified serial interfaces for the PE and CE and chose Frame Relay as the encapsulation, specify the encapsulation information for the PE and CE, and Data-Link Connection Identifier (DLCI) numbers for the PE-CE link.

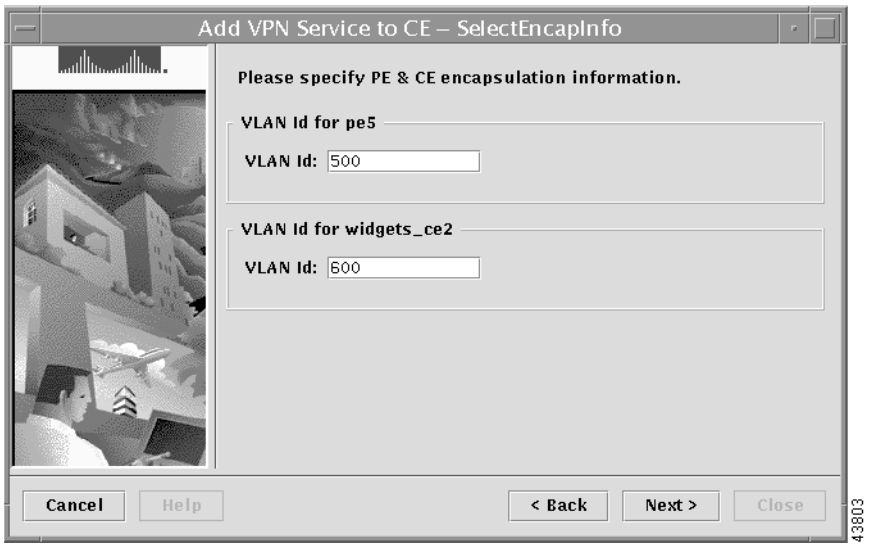
   The dialog box shown in Figure 4-16 is displayed only for serial interfaces and Frame Relay encapsulation.

Figure 4-16 Protocol Encapsulation Information



If you specified LAN interfaces, the wizard displays the dialog box shown in Figure 4-17.

Figure 4-17 Specifying VLAN IDs for the PE and CE



Step 6 Enter the VLAN IDs for the indicated PE and CE, then click **Next**.

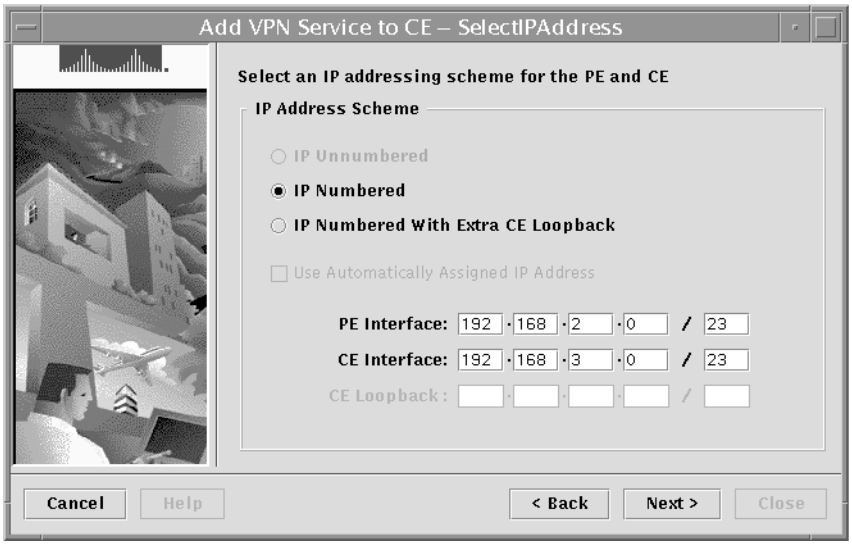
The valid values are any integer from 1 to 1000.

Choosing an IP Addressing Scheme

The next dialog box in the Add VPN Service to the CE wizard (see Figure 4-18) provides a way to define the IP addressing scheme that is appropriate for this PE-CE link.

A point-to-point link between two routers can be either a *numbered* IP address or an *unnumbered* IP address. The service provider must determine whether to use numbered or unnumbered IP addresses for the PE-CE link. Defining the link to use unnumbered addresses can save precious IP addresses because many interfaces can borrow the same IP address.

Figure 4-18 IP Addressing Scheme Dialog Box



Step 1 Choose an IP addressing scheme for the PE and CE.

You can choose among four options:

- IP unnumbered

  IP addresses are drawn from the loopback IP address pool. An unnumbered IP address means that each interface "borrows" its address from another interface on the router (usually the loopback interface). Unnumbered addresses can only be used on point-to-point WAN links (such as Serial, Frame, and ATM), not on LAN links (such as Ethernet). If using IP unnumbered, then both the PE and CE must use the same IP unnumbered addressing scheme. When you choose **IP unnumbered**, VPN Solutions Center creates a static route for the PE-CE link.

  When you choose **IP unnumbered**, VPN Solutions Center software automatically creates a loopback interface (unless a loopback interface already exists with the correct attributes). For related information, see the next section, "Using an Existing Loopback Interface Number."

  If you select **IP unnumbered** and choose to not use automatically assigned IP addresses, you can enter the IP addresses for the PE interface and CE interface in the fields provided. Entering the IP addresses in these fields forces the MPLS VPN software to use the indicated addresses.

- IP numbered

  If you select **IP numbered** and choose to not use automatically assigned IP addresses, you can enter the IP addresses for the PE interface and CE interface in the fields provided. Entering the IP addresses in these fields forces the MPLS VPN software to use the indicated addresses.

- IP numbered with extra CE loopback

  Even though a numbered IP address does not require a loopback address, VPN Solutions Center software provides the option to specify **IP numbered with extra CE loopback**. This option places an IP address on a CE router that is not tied to any physical interface.

  If you select **IP numbered with extra CE loopback**, you can enter the addresses for the PE and CE interfaces, plus the CE loopback address.

- Use Automatically Assigned IP Address

  If you choose **IP unnumbered** and also check the **Use Automatically Assigned IP Address** check box, VPN Solutions Center picks two IP addresses from a /32 subnet point-to-point IP address pool.

  If you choose **IP numbered** and also check the **Use Automatically Assigned IP Address** check box, VPN Solutions Center picks IP addresses from a /30 subnet point-to-point IP address pool.

Step 2 When finished, click **Next**. The Specify VRF Parameters dialog box appears (see Figure 4-19).

Using an Existing Loopback Interface Number

On each PE, there is one loopback interface number per VRF for interfaces using IP unnumbered addresses. By default, VPN Solutions Center software assigns a loopback number associated with a particular loopback address.

However, if a service provider wants VPN Solutions Center to use an existing loopback interface number (for example, Loopback0), the service provider must modify the loopback interface description line in the configuration files for the pertinent routers (PE or CE).

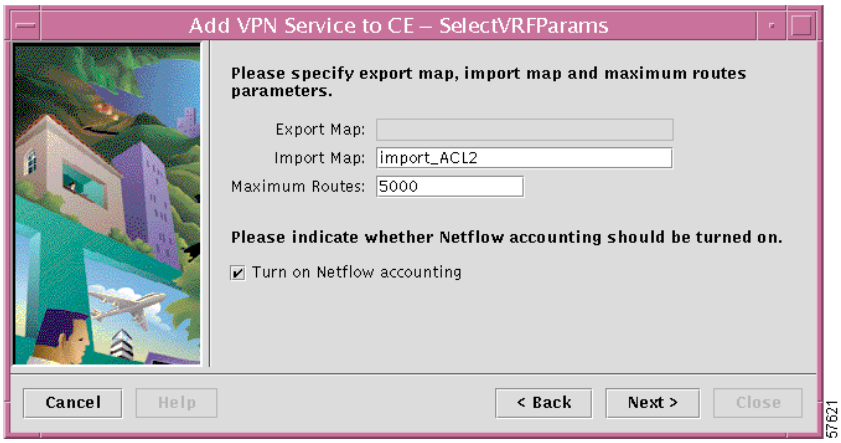
To use the existing loopback interface number, you must modify the loopback interface description line so that it includes the keyword **VPN-SC**, as shown in this example of a router configuration file:

```
interface Loopback0
description Provisioned by VPN-SC
ip address 209.165.202.129 255.255.255.224
```

Specifying VRF Parameters

The Specify VRF Parameters dialog box lets you set values for import and export maps, maximum routes into the VRF table, and enable NetFlow accounting.

Figure 4-19 Specify VRF Parameters Dialog Box



Step 1 If necessary, enter the name of the export map in the *Export Map* field.

The *Export Map* field is the name of an existing export route map on the PE.

Note The Cisco IOS supports only one export route map per VRF (therefore, there can be only one export route map per VPN).

When you use the VPN Solutions Center software to define a management VPN (see the "Defining CERC Membership and Joining the Management VPN" section on page 4-9), the software automatically generates an export route map for the management VPN. Because the Cisco IOS supports only one export route map per VRF and that route map is reserved for the management VPN, the *Export Map* field is not available if the VRF is part of the management VPN (as shown in Figure 4-19).

An export route map does not apply a filter; it can be used to override the default set of route targets associated with a route.

For information on the **route-map** command, refer to the Cisco IOS documentation on IP routing protocol-independent commands.

Step 2 Enter the name of the import map in the *Import Map* field.

The *Import Map* field is the name of an existing import route map on the PE.

Note The Cisco IOS supports only one import route map per VRF (therefore, there can be only one import route map per VPN).

An import route map does apply a filter. Therefore, if you want to exclude a particular route from the VRF on this PE, you can either set an export route map on the sending router to make sure it does not have any route targets that can be imported into the current VRF, or create an import route map on this PE to exclude the route.

For command reference details on the **import map** command, see the "import map" section on page C-6.

Step 3 In the *Maximum Routes* field, specify the maximum number of routes that can be imported into the VRF on this PE.

Step 4 To enable NetFlow accounting, check the **Turn on NetFlow accounting** checkbox.

For more information, see the "NetFlow Collector and VPN Solutions Center Software" section on page 1-29 and the "MPLS VPN NetFlow Accounting" section on page 5-2.

Step 5 When you have completed the fields as necessary in the Specify VRF Parameters dialog box, click **Next**.

Overriding the Default VRF Name and Route Distinguisher Values

When you enable the VRF-RD Override property in the *csm.properties* file, the Select VRF Parameters dialog box presents options that allow you to override the default VRF name and Route Distinguisher (RD) values.

Caution Changing the default values for the VRF name and the Route Distinguisher value can alter or disable other service requests if not done correctly. Please make these changes with caution and only when absolutely necessary.

To override the default VRF name or the default RD values, follow these steps.

Step 1 On the VPN Solutions Center workstation, log in as **root** (**su**).

Step 2 Go to the */opt/vpnadm/vpn/etc* directory.

Step 3 Open the *csm.properties* file with a text editor.

Step 4 Find the following section in the csm.properties file:

```
# Override VRF names and RD values.
# WARNING: This is an advanced feature. Overriding VRF names and RD values
# can potentially modify the intent of other service requests.

netsys.srvc.VRFRDOverride.unix=false
```

Step 5 Change the *false* value to *true*, then save your changes and exit the file.

Step 6 In the VPN Console, proceed through the Add Service to CE wizard as described in the previous sections.

When the Select VRF Parameters dialog box appears, it now displays fields for the VRF name and the RD value (see Figure 4-20).

Figure 4-20 VRF Name and RD Override Options

Step 7 To override the default VRF name, enter the new VRF name in the *VRF Name* field.

The maximum number of characters for the VRF name is 32.

Step 8 To override the default Route Distinguisher value, enter the new RD value in the *RD Value* field.

Step 9 When finished entering the necessary information, click **Next**. The Class of Service Profile dialog box appears.

Selecting a Class of Service Profile for the PE-CE Link

Step 1 If desired, select a Class of Service (CoS) profile to assign to the PE-CE link.

You can create a Class of Service (CoS) profile when you define the Provider Administrative Domain. For information on creating a CoS Profile, see the "Defining a Class of Service Profile" section on page 2-67. For a discussion on the Class of Service feature, see the "Quality of Service and Class of Service" section on page 1-25.

Class of Service profiles are applied to the Provider Edge Router (PE), but the CoS definition is enforced across the PE-CE link on both the PE and CE.

Step 2 Click **Next**.

The next dialog box lets you integrate a VPN Solutions Center template with the current service request definition.

Integrating VPN Solutions Center Templates with a Service Request

VPN Solutions Center provides a way to integrate a template with VPN Solutions Center configlets. For information on creating and employing VPN Solutions Center templates, see Chapter 8, "Provisioning with the VPN Solutions Center Template Manager."

Tips Before you can integrate templates with service requests as described in this section, you must edit the *csm.properties* file and change the following property that is by default set to false to **true**:

```
netsys.vpn.serviceRequest.showTemplates=false
```

For a given customer edge router, you specify the following:

- Template name
- Template data file name
- Whether the Template configuration file should be appended or prepended to the VPN Solutions Center configlet
- Whether the Template configuration file is active or inactive for downloading to the edge device

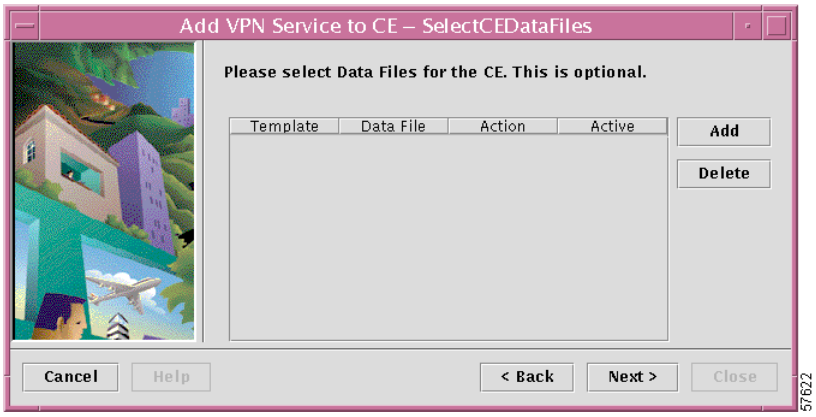
The template data files are tightly linked with its corresponding template. You can use a data file and its associated template to create a template configuration file. The template configuration file is merged with (either appended to or prepended to) the VPN Solutions Center configlet. VPN Solutions Center downloads the combined VPN Solutions Center configlet and template configuration file to the edge device router.

- You can download a template configuration file to a router. For details, see the "Provisioning a Template Configuration File Directly to a Router" section on page 8-23.
- You can apply the same template to multiple edge routers, assigning the appropriate template data file for each device. Each template data file includes the specific data for a particular device (for example, the management IP address or host name of each device).

Specifying a Template for the Customer Edge Router

Figure 4-21 shows the initial template integration dialog box. You first specify which template data file you want associated with the CE in the current link.

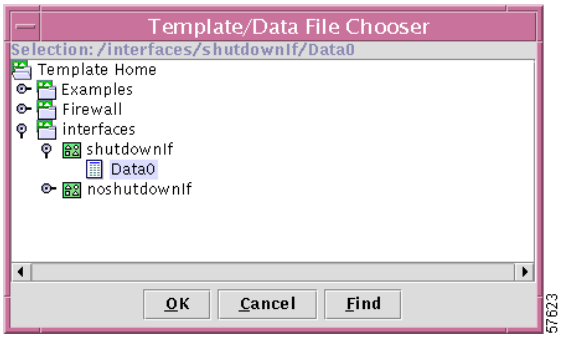
Figure 4-21 Initial Dialog Box for Integrating a Template



Step 1 In the Select CE Data Files dialog box, click **Add**.

The Template/Data File Chooser dialog box appears (see Figure 4-22).

