CHAPTER 2

Setting Up the MPLS VPN Environment

Cisco VPN Solutions Center: MPLS Solution is an MPLS VPN provisioning and auditing tool. The software focuses on the provider edge routers (PEs), customer edge routers (CEs), and the link between them. VPN Solutions Center software uses the Telnet Gateway Server (TGS) software to transport configuration file information to and from target routers. Additional features include Class of Service (CoS) provisioning, VPN-aware NetFlow accounting, and Service Level Agreement (SLA) monitoring.

The Cisco VPN Solutions Center (VPNSC) also provides external access to its provisioning, accounting, and SLA monitoring features through CORBA APIs.

Starting the VPN Solutions Center Software

Before you can start the VPN Solutions Center software, you must install the license key (see the "Installing the VPN Solutions Center License" section on page 2-4). The license key is supplied in the *Right to Use* document that is provided when you purchase VPN Solutions Center software.

As shown in Figure 2-3 on page 2-4, the Install License dialog box displays the number of edge devices you have a license for and the number of edge devices currently created. As you add edge devices to the VPNs defined in the VPN Solutions Center software, the number of edge devices created is incremented.

You can check the number anytime by choosing **Tools > License Administration** from the VPN Console menu bar and viewing the updated number of edge devices created.

When you reach 90 percent of the number of devices you are licensed for, VPN Solutions Center sends you a message to alert you to that situation. Cisco Systems strongly recommends that you take measures to upgrade your license agreement at that time.

Note When the number of edge routers created equals the number of edge routers licensed, you receive an email message to inform you. You cannot add any additional edge routers until you purchase an updated license and install the license key as described in this section.

Before you start the VPN Solutions Center software, complete these tasks:

Step 1 Log into the VPN Solutions Center (VPNSC) workstation under your own login name.

Step 2 *To keep the startup operations conveniently organized, open three terminal windows*—one window for the xhost process, one for the VPN Console and Watchdog, and a third window for Orbix.

Step 3 In the first terminal window, enter the following command:

```
xhost VPNSC_hostname
```

The *VPNSC_hostname* parameter is the name of the VPN Solutions Center workstation. This command configures your system so that the Orbix administrative user (orbixadm) and the MPLS VPN administrative user (vpnadm) can communicate with your client system.

Starting Orbix

Starting the VPN Solutions Center software requires that you first start the Orbix process and then start the Watchdog process and the VPN Console as described below. To start the Orbix software, follow these steps:

Step 1 Go to the terminal window for the Orbix software.

Step 2 Log in as administrative user of the Orbix process (*orbixadm*).

```
su - orbixadm
```

Or if you are logging in remotely, enter this command:

```
rlogin VPNSC_hostname -l orbixadm
```

Step 3 Change directory to the directory where Orbix is installed:

```
cd /opt/orbixamd/orbix/Orbix3
```

Step 4 Issue the following command to source the environment as required for your shell:

C-shell: **source setenvs.csh**

K-shell: . **setenvs.sh**

Step 5 Start the Orbix process in the background:

```
orbixd &
```

Starting the Watchdog and the VPN Console

Step 1 Go to the terminal window for the Watchdog and the VPN Console.

Step 2 Log in as the administrative user of the VPN Solutions Center software (*vpnadm)*.

```
su - vpnadm
```

Or if you are logging in remotely, enter this command:

```
rlogin VPNSC_hostname -l vpnadm
```

Step 3 Go to the directory where VPN Solutions Center is installed.

```
cd /opt/vpnadm/vpn/
```

Step 4 Issue the appropriate command to source the environment as required for your shell.

C-shell: **source vpnenv.csh**

K-shell: . **vpnenv.sh**

Step 5 Set the display variable for the VPN Solutions Center workstation:

C-shell: **setenv DISPLAY** *VPNSC_hostname*:0.0

K-shell: **export DISPLAY=**VPNSC_hostname:0.0

The "VPNSC_hostname" you enter here should be the hostname used to Telnet to the VPN Solutions Center workstation.

Step 6 Start the application's Watch Dog processes:

```
startwd
```

To stop the Watch Dog process, issue the **stopwd -y** command.

The Watch Dog log file is located at */opt/vpnadm/vpn/tmp/wdlog*.