Figure 4-22 The Template/Data File Chooser Dialog Box



Step 2 Expand the Template Home hierarchy until you can see the pertinent template name and its data files.

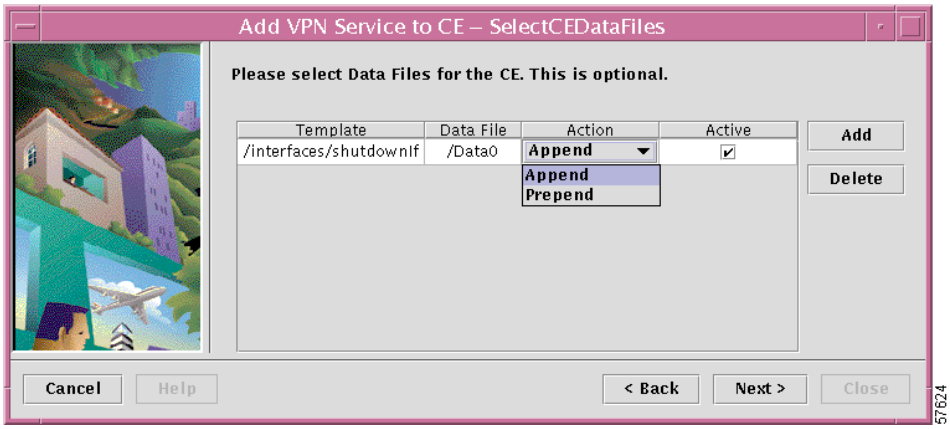
The template data files are tightly associated with its corresponding template. You can use a data file and its associated template to create a template configuration file. The template configuration file is merged with (either appended to or prepended to) the VPN Solutions Center configlet. VPN Solutions Center downloads the combined configlet to the customer edge router.

Step 3 Select the data file of interest, then click **OK**.

You return to the Select CE Data Files dialog box (see Figure 4-23).

Determining the Placement and Active Status of the CE Template Data File

Figure 4-23 CE Data Files Dialog Box After Selecting a Template Data File



The **Action** column in the dialog box lets you specify where the template configuration file is placed in the VPN Solutions Center configlet—either prepended or appended.

The **Active** column lets you determine whether you want the template configuration file to be merged with the VPN Solutions Center configlet and downloaded to the target router.

Step 4 To specify the placement of the template configuration file, click the *Action* field for the appropriate template, then choose **Append** or **Prepend**.

- If you choose **Append**, the template configuration file is appended to (that is, placed at the end of) the VPN Solutions Center configlet prior to being downloaded to the target customer edge router.
- If you choose **Prepend**, the template configuration file is prepended to (that is, placed at the beginning of) the VPN Solutions Center configlet prior to being downloaded to the target customer edge router.

Step 5 Specify the Active status of the template configuration file.

- If you set the Active checkbox as checked, the template configuration file is merged with the VPN Solutions Center configlet and downloaded to the target router.
- If you uncheck the Active checkbox, the template configuration file is not merged at this time with the VPN Solutions Center configlet.

Step 6 To designate additional templates for the selected service request, click **Add**, then repeat Step 1 through Step 5 as described in this procedure.

Step 7 When the CE templates fields are set to your satisfaction, click **Next**.

Specifying a Template for the Provider Edge Router

The Select PE Data Files dialog box appears. You can now specify a template to be integrated into the PE's configuration file.

Step 1 In the Select PE Data Files dialog box, click **Add**.

The Template/Data File Chooser dialog box appears.

Step 2 Expand the Template Home hierarchy until you can see the pertinent template name and its data files.

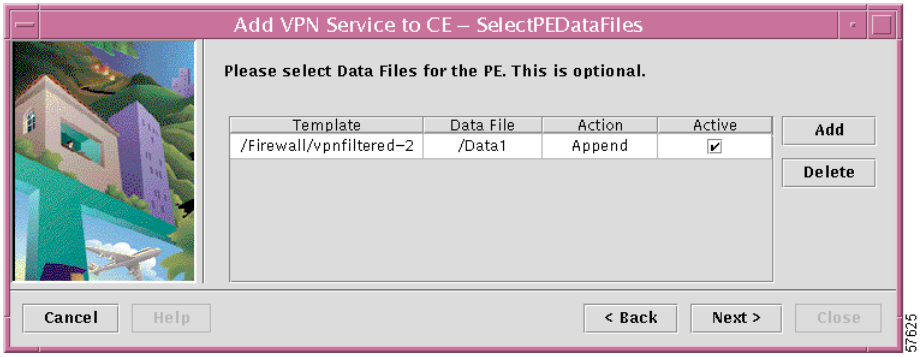
The template data files are tightly associated with its corresponding template. You can use a data file and its associated template to create a template configuration file. The template configuration file is merged with (either appended to or prepended to) the VPN Solutions Center configlet. VPN Solutions Center downloads the combined configlet to the provider edge router.

Step 3 From the Template/Data File Chooser dialog box, select the data file of interest, then click **OK**.

You return to the Select PE Data Files dialog box.

Determining the Placement and Active Status of the PE Template Data File

Figure 4-24 PE Data Files Dialog Box After Selecting a Template Data File



The **Action** column in the dialog box lets you specify where the template configuration file is placed in the VPN Solutions Center configlet—either prepended or appended.

The **Active** column lets you determine whether you want the template configuration file to be merged with the VPN Solutions Center configlet and downloaded to the target router.

Step 4 To specify the placement of the template configuration file, click the *Action* field for the appropriate template, then choose **Append** or **Prepend**.

- If you choose **Append**, the template configuration file is appended to (that is, placed at the end of) the VPN Solutions Center configlet prior to being downloaded to the target provider edge router.
- If you choose **Prepend**, the template configuration file is prepended to (that is, placed at the beginning of) the VPN Solutions Center configlet prior to being downloaded to the target provider edge router.

Step 5 Specify the Active status of the template configuration file.

- If you set the Active checkbox as checked, the template configuration file is merged with the VPN Solutions Center configlet and downloaded to the target provider edge router.
- If you uncheck the Active checkbox, the template configuration file is not merged at this time with the VPN Solutions Center configlet.

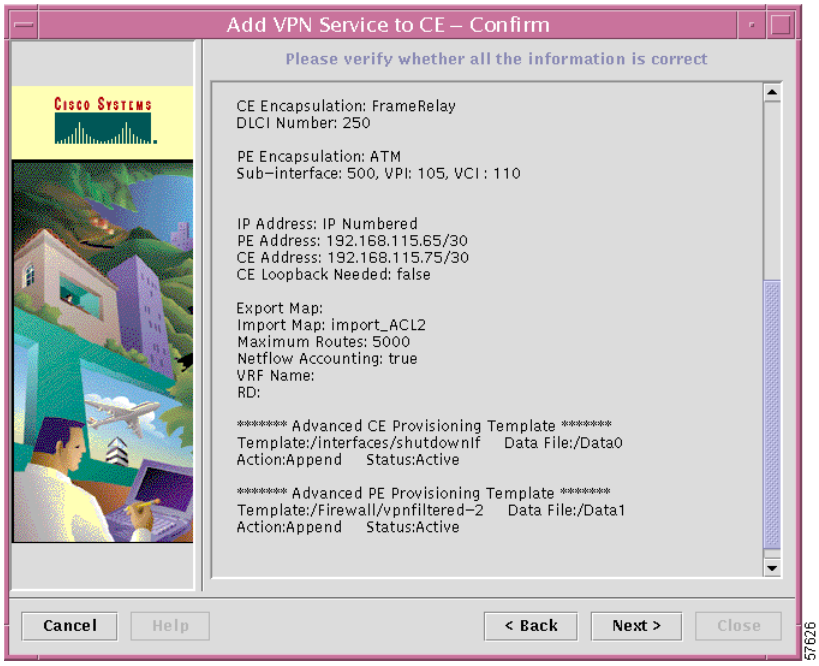
Step 6 To designate additional templates for the selected service request, click **Add**, then repeat Step 1 through Step 5 as described in this procedure.

Step 7 When the PE templates fields are set to your satisfaction, click **Next**.

Confirming the VPN Service Settings

VPN Solutions Center displays a summary of all the service settings defined for this VPN, including the information on template provisioning for the CE and PE (see Figure 4-25).

Figure 4-25 Confirm VPN Service Information Window



Step 1 Verify that the service request information is correct.

Step 2 If the information is not what you intended, click **Back** until you reach the provisioning dialog boxes in question, and edit as necessary.

Step 3 When satisfied with the settings, click **Next**.

The wizard displays the following message:

Your request to "Add VPN Service to CE" has been submitted with ID number *n*. This service request can be deployed by using the "Deploy Service Requests" wizard or by using the "Deploy VPN Service" item under the "Provisioning" option of a VPN service request report.

Step 4 Press **Close**.

You have now queued a service request. It is entered into the VPN Solutions Center Repository and placed in the initial "Requested" state.

Deploying a VPN Service

When you have queued a service request, you can then deploy it using the following method. This method automatically generates an Audit New Service Request type of audit. This audit passes the service request into an operational state.

Step 1 From the VPN Console, choose **Provisioning > Deploy Service Requests**.

The Deploy Service Requests wizard begins. The introductory window provides the following information:

This wizard sets up a scheduled task that deploys service requests to the appropriate routers. This involves computing the configlets for each service request, downloading the configlets to the routers, and running audit reports to determine whether the service was successfully deployed.

Click **Next**.

Step 2 Choose to deploy all or selected service requests, then click **Next**.

- Deploy all new service requests

  For all service requests that are in the Requested state, this option initiates the process of uploading the configuration files from the PEs and managed CEs in the VPN, generates configlets, and downloads the configlets to the PEs and managed CEs.

- Deploy selected service requests

  This option deploys the selected service requests regardless of which state they are in.

  If you choose this option, the dialog box shown in Figure 4-26 appears.

Figure 4-26 Selecting a Specific Service Request for Deployment

Step 3 Choose the service request you wish to deploy, then click **Next**.

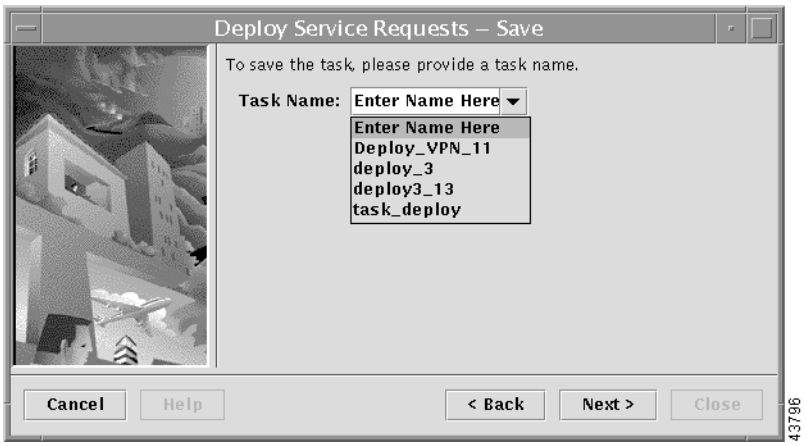
The Select Audit Options dialog box appears. It presents two options:

- **Generate audit reports**
- **Do not generate audit reports**

Running audit reports is the only way that service requests can progress from the Requested state to an operational state, such as Deployed. You have the option to not generate audit reports, but this option is not recommended.

Step 4 From the Select Audit Options dialog box, choose to generate audit reports, then click **Next**. The Save Task dialog box appears.

Figure 4-27 The Save Task Dialog Box



To help you enter a unique task name, the Save Task dialog box provides a list of up to 30 existing task names for the appropriate task type.

Step 5 Enter a unique task name, then click **Next**.

The next screen asks if you want to create a schedule for the task **Now**, in the **Future**, or **No**.

- If you choose **Now**, the service will be deployed immediately.
- If you choose **No**, the Task Manager saves the task, but the service is not scheduled for deployment.
- If you choose **Future**, the Schedule dialog box appears.

Step 6 Complete the fields in the Schedule dialog box to schedule the service request as needed.

a. From the *Frequency* list, choose the desired frequency: **Once**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.

b. Set the *Start Time*: **Now** or **Later**.

c. If you choose **Later**, specify the date and time to start and end the service.

d. If you choose anything other than **Once**, specify how often the service should run from the **Every** drop-down list.

Step 7 When you have scheduled the service request to your satisfaction, click **Add**.

The service request is added to the Schedule List, displayed in the upper area of the dialog box.

Step 8 Click **Next** twice, then click **Close**.

Generating a Service Request Audit

When you initiate VPN Solutions Center service request audit, the audit tests each link in the VPN. The service request is promoted to the Deployed state only when all the links have passed the audit.

When a service request moves beyond the control of the Provisioning system, the Auditor for VPN Solutions Center takes control. The Auditor is a mechanism that monitors and reports the current state of a VPN service request over its lifetime. The lifetime of a VPN service request spans from the Requested state to the Closed state (see the "Service Request Summary" section on page 4-1). The Auditor also provides the reasons why the service request is in its current state. The Auditor saves the state transition (if any) into the VPN Inventory Repository.

To audit the service requests for an MPLS VPN, follow these steps:

Step 1 From the VPN Console hierarchy pane, expand the VPN Console hierarchy to display the **VPN Customers** folder.

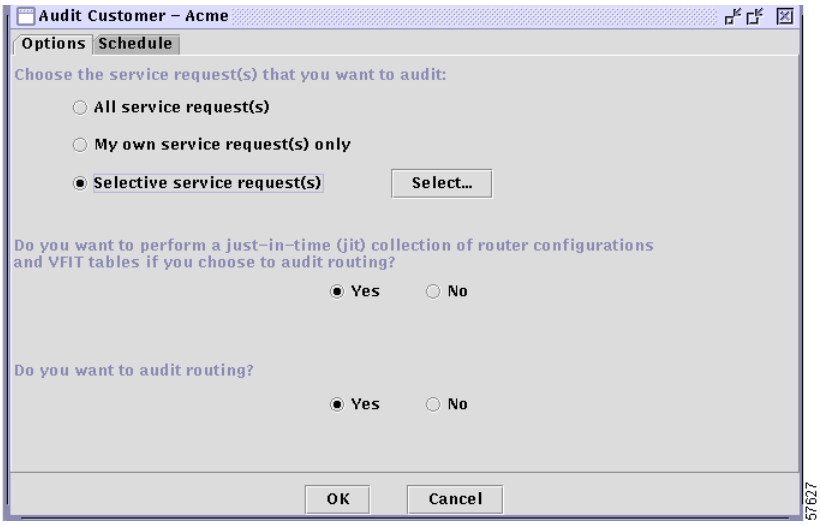
Step 2 Expand the VPN Customers folder to see the list of VPNs.

Step 3 Select the name of the VPN you want to audit, then **right-click**.

Step 4 From the menu, choose **Audit Service Requests**.

The dialog box shown in Figure 4-28 appears.

Figure 4-28 Choosing Which Service Requests to Audit



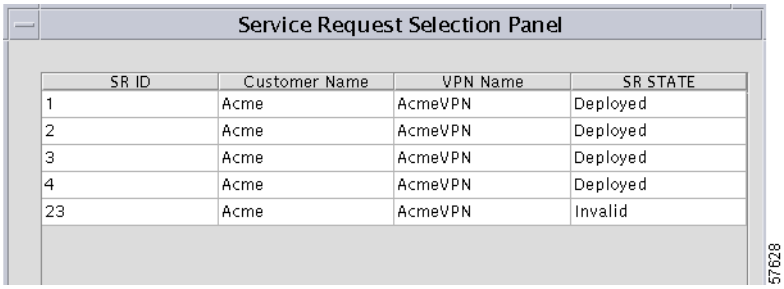
Step 5 Choose which service requests you want to audit:

- All service requests for the selected VPN
- Your own service requests only
- Selected service requests

Step 6 If you want to audit only selected service requests, select the **Selective service requests** option, then click **Select**.

A table showing the service requests from which you can select is displayed (see Figure 4-29).

Figure 4-29 List of Service Requests to Choose From



a. Select one or more service requests from the list.

b. Click **OK**.

You return to the Audit Options dialog box shown in Figure 4-28.

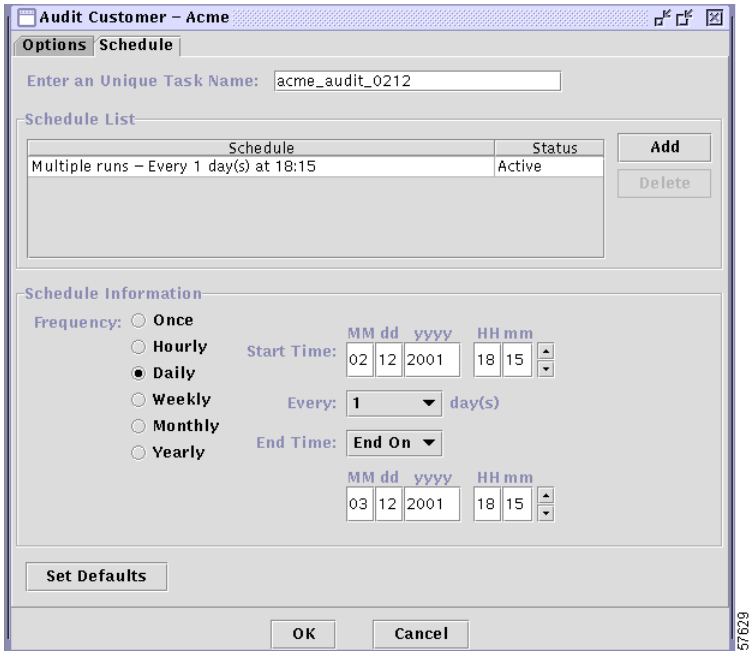
Step 7 If you want to collect the latest router configuration files from the routers effected by the selected service request before VPN Solutions Center runs the audit, accept the **Yes** option.

If you do not want to collect the latest router configuration files before the audit begins, click **No**.

Step 8 When the audit options are set to your satisfaction, click the **Schedule** tab.

The Audit Schedule dialog box appears (see Figure 4-30).

Figure 4-30 Scheduling the Audit



Step 9 Complete the fields in the dialog box to schedule the audit as needed.

a. From the *Frequency* list, choose the desired frequency: **Once**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.

b. Set the *Start Time*: **Now** or **Later**.

c. If you choose **Later**, specify the date and time to start and end the audit.

d. If you choose anything other than **Once**, specify how often the audit should run from the **Every** drop-down list.

Step 10 When you have scheduled the audit to your satisfaction, click **Add**.

The audit is added to the Schedule List, displayed in the upper area of the dialog box (as shown in Figure 4-30).

Step 11 Click **OK**.

You return to the VPN Console.

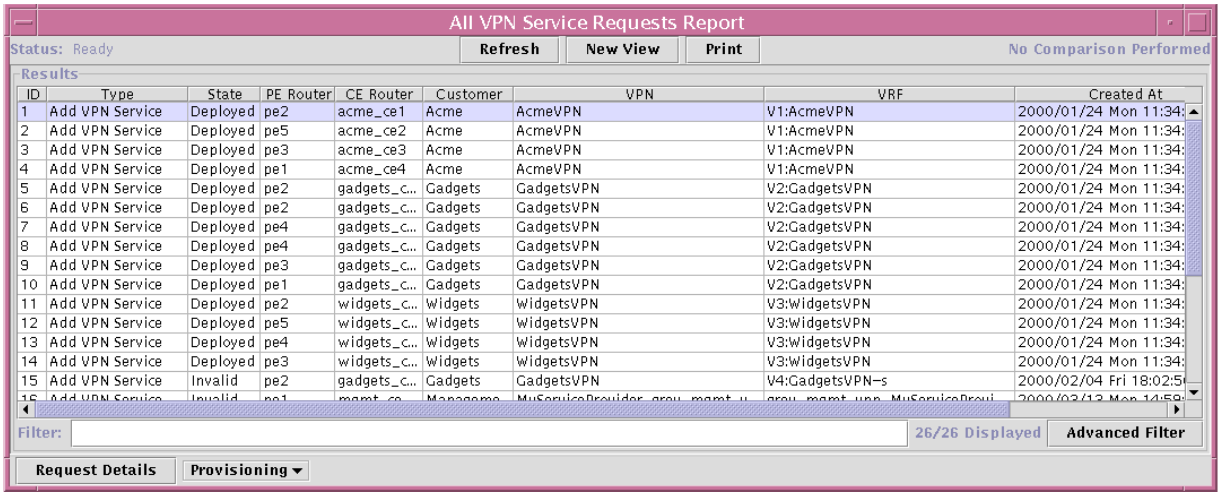
Viewing Audit Reports

Before you view audit reports, you must first generate an audit as described in the previous section. To view audit reports, follow these steps:

Step 1 From the VPN Console menu, choose **Provisioning > List All Service Requests**.

The All VPN Service Requests Report appears (see Figure 4-31).

Figure 4-31 All VPN Service Requests Report



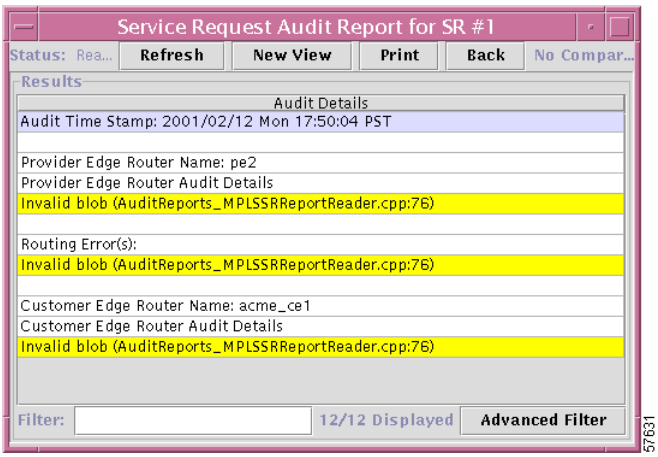
Step 2 Click **Request Details**.

The Service Request Details Report appears (see Figure 4-34 on page 4-36).

Step 3 From the Service Request Details Report, click **Audit Detail**.

The Service Request Audit Report appears (see Figure 4-32).

Figure 4-32 Audit Details Report



Those items that the audit discovered problems with are highlighted in yellow.

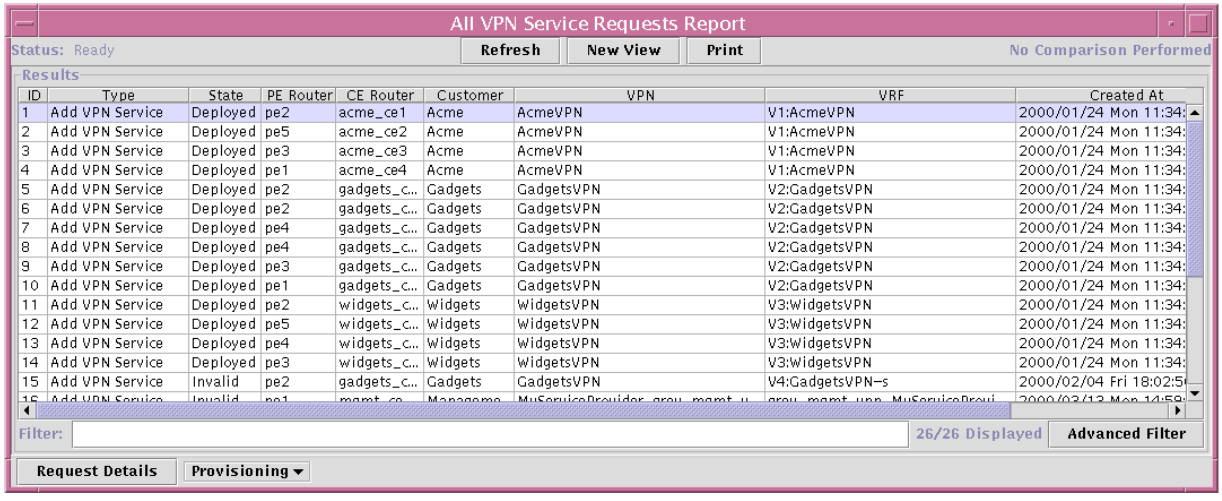
Checking Service Request Deployment Details

Once you have created and queued a service request, you can discover the details about its deployment. You can view the configlet generated for the service request. If the service request failed, you can discover why it failed by using the Service Request Audit report.

Step 1 To check service request details, choose **Provisioning>List All Service Requests**.

The All VPN Service Requests Report appears (see Figure 4-33).

Figure 4-33 All VPN Service Requests Report



This report provides the following information:

- Service request ID number

- Type of request
- Current state

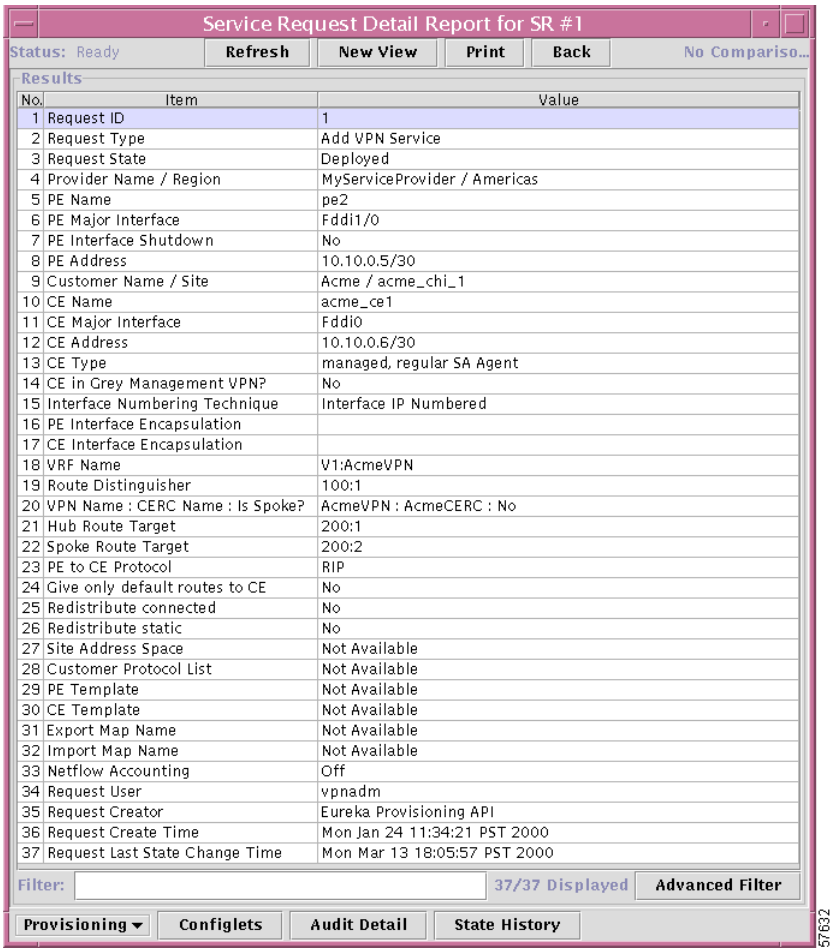
  If the current state is either Deployed or Functional, the service request is deployed.
- Names of the PE and CE router the service is for
- Customer name
- VPN name
- VRF name
- Time and date the service request was created
- Time and date when the service was last changed

Step 2 Select the service request you want detailed information on.

Step 3 Click **Request Details**.

The Service Request Details Report appears (see Figure 4-34).

Figure 4-34 Service Request Details Report

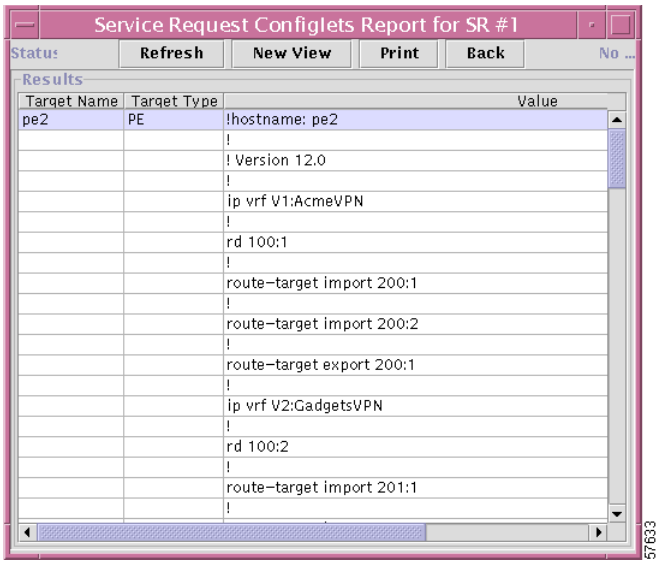


No.	Item	Value
1	Request ID	1
2	Request Type	Add VPN Service
3	Request State	Deployed
4	Provider Name / Region	MyServiceProvider / Americas
5	PE Name	pe2
6	PE Major Interface	Fddi1/0
7	PE Interface Shutdown	No
8	PE Address	10.10.0.5/30
9	Customer Name / Site	Acme / acme_chi_1
10	CE Name	acme_ce1
11	CE Major Interface	Fddi0
12	CE Address	10.10.0.6/30
13	CE Type	managed, regular SA Agent
14	CE in Grey Management VPN?	No
15	Interface Numbering Technique	Interface IP Numbered
16	PE Interface Encapsulation	
17	CE Interface Encapsulation	
18	VRF Name	V1:AcmeVPN
19	Route Distinguisher	100:1
20	VPN Name : CERC Name : Is Spoke?	AcmeVPN : AcmeCERC : No
21	Hub Route Target	200:1
22	Spoke Route Target	200:2
23	PE to CE Protocol	RIP
24	Give only default routes to CE	No
25	Redistribute connected	No
26	Redistribute static	No
27	Site Address Space	Not Available
28	Customer Protocol List	Not Available
29	PE Template	Not Available
30	CE Template	Not Available
31	Export Map Name	Not Available
32	Import Map Name	Not Available
33	Netflow Accounting	Off
34	Request User	vpnadm
35	Request Creator	Eureka Provisioning API
36	Request Create Time	Mon Jan 24 11:34:21 PST 2000
37	Request Last State Change Time	Mon Mar 13 18:05:57 PST 2000

Step 4 To view the configlets generated for the selected service request, click **Configlets**.

The report shown in Figure 4-35 appears.

Figure 4-35 Service Request Configlets Report



To return to the Service Request Detail Report, click **Back**.

Modifying an Existing Service

A service request is an instance of service contract between a CE and a PE. You can modify this service by creating a new service request. When you do so, VPN Solutions Center creates a new service request with a new ID. (The service request ID is displayed in the first column in the All VPN Service Requests Report as shown in Figure 4-33). The new service request subsumes the earlier one and becomes the current service request.

When you modify a service request, you can modify the settings for the PE-CE link, except for the CE and the PE themselves. This procedure takes through the same wizard as described in the "Adding a Service for a PE-CE Link" section on page 4-7, except that the settings are based on the service request's current values.

To modify a service, follow these steps:

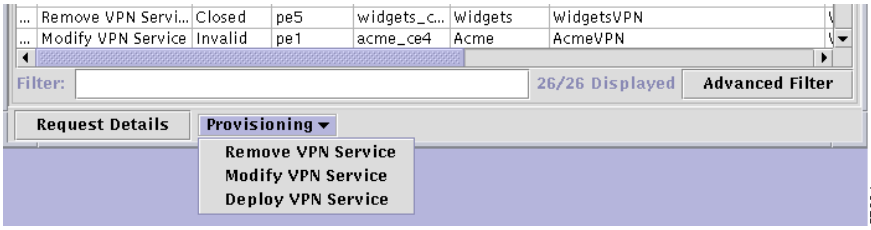
Step 1 Choose **Provisioning>List all Service Requests**.