Step 7 If you would like to confirm that the servers are running, issue the following command:

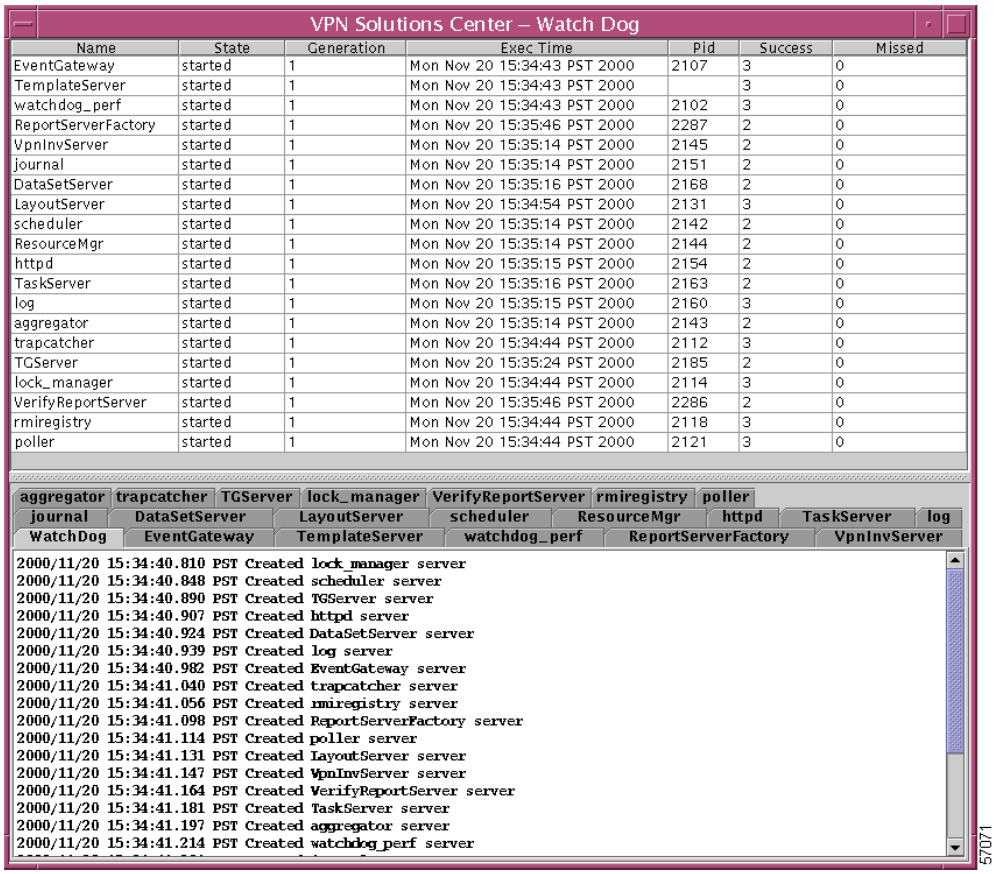
```
wdclient status
```

If you would prefer to bring up the Watch Dog graphical user interface, issue this command:

```
wdgui &
```

The Watch Dog interface appears (see Figure 2-1):

Figure 2-1 The VPN Solutions Center Watch Dog Interface



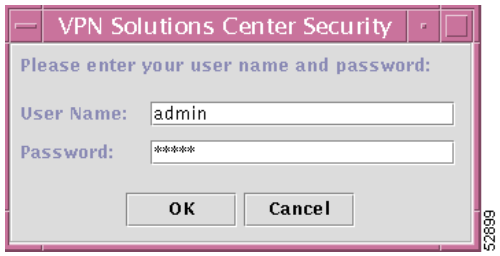
For a detailed description of the WatchDog graphical user interface, refer to the "wdgui Command" section in Chapter 2, "Watch Dog Commands," of the *Cisco VPN Solutions Center: MPLS Solution User Reference*.

Step 8 Issue the following command to start the VPN Console:

```
vpnconsole -mode mpls &
```

The VPN Solutions Center Security dialog box appears (see Figure 2-2).

Figure 2-2 The VPN Solutions Center Security Dialog Box



Step 9 Enter a valid user name and password, then click **OK**.

The default username is **admin**. The default password is **admin**.

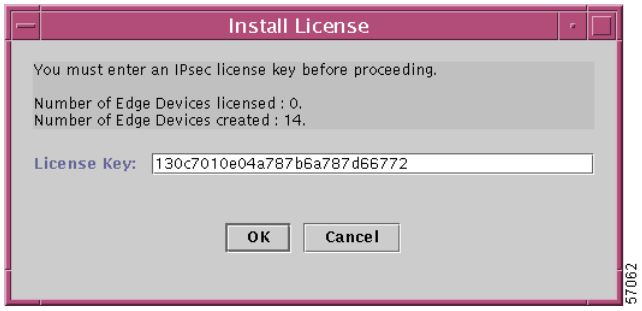
Note You cannot change the *admin* username, but you can change the password for the *admin* user. Additionally, you can add new usernames and assign their associated passwords. The password for the VPN Console must be at least six (6) characters in length and no more than eight (8) characters in length. For details, see "User Administration" in Chapter 9, "VPN Console: Tools Menu," of the *Cisco VPN Solutions Center: MPLS Solution User Reference, Release 2.0*.