The All VPN Service Requests Report appears.

Step 2 From the list of service requests, select the service request you need to modify.

Step 3 From the All VPN Service Requests Report, click the **Provisioning** button (see Figure 4-36).

Figure 4-36 Service Request Provisioning Menu



Step 4 From the drop-down menu, select **Modify VPN Service**.

The Modify Existing VPN Service wizard appears. The first window provides a message like this:

This wizard submits a new service request to modify the VPN service between the PE "PE_name" and the CE "*CE_name*" (specified in service request *ID_number*). The new service request replaces service request *ID_number*.

Click **Next**.

Step 5 Choose the routing protocol for the PE-CE link.

The routing protocol you choose must run on both the PE and the CE. For details on each of the options for the routing protocols, see the "Choosing the Routing Protocol for the Link" section on page 4-10.

Step 6 If necessary, specify the routing protocols that must be redistributed from the CE, then click **Next**.

For details, see the "Specifying Redistributed Protocols on the Link" section on page 4-17.

Step 7 Define the interfaces for the PE-CE link.

For details, see the "Defining the Interfaces on the PE-CE Link" section on page 4-18.

Step 8 Choose an IP addressing scheme for the PE and CE.

For details, see the "Choosing an IP Addressing Scheme" section on page 4-20.

When finished, click **Next**.

Step 9 If desired, select a Class of Service (CoS) profile to assign to the PE-CE link.

Class of Service profiles are applied to the Provider Edge Router (PE), but the CoS definition is enforced across the PE-CE link on both the PE and CE.

create a Class of Service (CoS) profile when you define the Provider Administrative Domain. For information on creating a CoS Profile, see the "Defining a Class of Service Profile" section on page 2-67. For a discussion on the Class of Service feature, see the "Quality of Service and Class of Service" section on page 1-25.

Step 10 If desired, specify a VPN Solutions Center template to be integrated into the CE's configuration file.

For details, see the "Integrating VPN Solutions Center Templates with a Service Request" section on page 4-25.

VPN Solutions Center software displays a summary of all the service settings defined for this VPN.

Step 11 If desired, specify a VPN Solutions Center template to be integrated into the PE's configuration file.

For details, see the "Integrating VPN Solutions Center Templates with a Service Request" section on page 4-25.

Step 12 Verify that the service request information is correct, then click **Next**.

The wizard displays the following message:

Your request to "Modify Existing VPN Service" has been submitted with ID number n. This replaces existing service request. This service request can be deployed by using the "Deploy VPN Service Requests" wizard or by using the "Deploy VPN Service" item under the "Provisioning" option of a VPN service request report.

Step 13 Press **Close**.

You have now queued a service request. It is entered into the product database and is in the state "Requested."

Decommissioning a Service

Decommissioning a service request from VPN Solutions Center is a four-task process:

- *Create a service request to initiate the decommissioning of the selected VPN service.*

  When you decommission a VPN service, VPN Solutions Center replaces the old service request with a new one whose purpose is to remove the pertinent commands from the PE and CE router configuration files.

- *Deploy the remove VPN service request.*

  The new remove VPN service request will be in Requested state, and you should deploy it as you do any other service request.

  Deploying a "Remove VPN Service" request deletes individual commands from the PE and CE configuration files, which were put there by the original provisioning request, and are not in use by any other service or feature in the router configuration.

  To ensure that the service removal is safe requires that not all commands that were provisioned are removed. In cases where VPN Solutions Center cannot know whether a provisioned command is being used for some other purpose, the command is not removed. Examples of router commands not removed for a "Remove VPN Service" request include routing protocols created during service provisioning, such as BGP or RIP. These are not removed from the router's configuration file, although some of their subcommands are removed when they support only the original service request.

- *Audit the remove VPN service request.*

  The auditing process uploads the revised configuration file into VPN Solutions Center and checks to confirm that the appropriate commands have been removed from the file. If the audit is successful, the remove VPN service is moved to the Closed state. Though this step is not required, it is highly recommended.

- *Purge the remove VPN service request.*

  To delete the remove VPN service request from the Repository, you must purge the service request.

To remove a service, follow these steps:

Creating a Remove VPN Service Request

To create a service request to decommission a specified VPN service, follow these steps:

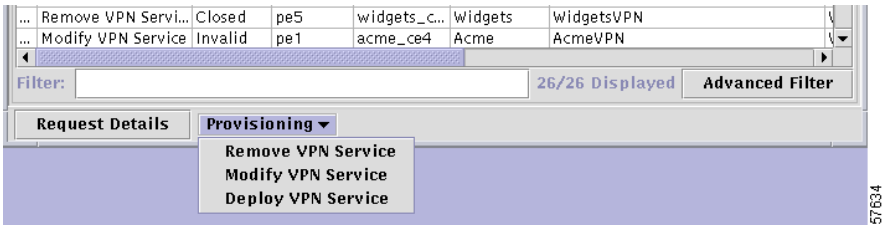
Step 1 From the VPN Console, choose **Provisioning > List All Service Requests**.

The All VPN Service Requests Report appears.

Step 2 From the list, select the service request you wish to remove.

Step 3 From the Service Request Provisioning menu (at the bottom of the window), click **Provisioning** as shown in Figure 4-37.

Figure 4-37 Service Request Provisioning Menu



Step 4 Choose **Remove VPN Service**.

You receive this warning message:

This will submit a new service request to remove the VPN service between the PE and CE. New configlets will be generated with the appropriate "no" commands to remove the VPN service. Service Request n to Add VPN Service will no longer be active. Do you want to continue?

Step 5 Click **Yes** to proceed, or **No** to cancel the Remove operation.

If you click **Yes**, you receive the following message:

A new service request has been submitted to remove the VPN service specified in service request n.

Step 6 Click **OK**.

Deploying the Remove VPN Service Request

To deploy a remove VPN service request, follow these steps:

Step 1 From the VPN Console, choose **Provisioning > List All Service Requests**.

The All VPN Service Requests Report appears.

Step 2 From the list, select the service request you wish to deploy.

Step 3 From the Service Request Provisioning menu (at the bottom of the window), click **Provisioning**.

Step 4 From the drop-down menu, choose **Deploy VPN Service**.

The following message is displayed:

This will deploy the selected VPN service request now. Do you want to continue?

Step 5 Click **Yes**.

The selected service request is Deployed and placed in the Pending state.

Auditing the Remove VPN Service Request

The auditing process uploads the revised configuration file into VPN Solutions Center and checks to confirm that the appropriate commands have been removed from the file. If the audit is successful, VPNSC sets the remove VPN service to the Closed state.

Note Though this step is not required, it is highly recommended. If you choose not to audit the remove VPN service, you can close the service manually as described in the "Closing Service Requests Manually" section on page 4-42.

To audit the remove VPN service, follow these steps:

Step 1 From the VPN Console hierarchy pane, expand the VPN Console hierarchy to display the **VPN Customers** folder.

Step 2 Expand the VPN Customers folder to see the list of VPNs.

Step 3 Select the name of the VPN you want to audit, then **right-click**.

Step 4 From the menu, choose **Audit Service Requests**.

The Audit Customer dialog box appears.

Step 5 From the Audit Customer dialog box, choose the **Selective service requests** option, then click **Select**.

A table showing the service requests from which you can select is displayed.

Step 6 Select the remove VPN service request from the list, then click **OK**.

You return to the Audit Options dialog box.

Step 7 If you want to collect the latest router configuration files from the routers effected by the selected service request before VPN Solutions Center runs the audit, accept the **Yes** option.

If you do not want to collect the latest router configuration files before the audit begins, click **No**.

Step 8 When the audit options are set to your satisfaction, click the **Schedule** tab.

The Audit Schedule dialog box appears.

Step 9 Complete the fields in the dialog box to schedule the audit as needed.

a. From the *Frequency* list, choose the desired frequency: **Once**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.

b. Set the *Start Time*: **Now** or **Later**.

c. If you choose **Later**, specify the date and time to start and end the audit.

d. If you choose anything other than **Once**, specify how often the audit should run from the **Every** drop-down list.

Step 10 When you have scheduled the audit to your satisfaction, click **Add**.

The audit is added to the Schedule List, displayed in the upper area of the dialog box.

Step 11 Click **OK**.

You return to the VPN Console.

Purging a Closed Service from the Repository

The final task in removing a VPN service is to purge the service from the Repository. VPN Solutions Center software does not automatically remove closed service requests from the Repository (in case you need them for your records). But keeping closed service requests can be a waste of disk space, therefore, the VPN Solutions Center software provides a way to purge obsolete request data from the Repository.

To purge closed service requests from the Repository, follow these steps:

Step 1 If you have not already done so, close the service requests you want to remove as described in the previous section.

Step 2 From the VPN Console, choose **Provisioning > Purge Closed Requests from Database**.

You receive the following Delete Confirmation prompt:

All closed service requests will be removed from the database.

Do you want to purge closed requests now?

Step 3 If you wish to proceed with the service request removal operation, click **Yes**.

Closing Service Requests Manually

When you manually close a service request, VPN Solutions Center changes the state of the service to Closed in the Repository. VPN Solutions Center does not make any modifications to the router's configuration file when you close a service request. You cannot remove a service request from the Repository until it is closed.

Enabling Manual Closure of Service Requests

Before you can manually close a service request, you must enable a certain property in the *csm.properties* file. Changing this value in the *csm.properties* file provides a new option in the VPN Console that allows you to remove service requests in any state.

Step 1 If VPN Solutions Center is running, shut it down.

Step 2 On the VPN Solutions Center workstation, log in as the *vpnadm* administrative user.

Step 3 Go to the */opt/vpnadm/vpn/etc* directory.

Step 4 Open the *csm.properties* file with a text editor.

Step 5 Find the following property in the *csm.properties* file:

```
netsys.close.sr.option.unix = Off
```

Step 6 Change the `Off` value to **On** as follows:

```
netsys.close.sr.option.unix = On
```

Step 7 Save your changes and exit from the file.

Step 8 Restart VPN Solutions Center.

Closing a Service Request

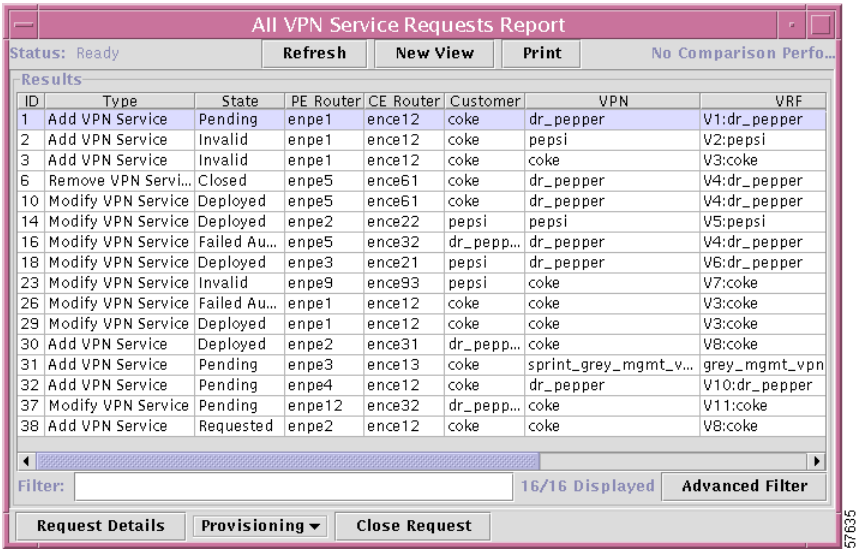
To manually close a service request, follow these steps:

Step 1 From the VPN Console menu bar, choose **Provisioning > List All Service Requests**.

The All VPN Service Requests Report appears (see Figure 4-38).

A new option for closing service requests—**Close Request**—is displayed on the menu bar at the bottom of the All VPN Service Requests Report.

Figure 4-38 Close Service Request Option Enabled



Step 2 Select the service request you want to close.

Step 3 From the menu bar at the bottom of the All VPN Service Requests Report, click **Close Request**.

You receive the following confirmation prompt:

Are you sure you want to close the selected service request(s)?

Step 4 To close the selected service requests, click **Yes**.

To cancel the close operation, click **No**.

VPN Solutions Center changes the state of the selected services to Closed in the Repository.

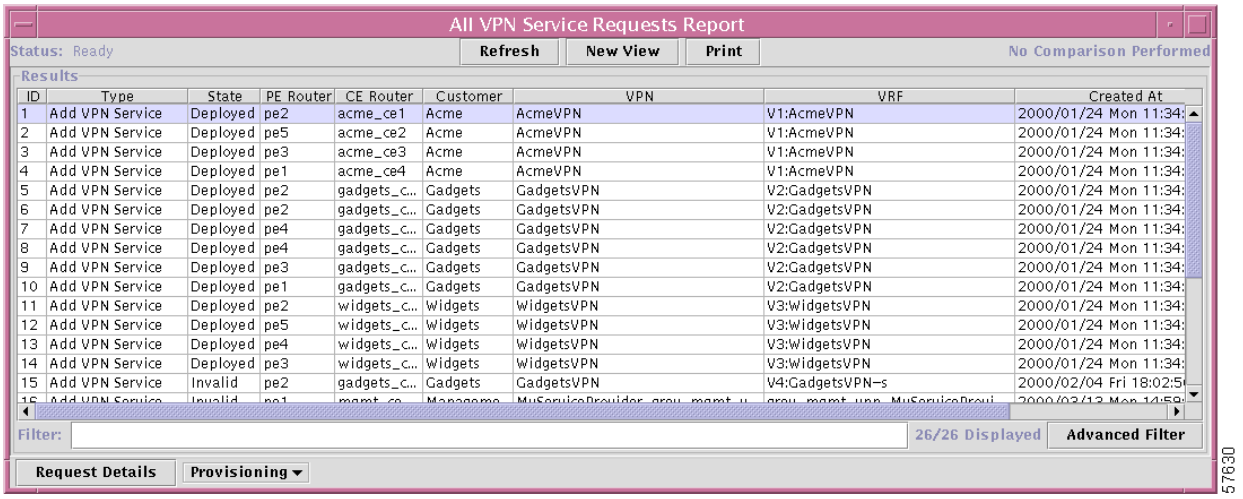
Performing a Customized Service Request Deployment

The procedure to perform a customized service request deployment deploys the service request immediately. This customized deployment does not perform an audit, nor does it allow you to schedule the audit.

Step 1 From the VPN Console, choose **Provisioning>List All Service Requests**.

The All VPN Service Requests Report appears (see Figure 4-39).

Figure 4-39 All VPN Service Requests Report

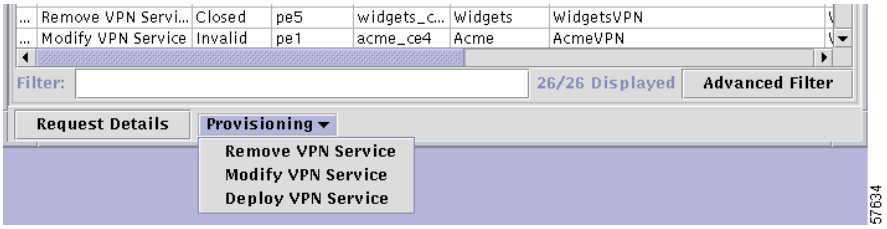


Step 2 Select the service request you want to deploy.

Step 3 From the Provisioning menu at the bottom of the window, click **Provisioning**.

The Service Request Provisioning drop-down menu appears.

Figure 4-40 Service Request Provisioning Menu



Step 4 From the drop-down menu, choose **Deploy VPN Service**.

The following message is displayed:

This will deploy the selected VPN service request now. Do you want to continue?

Step 5 Click **Yes**.

The selected service request is Deployed and placed in the Pending state.

Performing a Customized Audit

VPN Solutions Center software performs a basic audit (Audit New Service Request) by default each time you deploy a service request as described in the "Deploying a VPN Service" section on page 4-30. You need only schedule the audit separately as described in this section if you want to run it more frequently or if you customized audits.

When a service request moves beyond the control of the Provisioning system, the Auditor for VPN Solutions Center takes control. The Auditor is a mechanism that monitors and reports the current state of a VPN service request over its lifetime. The lifetime of a VPN service request spans from the Requested state to the Closed state. The Auditor also provides the reasons why the service request is in its current state. The Auditor saves the state transition (if any) into the VPN Inventory Repository.

After you populate targets (PEs and CEs) and the Repository, prior to any other steps, you must collect router configuration files to audit the services provisioned by MPLS VPN Solution.

Setting Up Routers for Collecting Configuration Files

The basic audit (Audit New Service Requests) does collect the configuration files. You need only set up the routers as described in this section if you are performing a customized audit procedure. This ensures that you have the most current version of the configuration files for the audit procedure.

To set up routers for collecting router configuration files, be sure to implement the following requirements:

- Set the *csm.properties* file for a customized router prompt

  The *csm.properties* file is in the */opt/vpnadm/vpn/etc* directory.
- Set up the Domain Name server

Setting the csm.properties File for Customized Router Prompt

When setting up configuration file collection from routers, be sure that all the routers have the same prompts as in the *csm.properties* file for *netsys.router.loginprompt* and *netsys.router.passwordprompt*. The default values match the default values on Cisco routers. They are as follows:

```
netsys.router.loginprompt = Username:
netsys.router.passwordprompt = Password:
```

If you use nonstandard router prompts in the *csm.properties* file, be sure you set the same values for all the routers from which you collect information.

Setting Up the Domain Name Server

For the collection module of MPLS VPN Solution, enable or disable the Domain Name Server (DNS) on the routers. If DNS is not properly configured on the routers, collections fail due to a time-out.

Note Enabling DNS causes DNS to handle the name resolution. Otherwise, name resolution is handled by the routers.

Enabling DNS

To enable DNS, enter the following commands on the router:

ip domain-lookup

ip name-server `a.b.c.d`

where *a.b.c.d* is a valid Domain Name server.

Disabling DNS

To disable DNS, it is important to enter the following command on all routers:

no ip domain-lookup

Configuring the SNMP Settings on the PEs and CEs

To determine whether SNMP is enabled and set the SNMP community strings, execute the following steps for each PE and CE in the service provider network:

	Command	Description of Task
Step 1	`> telnet routername`	*routername* is the name of the router you are checking.
Step 2	`Router> enable` `Router> enable-password`	Enter Enable mode and enter the enable password.
Step 3	`Router# show snmp`	Check the output to see whether the following command is present: **SNMP agent not enabled**
Step 4	`Router# configure terminal`	Enter global configuration mode. You can abbreviate the command to **config t**.
Step 5	`Router(config)# snmp-server community userstring RO`	Set the community read-only string.
Step 6	`Router(config)# snmp-server community userstring RW`	Set the community read-write string.
Step 7	`Router(config)# Ctrl+Z`	Return to privileged Exec mode.
Step 8	`Router# copy running startup`	Save the configuration changes to NVRAM.

Updating Router Configuration Files

This procedure sets up a scheduled task that allows you to update Cisco router configuration files in two ways:

- Updating configuration information directly from selected routers.
- Updating configuration information by importing from files on the VPN Solutions Center workstation.

You can collect additional information, including router types, Frame Relay/ATM PVC information, and IP unnumbered connectivity information.

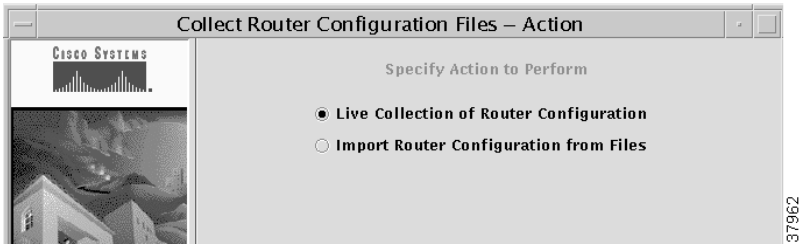
To update router configuration files, follow these steps:

Step 1 From the VPN Console, choose **Monitoring>Collect Router Configuration Files**.

The first panel provides introductory information.

Click **Next**.

Figure 4-41 Specifying Configuration File Collection Method



Step 2 In this dialog box, select one of the following ways of updating configuration file information:

- Live Collection of Router Configuration

  This task performs a Telnet operation to the routers to collect the running configuration of each selected router.

- Importing Router Configuration from Files

  This task imports collected configuration files that exist in a directory on the VPN Solutions Center workstation. All the files in the directory must be configuration files.

Updating Configuration Information by Collecting From Targets

To update router configuration files by collecting the information from existing targets, follow these steps:

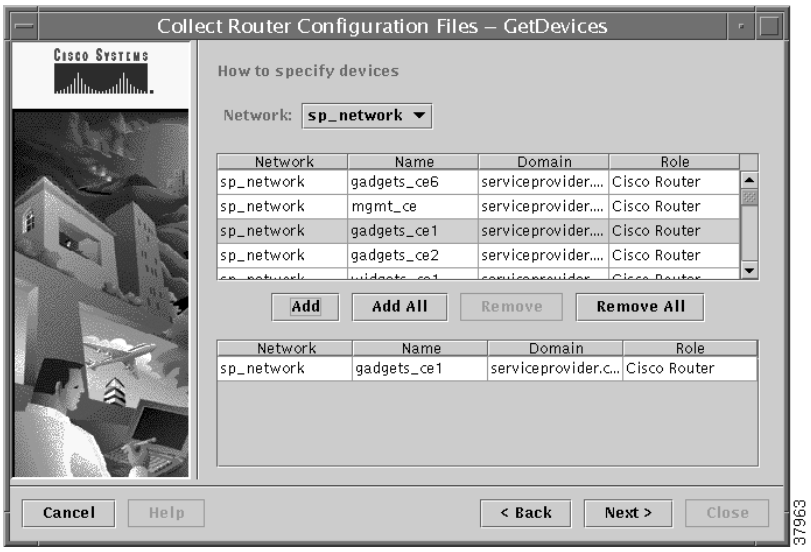
Step 1 Choose **Live Collection of Router Configuration Files**, then click **Next**.

The Get Devices dialog box appears.

Step 2 From the Get Devices dialog box, click the Network drop-down menu to choose a specific network.

As shown in Figure 4-42, all the router names in this network appear in the upper pane. If you want to sort the information, click on the column header for which you want to sort.

Figure 4-42 Updating Router Configuration Files from Selected Targets



a. Select the routers from the upper pane that you want to collect router configuration data from, then click **Add**.

   You can also select all the routers listed by clicking **Add All**.

   Your selections appear in the lower pane.

Note You can remove one or more of the routers selected in the bottom pane by selecting specific routers and clicking **Remove** or **Remove All**.

b. When the lower pane includes all the devices from which router configuration data is to be collected, click **Next**.

Step 3 In the next dialog box, you can choose the **Mask passwords in collected files** option. This allows you to place a group of *x* marks in the router's password field to mask the actual characters that are typed in the field. Click **Next**.

Step 4 In the next dialog box, provide a unique task name, then click **Next**.

The next screen asks if you want to create a schedule for the task **Now**, in the **Future**, or **No**.

- If you choose **Now**, the service will be deployed immediately.
- If you choose **No**, the Task Manager saves the task, but the service is not scheduled for deployment.
- If you choose **Future**, the Schedule dialog box appears.

Step 5 Complete the fields in the Schedule dialog box to schedule the collection task as needed.

a. From the *Frequency* list, choose the desired frequency: **Once**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.

b. Set the *Start Time*: **Now** or **Later**.

c. If you choose **Later**, specify the date and time to start and end the collection task.

d. If you choose anything other than **Once**, specify how often the collection task should run from the **Every** drop-down list.

Step 6 When you have scheduled the collection task to your satisfaction, click **Add**.

The collection task is added to the Schedule List, displayed in the upper area of the dialog box.

Step 7 Click **Next** twice, then click **Close**.

Updating Configuration Information by Importing From Files on the VPNSC Workstation

This task imports the configuration files that exist in a specified directory on the VPN Solutions Center workstation.

Tips If your fully qualified device (target) name includes a domain name, then the configuration filenames must include the domain name as specified here.
The default convention for naming configuration files is:
device_name.domain.com

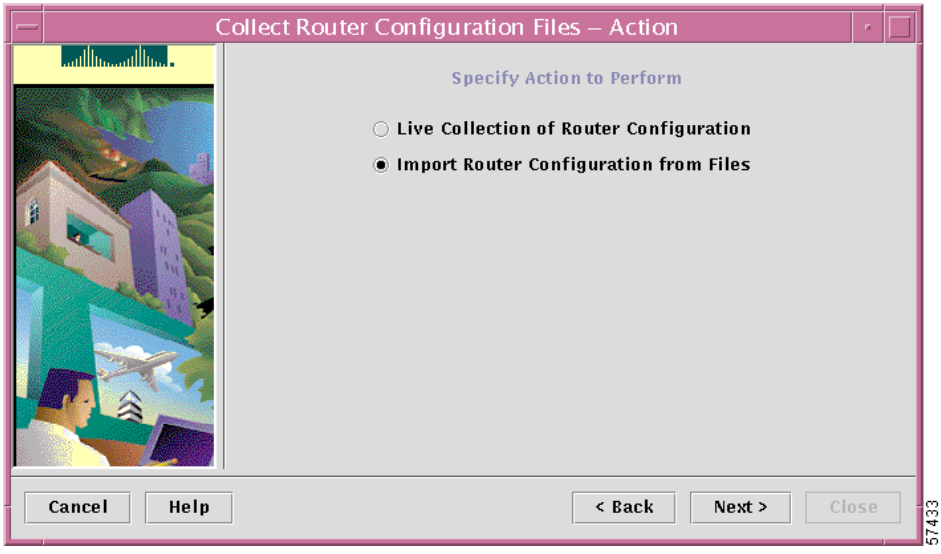
To update router configuration information by importing the configurations from files on the VPN Solutions Center workstation, follow these steps:

Step 1 From the VPN Console, choose **Monitoring>Collect Router Configuration Files**.

The first panel provides introductory information.

Click **Next**. The dialog box shown in Figure 4-43 appears.

Figure 4-43 Specifying Configuration File Update Method

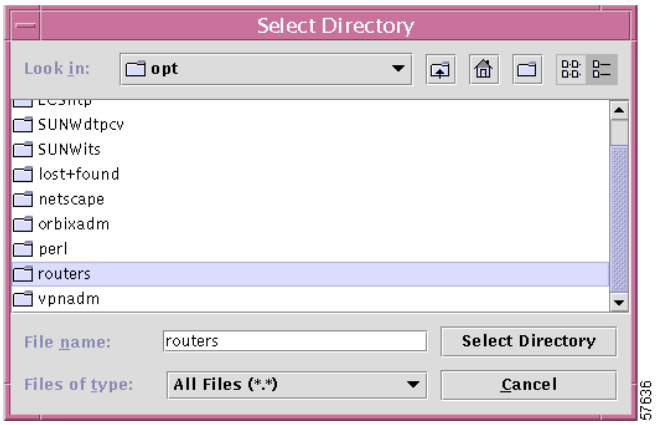


Step 2 In this dialog box, choose **Import Router Configuration from Files**, then click **Next**.

Step 3 From the Get Directory dialog box, click **Browse**.

The Select Directory dialog box appears (see Figure 4-44).

Figure 4-44 Selecting the Directory to Import Configuration Files From



a. Choose the name of the directory that has the configuration files that you want to import.

Note All the files in the directory must be configuration files.

b. Click **Select Directory**.

The selected directory path is now displayed in the Get Directory field.

Step 4 In the Get Network dialog box, select the name of the service provider network, then click **Next**.

Step 5 In the next dialog box, enter a unique task name, then click **Next**.

The next screen asks if you want to create a schedule for the task **Now**, in the **Future**, or **No**.

- If you choose **Now**, the service will be deployed immediately.
- If you choose **No**, the Task Manager saves the task, but the service is not scheduled for deployment.
- If you choose **Future**, the Schedule dialog box appears.

Step 6 Complete the fields in the Schedule dialog box to schedule the service request as needed.

a. From the *Frequency* list, choose the desired frequency: **Once**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.

b. Set the *Start Time*: **Now** or **Later**.

c. If you choose **Later**, specify the date and time to start and end the service.

d. If you choose anything other than **Once**, specify how often the service should run from the **Every** drop-down list.

Step 7 When you have scheduled the service request to your satisfaction, click **Add**.

The service request is added to the Schedule List, displayed in the upper area of the dialog box.

Step 8 Click **Next** twice, then click **Close**.

Running IOS Commands from the VPN Console

You can run Cisco IOS commands on a router's command line by using VPN Solutions Center's Exec Command feature. This feature makes it easy to run commands on multiple routers at once. The Exec Command Console puts you in Enable mode, thus you can run any IOS commands that are executable in Enable mode.

Executing commands in this way does not change the router's configuration file. VPN Solutions Center simply runs the commands you enter and returns the command's response, just as it does when communicating with a router through a console.

To execute an IOS command on a router, follow these steps:

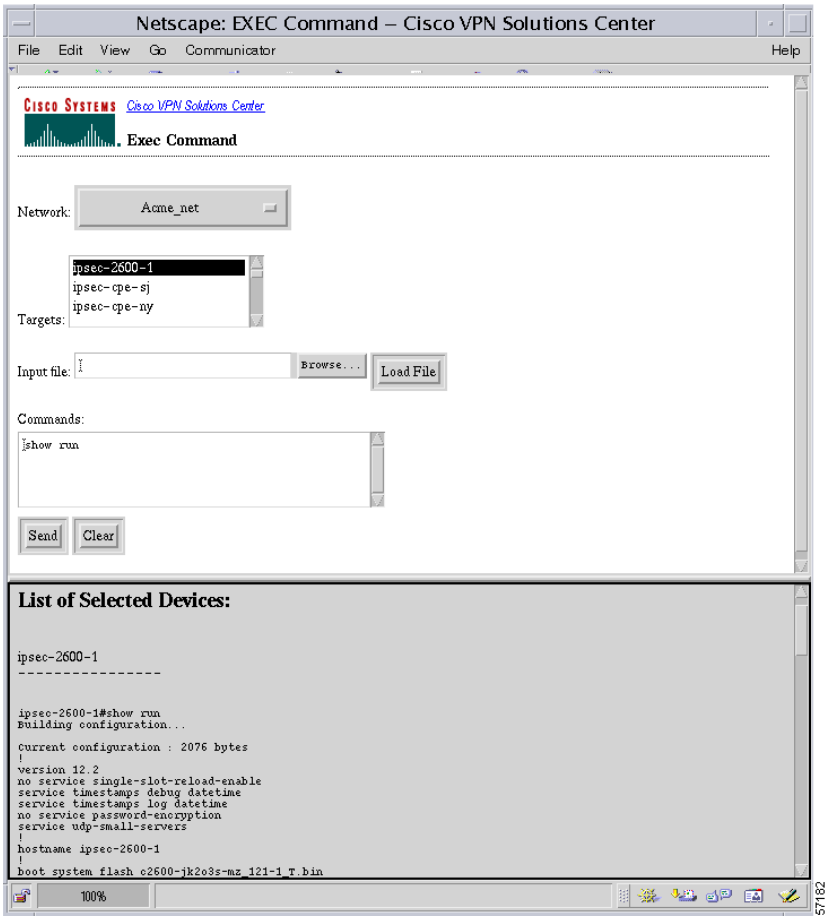
Step 1 From the VPN Console menu bar, choose **Tools > Exec Command**.