Installing the VPN Solutions Center License

An edge device is counted only once when it is added to a VPN as a CE or PE. If another VPN uses an edge device already counted in another VPN, it is not added again to the license count.

After you log in, the Install License dialog box appears (see Figure 2-3).

Figure 2-3 Installing the License Key



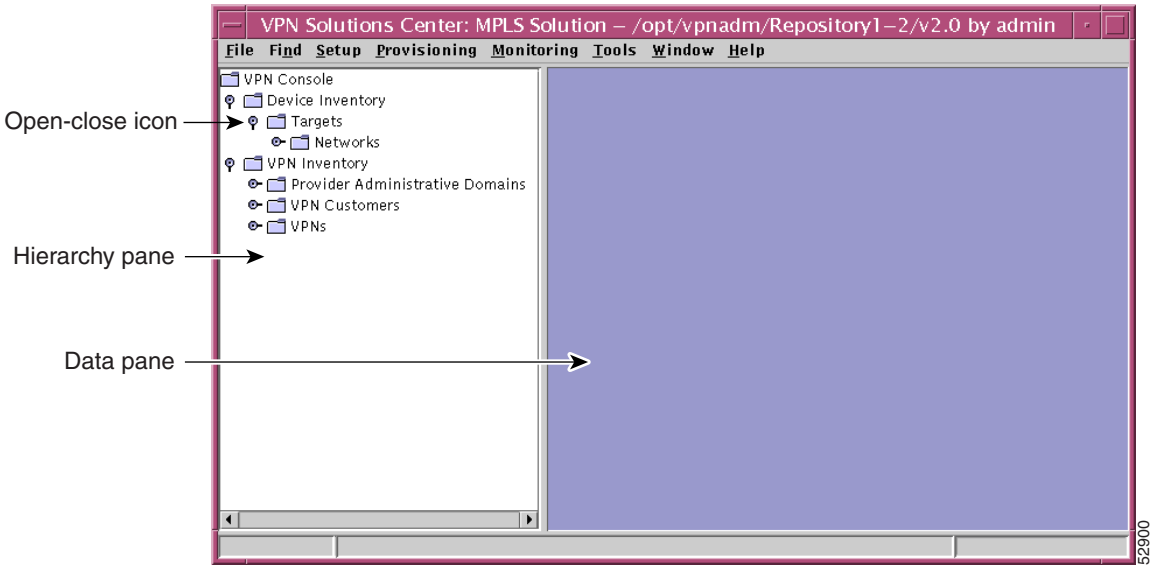
Step 10 Enter the License Key you received with the VPN Solutions Center software.

Your License Key is supplied in the *Right to Use* document.

Step 11 Click **OK**.

The VPN Solutions Center VPN Console appears, as illustrated in Figure 2-4.

Figure 2-4 The VPN Console (MPLS Solution)



Proceed to the "Setting Up the Network in the VPN Solutions Center Software" section on page 2-24.

Shutting Down the VPN Solutions Center Software

This section assumes that the VPN Solutions Center software is running, and that the software user names—vpnadm and orbixadm—are active. It also assumes that Orbix is running as a background process. To shut down the VPN Solutions Center software, execute these commands:

Step 1 If the VPN Console is running, close it by choosing **File > Exit**.

Step 2 If the Watchdog user interface (wdgui) is running, close it by selecting the window, **right-click**, then choose **Close** from the menu.

Step 3 From the window where Watchdog was launched, close the Watchdog by issuing this command:

```
stopwd -y
```

Step 4 Log out (exit) from the vpnadm user.

Shutting down Orbix is optional. To shut down Orbix, follow these steps:

Step 5 From the terminal window from which you launched Orbix, shut down the Name Server:

```
killit NS
```

Step 6 Discover the process ID of orbixd:

```
ps -ef | grep orbixd
```

Step 7 Shut down the Orbix process by issuing this command:

```
kill orbixd_process_ID
```

Step 8 Log out (exit) from the orbixadm user.