The Cisco VPN Solutions Center browser appears. If the browser is not already running, you must log in.

Step 2 In the Netscape Password dialog box, enter the VPN Solutions Center administrative user name and password, then click **OK**.

The VPN Solutions Center Exec Command Console page appears (see Figure 4-45).

Figure 4-45 The Exec Command Console



You can run commands in the Exec Command Console in either of two ways:

- Specifying a command input file that contains a set of valid Cisco IOS commands.

  The command input file must be a text file. There is no practical limit to the number of commands that be included in a command input file.

- Entering commands manually in the Commands pane.

Step 3 From the Network drop-down menu, choose the name of the network that the target router resides in.

The routers in the selected network are displayed in the window below the *Network* field.

Step 4 From the list of routers, select one or more routers on which you want to run the command.

Step 5 To run IOS commands from a command input file:

a. Enter the path and name of the command input file in the *Input file* field.

You can also specify the name and path for the command input file by clicking **Browse** and selecting the file in its directory.

b. Click **Load File**.

c. Click **Send**.

Step 6 To enter commands manually, in the Commands pane, enter the commands you want to run, then click **Send**.

If you need to erase the contents of the Commands pane, click **Clear**. Then reenter the commands as needed.

The lower pane displays the output from the command you entered for each device you selected.

Modifying a Router's Configuration From the VPN Console

VPN Solutions Center provides a mechanism called the Download Console that allows you to download configuration files—or any set of IOS commands—to one or more routers. The Download Console adds the IOS commands to the router's existing configuration file. By default, VPN Solutions Center sets the modified configuration file as the running configuration.

The following procedure describes a typical scenario in which you need to download a previous version of a router's configuration file to one or more routers. To do that, you must first use the Version Console to retrieve a previous version of the configuration file, and then use the Download Console to download the configuration file to the selected routers.

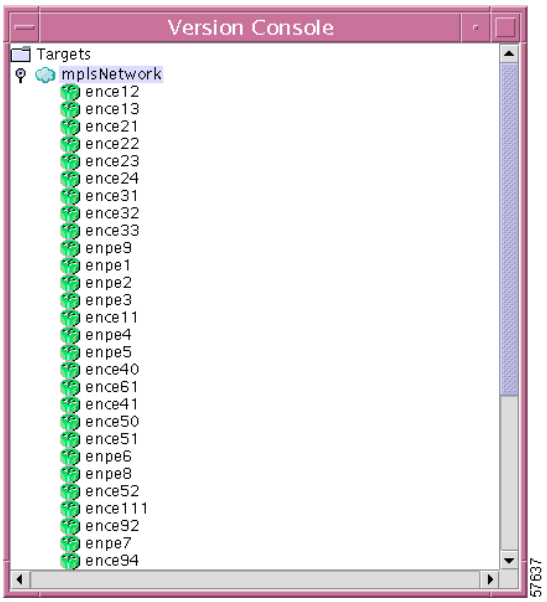
Retrieving a Previous Version of a Configuration File

To retrieve a previous version of a configuration file stored on the VPN Solutions Center workstation, follow these steps:

Step 1 From the VPN Console menu bar, choose **Tools > Version Console**.

The Version Console appears (see Figure 4-46).

Figure 4-46 The Version Console



The Version Console organizes the configuration files by networks and their associated routers.

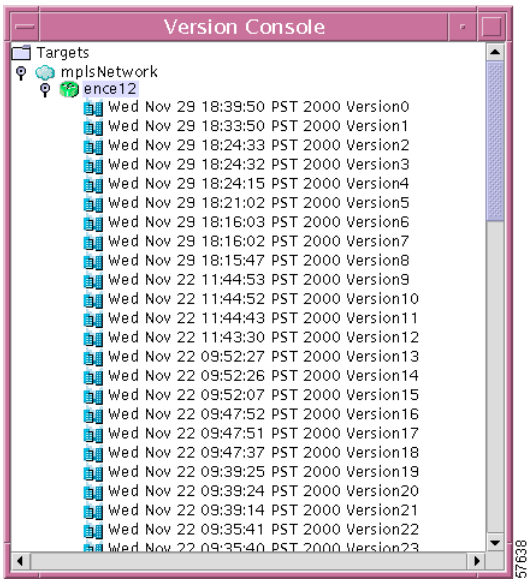
Step 2 Expand the Version Console hierarchy until you can see the router icons and the names of the routers in the pertinent network.

Step 3 Select the router icon for the router that contains the configuration file of interest, then **right-click**.

Step 4 Choose **Open**.

As shown in Figure 4-47, the Version Console displays the version list for the selected router. The versions are displayed according to the dates and times the configuration files were collected, and organized with the most recent version listed first, the next most recent second, and so on.

Figure 4-47 List of Configuration File Versions

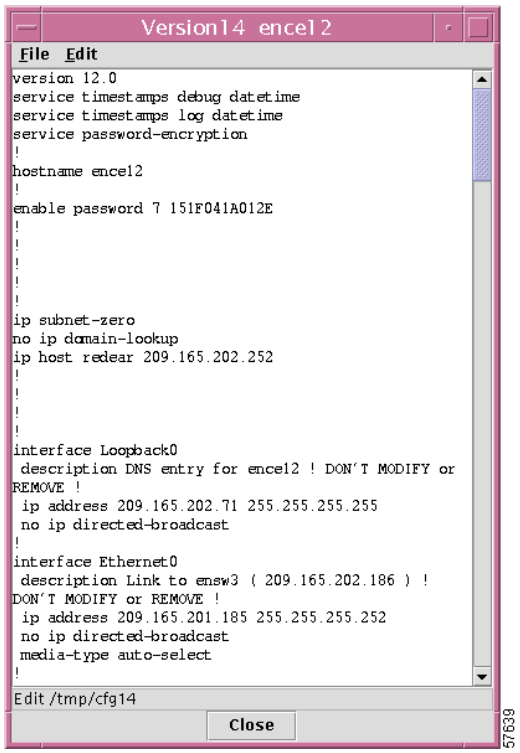


Step 5 To open one of the configuration file versions, select the appropriate version, then **right-click**.

Step 6 Choose **Open**.

The Version window appears, displaying the selected version of the configuration file (see Figure 4-48). The version number and hostname of the router are displayed in the title bar.

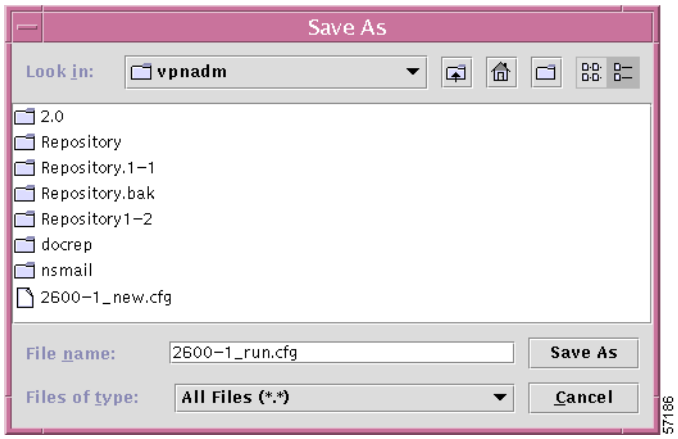
Figure 4-48 Previous Configuration File Displayed



Step 7 To save the desired version of the file to a specified file, from the Version window menu bar, choose **File > Save As**.

The Save As dialog box appears (see Figure 4-49).

Figure 4-49 Saving a Configuration File



Step 8 Enter the filename that you want to save the configuration file to, then click **Save As**.

You return to the Version window.

Step 9 Click **Close**.

Using the Download Console to Modify a Configuration

The Download Console downloads the IOS commands to the selected routers.You can download an actual IOS configuration file, or a file that contains a desired set of IOS commands. By default, VPN Solutions Center sets the modified configuration file as the running configuration.

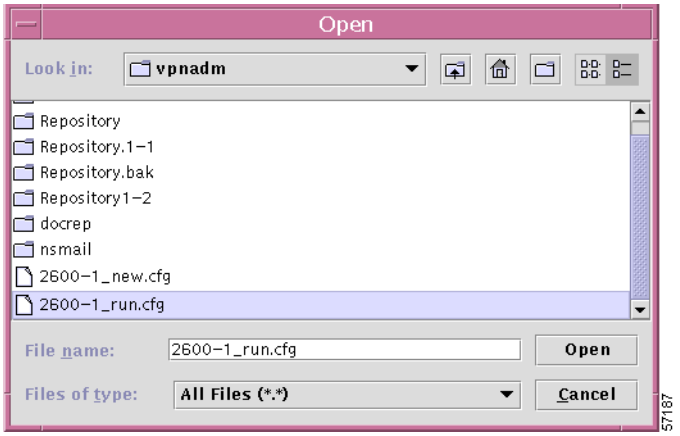
To download a set of IOS commands to one or more routers, follow these steps:

Step 1 From the VPN Console menu bar, choose **Tools > Download Console**.

The Download Console dialog box appears.

Step 2 To open a file from which you want to extract a set of IOS commands that you want to download to selected routers, from the Download Console dialog box, choose **File > Import Config**. The Open dialog box appears (see Figure 4-50).

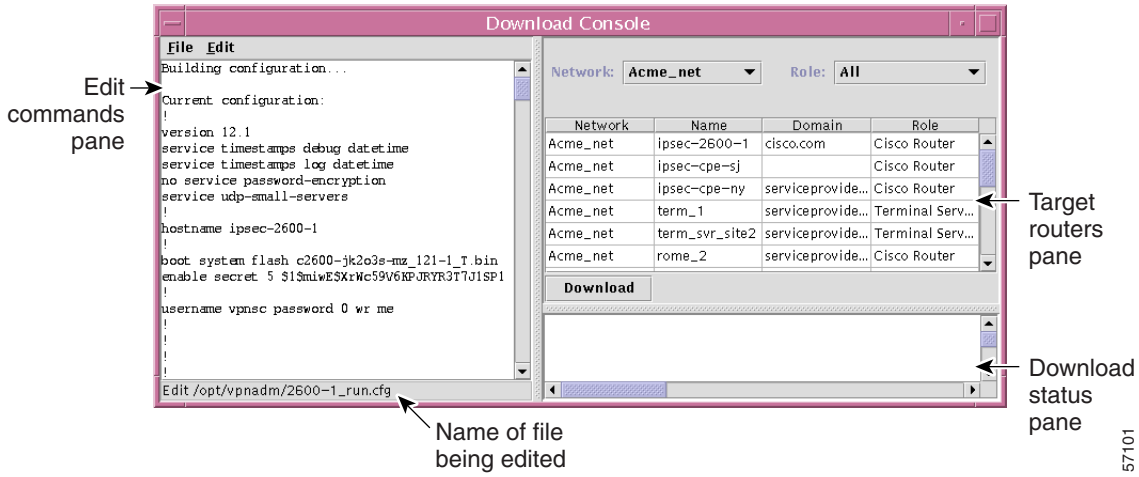
Figure 4-50 Opening the IOS Commands File



Step 3 Select the file you want to open, then click **Open**.

The contents of the selected file are displayed in the Edit Commands pane, as shown in Figure 4-51.The upper right pane displays the list of target routers in the Target Routers pane. The lower right pane is the Download Status pane.

Figure 4-51 The IOS Commands File Displayed in the Download Console



Step 4 You can edit the text displayed in the Edit Commands pane as necessary by using the standard keyboard commands to cut, copy, or paste the text.

Step 5 When you are satisfied with the set of commands displayed in the edit commands pane, select the routers that you want to download the IOS commands to from the target routers pane.

a. From the Network drop-down menu, choose the appropriate target network name.

The list of network devices in the selected network are displayed.

b. From the Role drop-down menu, choose **Cisco Router**.

The list of Cisco routers in the selected network are displayed.

c. From the Target Routers pane, select one or more target routers.

Step 6 Click **Download**.

You receive the following message:

Are you sure you wish to download the configlet to the selected routers?

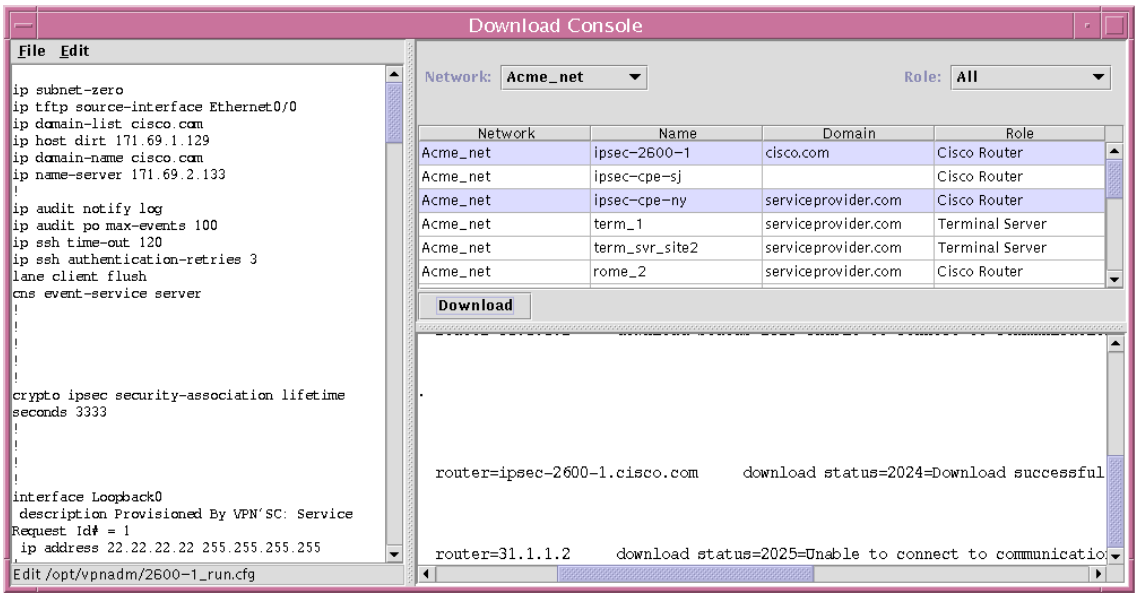
Step 7 To proceed with downloading the set of IOS commands, click **Yes**.

To cancel the IOS commands download operation, click **No**.

VPN Solutions Center downloads the commands displayed in the Edit Commands pane to the selected routers. These commands are added to the existing configuration on the selected routers.

Figure 4-52 shows the Download Console as it appears when the IOS command download operation is complete. The status of the download operation is displayed in the Download Status pane.

Figure 4-52 IOS Command File Download Operation Complete



Use the scroll bar in the Download Status pane to view the status information that the routers return in response to the downloaded IOS commands.

Step 8 To exit from the Download Console, choose **File > Exit**.

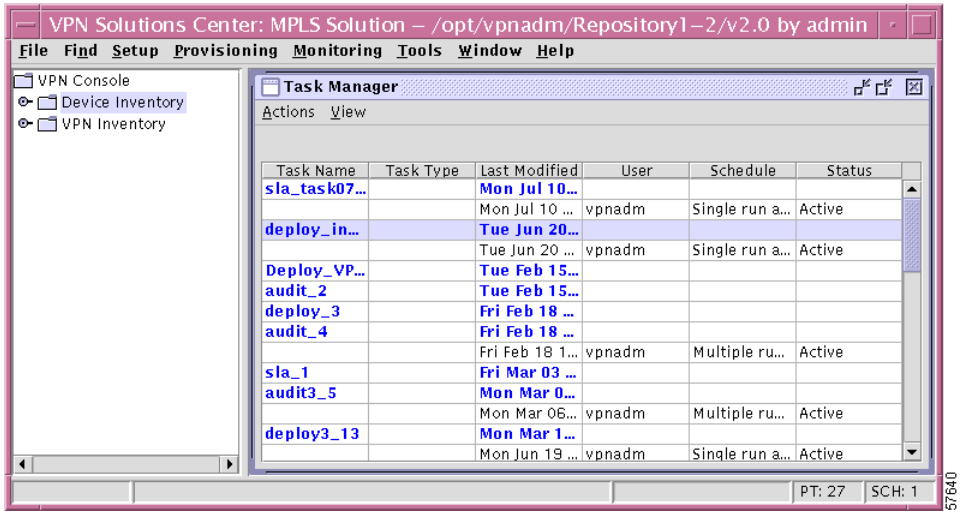
Using the Task Manager

VPN Solutions Center provides a Task Manager that allows you to view pertinent information about both current and expired provisioning tasks, as well as create and schedule tasks, delete specified tasks, and delete the expired tasks.

To bring up the Task Manager, choose **Tools > Tasks** from the VPN Console menu.

The Task Manager window appears (see Figure 4-53).

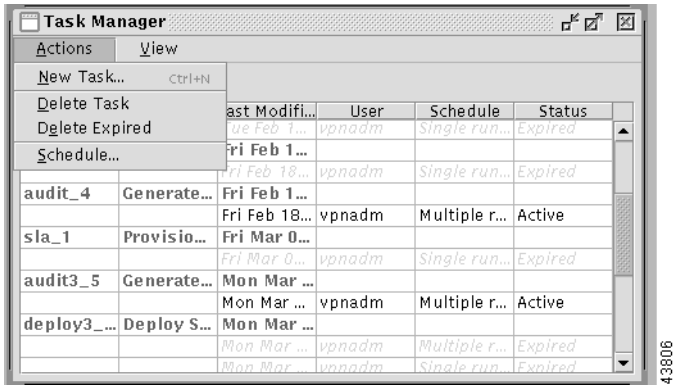
Figure 4-53 The Task Manager Window



The Task Manager window provides information on each task by name, including the task type, the date when the task was last modified, the VPN Solutions Center username, schedule summary information, and its current status—expired or active.

From the Actions menu (shown in Figure 4-54), you can execute all the necessary task-related functions:

Figure 4-54 The Task Manager Actions Menu



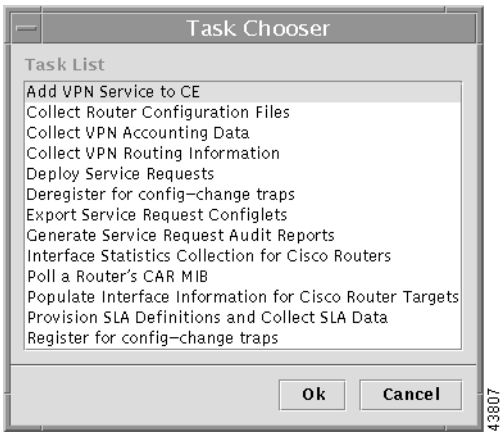
Creating a New Task

Step 1 From the VPN Console, choose **Tools > Tasks**. The Task Manager window appears.

Step 2 To create a new task, choose **Actions > New Task** from the Task Manager menu.

The Task Chooser appears (see Figure 4-55).

Figure 4-55 The Task Chooser



Step 3 From the Task List, choose the task you want to execute and press **OK**.

Step 4 Complete the task wizard as required.

Deleting a Task

When you delete a task through the Task Manager, you delete both the persistent and the scheduled tasks.VPN Solutions Center removes the task from the Task Repository and updates the task logs (see also the "Deleting Task Logs" section on page 4-68).

To delete one or more tasks, do the following:

Step 1 From the VPN Console, choose **Tools > Tasks**. The Task Manager window appears.

Step 2 In the Task Manager window, select one or more tasks to delete.

Step 3 Choose **Actions > Delete Task**.

You are asked to confirm the deletion request:

```
You have selected to delete n task(s) from the Repository. Do you want to continue?
```

Step 4 To delete the selected tasks, click **Continue**.

You can also cancel the operation at this point by clicking **Cancel**.

VPN Solutions Center deletes the selected tasks and redisplays the current list of tasks in the Task Manager window.

Deleting Expired Tasks

To delete tasks that have expired, follow these steps:

Step 1 From the VPN Console, choose **Tools > Tasks**. The Task Manager window appears.

Step 2 From the Task Manager, choose **Actions > Delete Expired**.

You are asked to confirm the deletion request:

You have selected to delete the expired tasks from the Repository. Do you want to continue?

Step 3 To delete the expired tasks, click **Continue**.

You can also cancel the operation at this point by clicking **Cancel**.

VPN Solutions Center deletes the expired tasks and redisplays the current list of tasks in the Task Manager window.

Scheduling a Task

The VPN Solutions Center Task Manager allows you to schedule a selected task. To schedule a task, follow these steps:

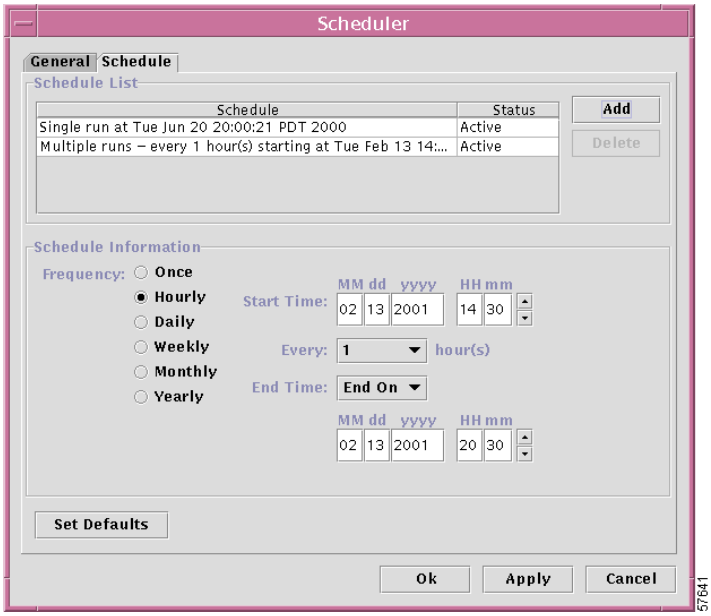
Step 1 From the VPN Console, choose **Tools > Tasks**. The Task Manager window appears.

Step 2 From the Task Manager window, select the task you want to schedule.

Step 3 From the Task Manager, choose **Actions > Schedule**.

The Scheduler dialog box appears (see Figure 4-56).

Figure 4-56 The Scheduler Dialog Box



Step 4 Complete the fields in the dialog box to schedule the task as needed.

a. From the *Frequency* list, choose the desired frequency: **Once**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.

b. Set the *Start Time*: **Now** or **Later**.

c. If you choose **Later**, specify the date and time to start and end the service.

d. If you choose anything other than **Once**, specify how often the service should run from the **Every** drop-down list.

Step 5 When you have scheduled the task to your satisfaction, click **Add**.

The task is added to the Schedule List, displayed in the upper area of the dialog box (as shown in Figure 4-56).

Step 6 Click **OK**.

You return to the VPN Console. The task is added to the VPN Solutions Center task queue; it will begin executing on the date and time specified.

Using the Task Logs

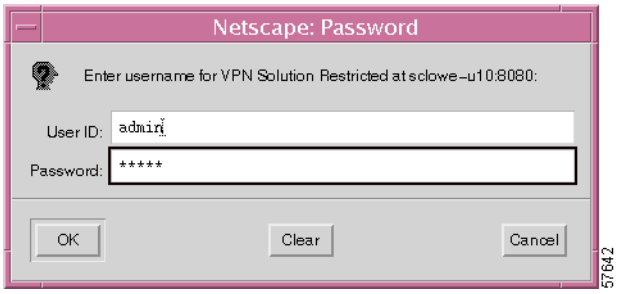
To access the VPN Solutions Center task logs, do the following:

Step 1 From the VPN Console, choose **Tools > Task Logs**.

VPN Solutions Center starts the browser and displays the Task Logs window.

If Netscape has not already started, the Netscape Password dialog box appears (see Figure 4-57).

Figure 4-57 Logging in to the VPN Solutions Center Browser

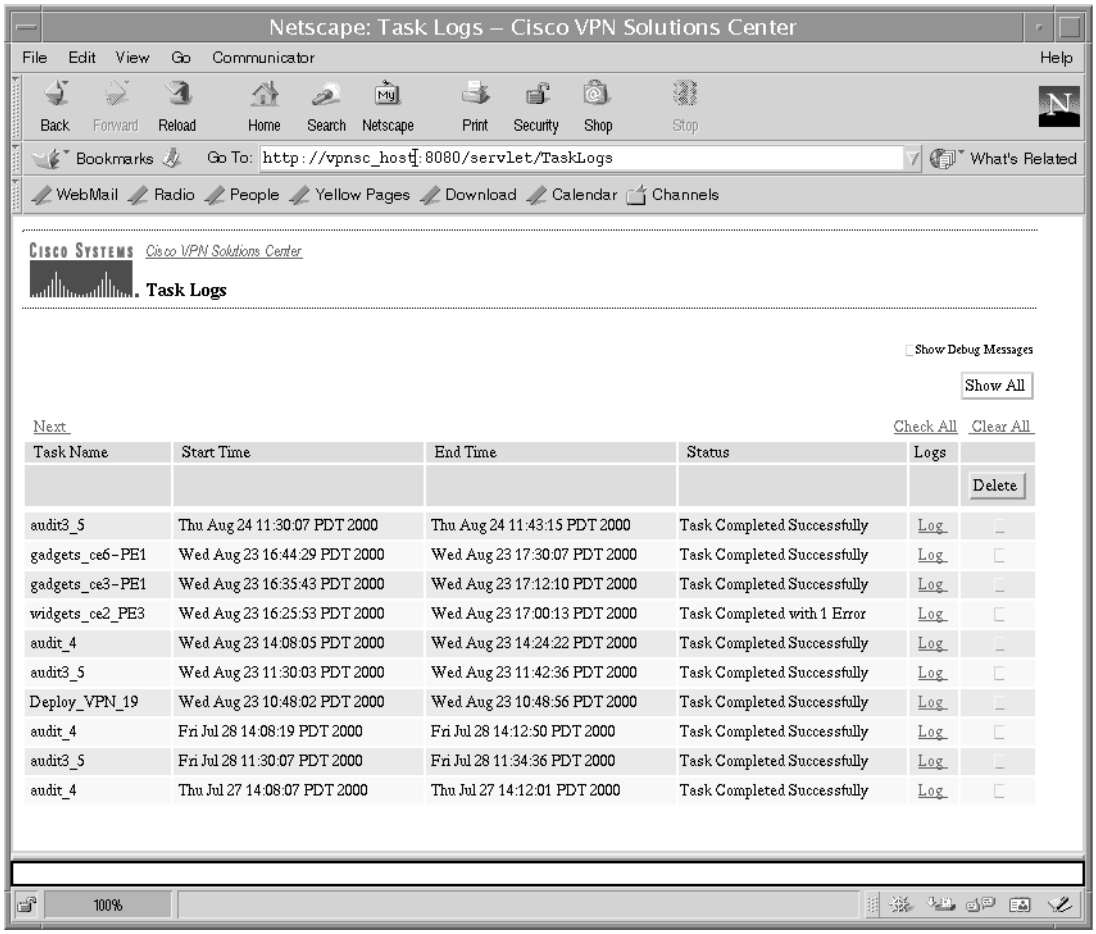


Step 2 In the Netscape Password dialog box, enter the VPN Solutions Center administrative username and password, then click **OK**.

The tasks are listed in order of the task start time; the task with the latest start time is listed at the top of list, and the task with the earliest start time is listed at the bottom of the list.

Notice the **Logs** column in Figure 4-58, which provides a **Log** link for every task listed.

Figure 4-58 Viewing the List of Tasks

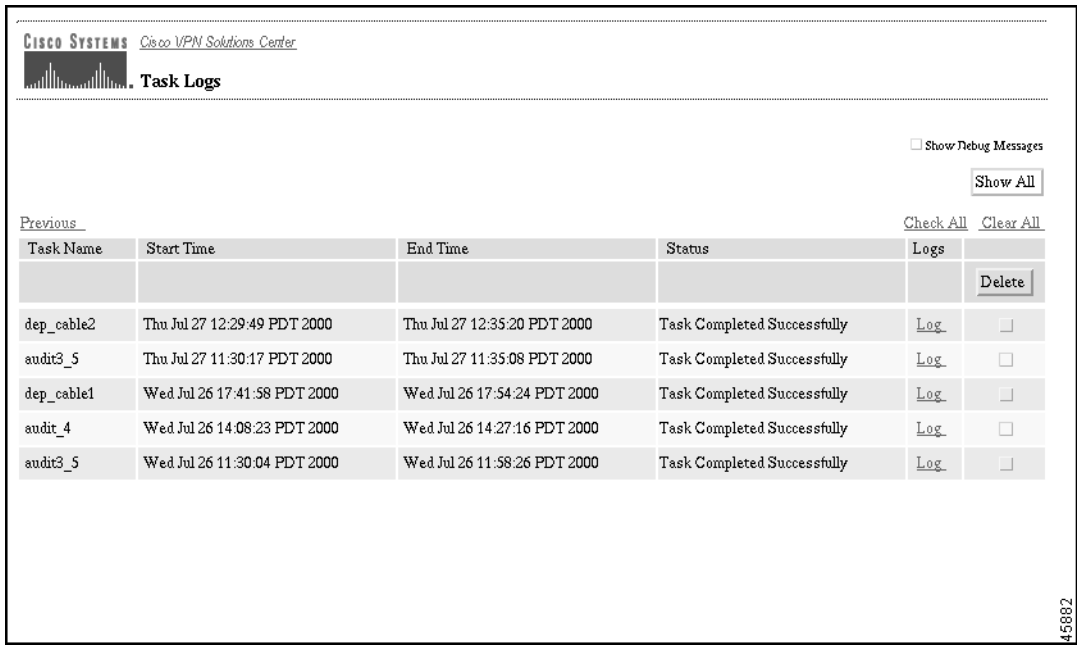


Task Name	Start Time	End Time	Status	Logs
audit3_5	Thu Aug 24 11:30:07 PDT 2000	Thu Aug 24 11:43:15 PDT 2000	Task Completed Successfully	Log
gadgets_ce6-PE1	Wed Aug 23 16:44:29 PDT 2000	Wed Aug 23 17:30:07 PDT 2000	Task Completed Successfully	Log
gadgets_ce3-PE1	Wed Aug 23 16:35:43 PDT 2000	Wed Aug 23 17:12:10 PDT 2000	Task Completed Successfully	Log
widgets_ce2_PE3	Wed Aug 23 16:25:53 PDT 2000	Wed Aug 23 17:00:13 PDT 2000	Task Completed with 1 Error	Log
audit_4	Wed Aug 23 14:08:05 PDT 2000	Wed Aug 23 14:24:22 PDT 2000	Task Completed Successfully	Log
audit3_5	Wed Aug 23 11:30:03 PDT 2000	Wed Aug 23 11:42:36 PDT 2000	Task Completed Successfully	Log
Deploy_VPN_19	Wed Aug 23 10:48:02 PDT 2000	Wed Aug 23 10:48:56 PDT 2000	Task Completed Successfully	Log
audit_4	Fri Jul 28 14:08:19 PDT 2000	Fri Jul 28 14:12:50 PDT 2000	Task Completed Successfully	Log
audit3_5	Fri Jul 28 11:30:07 PDT 2000	Fri Jul 28 11:34:36 PDT 2000	Task Completed Successfully	Log
audit_4	Thu Jul 27 14:08:07 PDT 2000	Thu Jul 27 14:12:01 PDT 2000	Task Completed Successfully	Log

The task logs are displayed in sets of 10 logs per page. To jump to the next page of task logs, click the **Next** link (in the upper left corner of the task logs table).