Tasks to Be Completed Before Using VPNSC Software

Before you use VPN Solutions Center: MPLS Solution software to provision an MPLS network, the Service Provider must complete the following tasks:

- IPv4 connectivity must be operational among all the routers in the MPLS VPN network routers before provisioning can take place.
- The Service Provider or Customer must create a loopback interface on each router.
- Each router must have a routable IP address.
- Optionally, you can set up the Secure Shell (SSH) on the CE routers (see the next section for details).
- Set up SNMP on all the edge routers in the network—see the "Setting Up SNMPv1 and SNMPv2 on the Routers in the Service Provider Network" section on page 2-8 and the "Setting the SNMPv3 Parameters on the Routers in the Service Provider Network" section on page 2-9.
- Enable SA Agent on all edge devices that you want to collect SLA data from—see the "Enabling SA Agent on Edge Device Routers" section on page 2-11.
- If you choose to use TFTP (Trivial File Transfer Protocol) as the default configuration transport method, you must enable TFTP on the VPN Solutions Center workstation and on the target routers—see the "Enabling TFTP on the VPN Solutions Center Workstation" section on page 2-11.
- If you are installing and using Telnet Gateway Servers on remote networks, complete the procedures described in the "Setting Up Connectivity to a Remote Telnet Gateway Server" section on page 2-14.

Caution Make sure that the file descriptor limit is *not* set in the VPN Solutions Center workstation login shell file (which can be the *.login* file, the *.cshrc* file, or the *.kshrc* file). If the login shell file contains a line with the **ulimit -n** command (for example, "`ulimit -n <number>`"), comment out this command line in the file.

VPN Solutions Center cannot override the file descriptor limitation setting in the login shell file. If the value is set incorrectly, VPN Solutions Center experiences operational problems.

Setting Up Devices in the VPN Solutions Center MPLS Environment

This section describes the tasks the Service Provider should complete to set up devices in the VPN Solutions Center MPLS environment.

Setting Up the Secure Shell (SSH) on Edge Routers

Service providers need a mechanism to deploy VPN configuration files to remote edge routers in a secure manner. The basic requirements for secured management are as follows:

- The edge device routers and VPN Solutions Center must be able to authenticate each other.
- An encrypted channel for uploading and downloading router configuration information must be in place.

VPN Solutions Center 2.0 uses TGS as the configuration file download mechanism. One of the modes that TGS can operate in is *Secure Shell (SSH) mode*. The Telnet Gateway Server uses SSH for both authentication and encryption.In this scheme, the edge device router functions as an SSH server, while VPN Solutions Center functions as the SSH client.

Note This configuration procedure assumes that the router's authentication database is stored locally on the router and not on a TACACS (Terminal Access Controller Access Control System) server.

The procedure for configuring SSH on edge device routers is as follows:

	Command	Description
Step 1	`Router# configure terminal`	Enter global configuration mode.
Step 2	`Router(config)# ip domain-name domain_name`	Specify the IP domain name.

Step 3	`Router(config)# crypto key generate rsa`	Generate keys for the SSH session.
		The **crypto key generate rsa** command is interactive. You will see the following prompt:
		`Choose the size of the key modulus in the range of 360 to 2048 for your general purpose keys.`
		`How many bits in the modulus (nnn):`

Step 4		Press **Enter** to accept the default number of bits.
Step 5	`Router(config)# username username password password`	Configure the user ID and password. Enter the VPNSC workstation username and password you are logged in as. For example, **username admin password vpnsc**.
Step 6	`Router(config)# line vty 0 4`	Enable SSH as part of the vty login transport.

	Command	Description
Step 7	`Router(config-line)# login local`	The **login** command can take either **local** or **tacacs** as its value. This command indicates that the router stores the authentication information locally.
Step 8	`Router(config-line)# transport input telnet ssh`	
Step 9	`Router(config-line)# Ctrl+Z`	Return to Privileged Exec mode.
Step 10	`Router# copy running startup`	Save the configuration changes to NVRAM.

Setting Up SNMPv1 and SNMPv2 on the Routers in the Service Provider Network

The Simple Network Management Protocol (SNMP) must be configured on each router and edge device in the service provider network. To determine whether SNMP is enabled and set the SNMP community strings on a router, execute the following steps for each router.

	Command	Description
Step 1	`> telnet router_name`	Telnet to the router you want to configure.
Step 2	`Router> enable` `Router> enable_password`	Enter enable mode, then enter the enable password.
Step 3	`Router# show snmp`	Check the output of the **show snmp** command to see whether the following statement is present: "*SNMP agent not enabled.*" If SNMP is not enabled, complete the steps in this procedure.
Step 4	`Router# configure terminal`	Enter global configuration mode.
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.