The next page of task logs provides a **Previous** link so you can jump to the previous page of task logs, as shown in Figure 4-59.

Figure 4-59 Jumping to the Next and Previous Pages of Task Logs

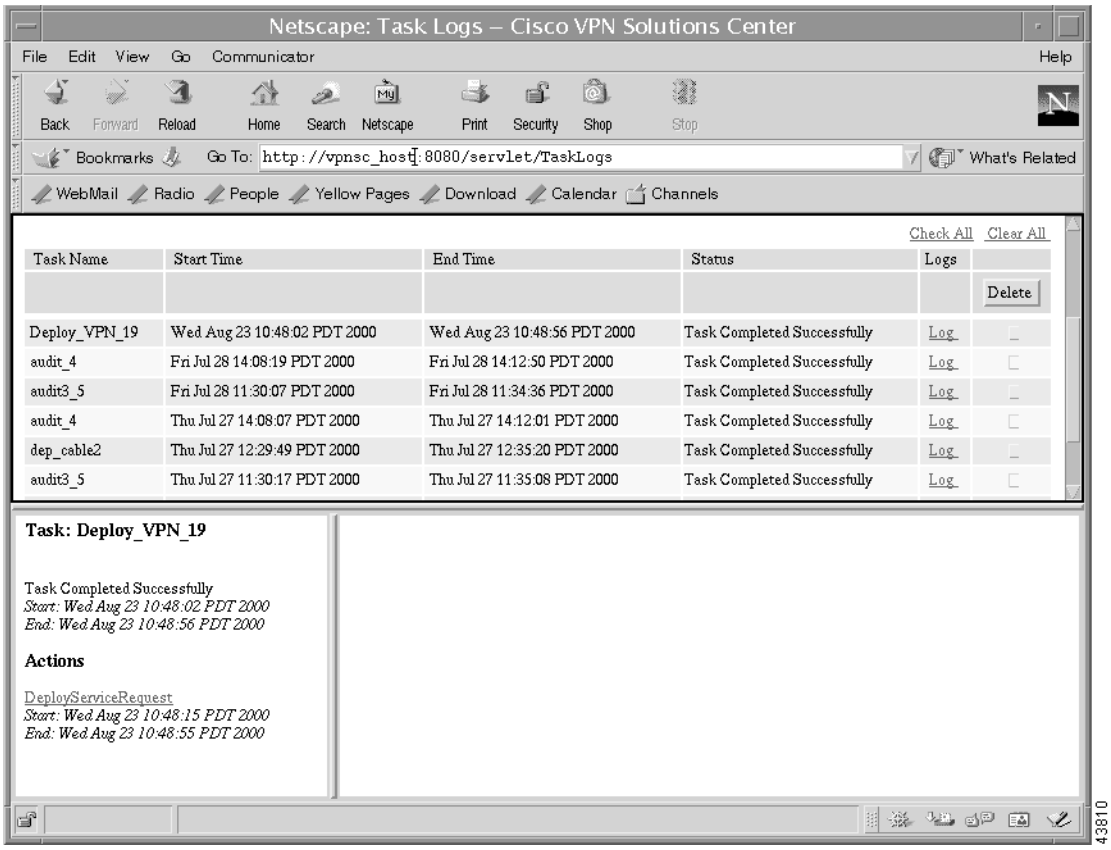


When there are task log pages above and below the current position, the task logs page provides both **Next** and **Previous** links so you can navigate efficiently through multiple pages.

Step 3 Scroll to the name of the task whose log you want to view, then click the corresponding **Log** link on that row.

The status report for the selected task appears in the lower left pane, as shown in Figure 4-60.

Figure 4-60 Displaying the Task Status



The status pane shows the following information for the selected task:

- Task status summary

  The possible task status summary states can be any one of the following: **Task Completed Successfully**, **Running**, **Task Terminated**, or **Task Completed with *n* Errors**.

- Start time
- End time
- All the actions under the currently selected task
- Start time and end time for all the actions

Viewing a Task Action Log

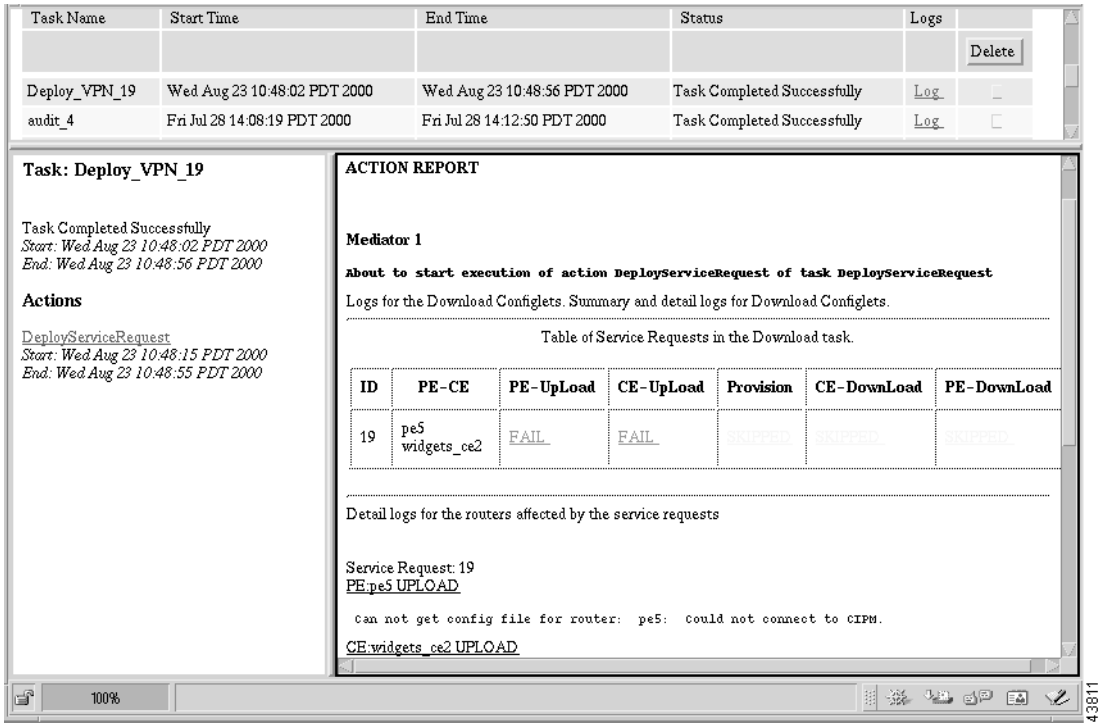
Step 4 To see an Action log for the selected action, click the link displayed under the Actions heading.

The Action log appears in the lower right pane (see Figure 4-61).

For example, for the task shown, *Deploy_VPN_19*, there is only one action—"Deploy Service Request." (Some tasks have more than one action listed.)

To view the action report for the action "Deploy Service Request" for task "Deploy_VPN_19," click the **DeployServiceRequest** link.

Figure 4-61 The Task Action Report

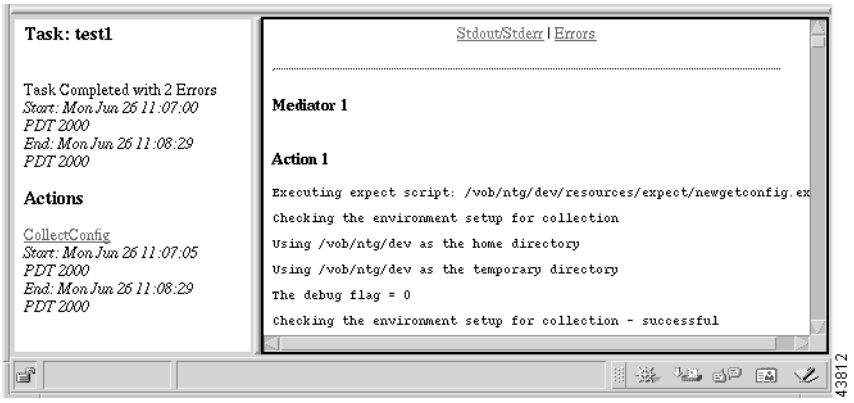


Viewing the Standard Output/Standard Error Log

Step 5 To view the standard output and error logs for the selected task, click the **Stdout/Stderr** link.

The Standard Output and Error log appears in the lower right pane (see Figure 4-62).

Figure 4-62 Standard Output and Error Logs

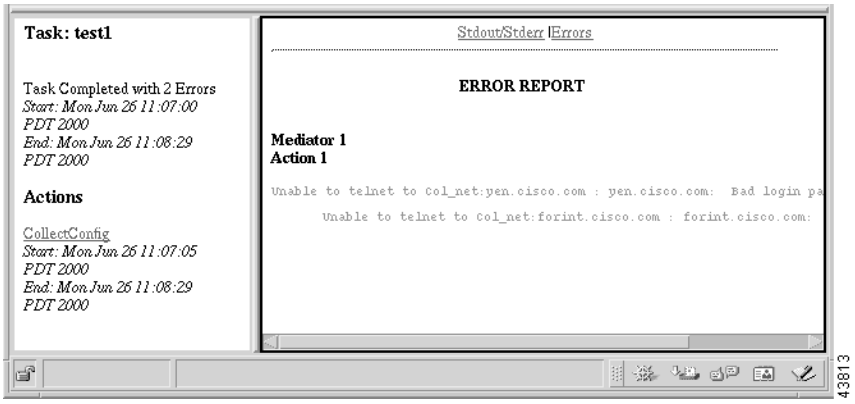


Viewing the Task Log Error Report

Step 6 To view the Error Report for the selected task log, click the **Errors** link.

The Task Log Error Report appears in the lower right pane (see Figure 4-63).

Figure 4-63 Task Log Error Report



Viewing Debug Messages

When you check the **Show Debug Messages** checkbox, you can view in the task logs any debug messages that were generated.

Deleting Task Logs

To save disk space, you can delete task logs when they become obsolete. When you delete a task from the task logs, you delete the run-time task and the logs associated with the task.

Tips

We recommend that you delete no more than 10 task logs at a time.
When you have a large number of tasks and would like to delete the oldest logs, you may find it more convenient to click the **Show All** button. **Show All** displays all the tasks in one page, so if you have a large number of tasks in the Repository, the browser often takes a long time to display all of the tasks. But the advantage to this procedure is that you can delete the oldest logs (which would be the last set of tasks in the list), rather than having to click **Next** many times to reach the last page of logs.

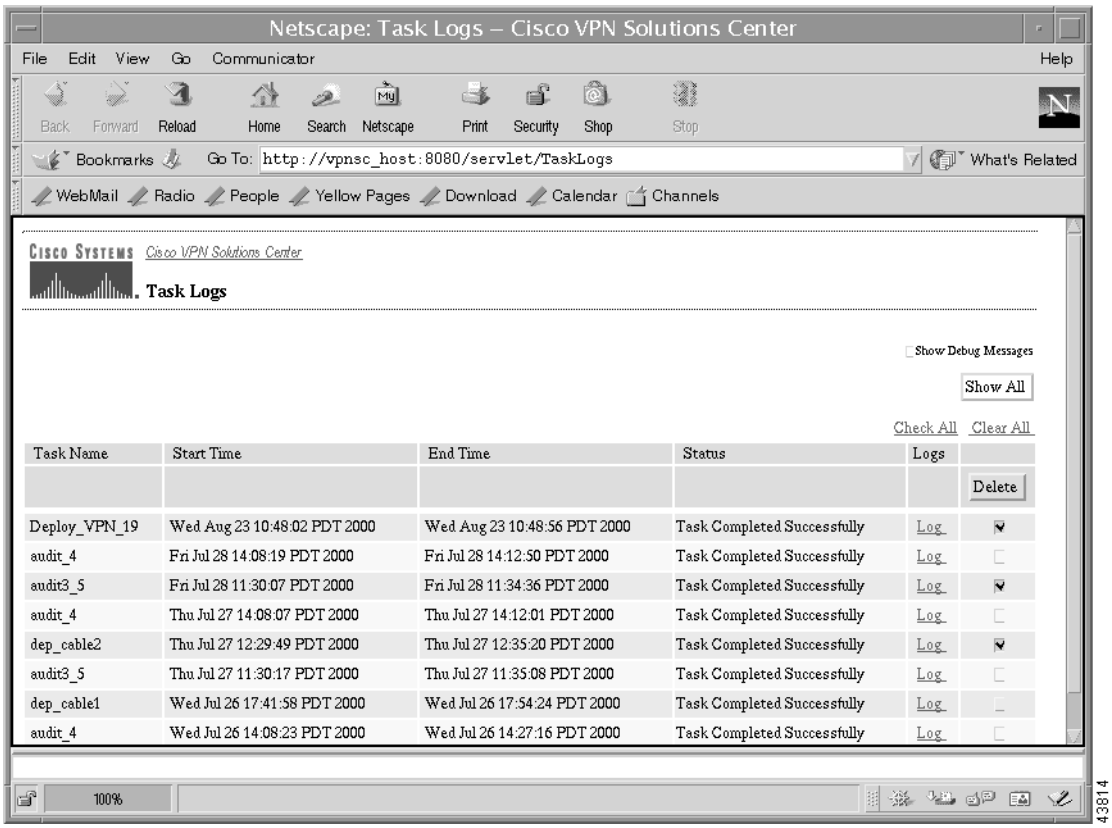
To delete task logs, follow these steps:

Step 1 From the VPN Console, choose **Tools > Task Logs**.

VPN Solutions Center starts the browser and displays the Task Logs window. Notice the **Delete** column (the rightmost column in the Task Logs window) as shown in Figure 4-64.

The tasks are listed in order of the task start time; the task with the latest start time is listed at the top of list, and the task with the earliest start time is listed at the bottom of the list.

Figure 4-64 The Task Logs Window



Task Name	Start Time	End Time	Status	Logs	
Deploy_VPN_19	Wed Aug 23 10:48:02 PDT 2000	Wed Aug 23 10:48:56 PDT 2000	Task Completed Successfully	Log	☑
audit_4	Fri Jul 28 14:08:19 PDT 2000	Fri Jul 28 14:12:50 PDT 2000	Task Completed Successfully	Log	☐
audit3_5	Fri Jul 28 11:30:07 PDT 2000	Fri Jul 28 11:34:36 PDT 2000	Task Completed Successfully	Log	☑
audit_4	Thu Jul 27 14:08:07 PDT 2000	Thu Jul 27 14:12:01 PDT 2000	Task Completed Successfully	Log	☐
dep_cable2	Thu Jul 27 12:29:49 PDT 2000	Thu Jul 27 12:35:20 PDT 2000	Task Completed Successfully	Log	☑
audit3_5	Thu Jul 27 11:30:17 PDT 2000	Thu Jul 27 11:35:08 PDT 2000	Task Completed Successfully	Log	☐
dep_cable1	Wed Jul 26 17:41:58 PDT 2000	Wed Jul 26 17:54:24 PDT 2000	Task Completed Successfully	Log	☐
audit_4	Wed Jul 26 14:08:23 PDT 2000	Wed Jul 26 14:27:16 PDT 2000	Task Completed Successfully	Log	☐

Step 2 Check the **Delete** check box for each task log you want to delete.

a. To mark all the tasks in the current page for deletion, click **Check All**.

When you click **Check All**, all the tasks on the current page are checked—not all the tasks in the Repository. Thus, when you click **Check All**, then click **Delete**, the application deletes only the tasks in the current page.

b. To clear all the check boxes in the current page, click **Clear All**.

Step 3 When you have indicated which task logs are to be deleted, click **Delete**.

The VPN Solutions Center software deletes the selected task logs and redisplays the Task Logs window.