Tips The SNMP strings defined in the VPNSC: MPLS Solution target password database must agree with those set on each router in the service provider network. The procedure for setting the SNMP parameters in the VPNSC: MPLS Solution software is described in the "Setting the SNMPv3 Parameters for VPNSC Target Routers" section on page 4-9.

Setting the SNMPv3 Parameters on the Routers in the Service Provider Network

Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

This section describes how to set the SNMPv3 parameters on the routers in the service provider network. To complete the task regarding SNMPv3 parameters, you also must set a selected set of parameters in the VPN Solutions Center software (see the "Setting the SNMPv3 Parameters for VPNSC Target Routers" section on page 4-9). The SNMPv3 parameters you set on the routers must match the SNMPv3 parameters you specify in the VPN Solutions Center software.

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensuring that a packet has not been tampered with in-transit.
- Authentication—Determining the message is from a valid source.
- Encryption—Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

Using SNMPv3, data can be collected securely from SNMP devices without fear of the data being tampered with or corrupted. Also, using the **SNMP Set** command, packets that change a router's configuration can be encrypted to prevent its contents from being exposed on the network.

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

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. Table 2-1 identifies the combinations of security models and levels.

Table 2-1 SNMP Security Models and Levels

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

SNMPv3 objects have the following characteristics:

- Each user belongs to a group.
- A group defines the access policy for a set of users.
- An access policy is what SNMP objects can be accessed for reading, writing, and creating.
- A group determines the list of notifications its users can receive.
- A group also defines the security model and security level for its users.

To check the existing SNMP configuration, use these commands:

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

To set the SNMPv3 *server group* and *server users* parameters on a router, execute the following steps:

	Command	Description
Step 1	`> telnet router_name`	Telnet to the router you want to configure.
Step 2	`Router> enable` `Router> enable_password`	Enter enable mode, then enter the enable password.
Step 3	`Router# configure terminal`	Enter global configuration mode.
Step 4	`Router(config)# snmp-server group` [*groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}] [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	The **snmp-server group** command configures a new SNMP group or a table that maps SNMP users to SNMP views. Each group belongs to a specific security level. Example: **snmp-server group v3auth v3 auth read v1default write v1default**
Step 5	`Router(config)# snmp-server user` *username* [*groupname* **remote** *ip-address* [**udp-port** *port*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {md5 | **sha**} *auth-password* [**priv des56** *priv-password*]] [**access** *access-list*]	The **snmp-server user** command configures a new user to an SNMP group. Example: **snmp-server user user1 v3auth v3 auth md5 user1Pass**
Step 6	`Router(config)# Ctrl+Z`	Return to Privileged Exec mode.
Step 7	`Router# copy running startup`	Save the configuration changes to NVRAM.

Enabling SA Agent on Edge Device Routers

If you want to collect SLA data from the edge devices in your network, you must enable SA Agent on each device from which you want to collect this data.

Note This procedure assumes that you have already enabled SNMP and set the SNMP parameters on the edge device router, as described in the previous sections of this chapter.

To enable SA Agent on an edge device router, execute the following steps:

	Command	Description
Step 1	`> telnet router_name`	Telnet to the router you want to configure.
Step 2	`Router> enable` `Router> enable_password`	Enter enable mode, then enter the enable password.
Step 3	`Router# configure terminal`	Enter global configuration mode.
Step 4	`Router(config)# rtr responder`	Enable SA Agent on the SLA probe's target router.
Step 5	`Router(config)# Ctrl+Z`	Return to Privileged Exec mode.
Step 6	`Router# copy running startup`	Save the configuration changes to NVRAM.

Enabling TFTP on the VPN Solutions Center Workstation

The VPN Solutions Center software in MPLS mode is set by default to use TGS_TELNET to transport configuration files to and from routers. To set VPN Solutions Center software to use TGS in TFTP mode instead, edit the *csm.properties* file as described below. Changing this value in the *csm.properties* file sets the default download mechanism for all the targets defined in the VPN Solutions Center Repository.

Note Setting the transport method in the VPN Console overrides the transport method setting in the *csm.properties* file. For instructions, see the "Specifying the Transport Method" section on page 2-29.

Step 1 On the VPN Solutions Center workstation, log in as the *vpnadm* administrative user.

Step 2 Go to the */opt/vpnadm/vpn/etc* directory (or wherever the */vpn* directory is installed).

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

Step 4 Find the following line in the *csm.properties* file:

```
netsys.gtl.transportMechanism = TGS_TELNET
```

Step 5 Change the `TGS_TELNET` value as follows:

```
netsys.gtl.transportMechanism = TGS_TFTP
```

Step 6 To specify the TFTP server IP address:

a. Find the **netsys.tgs.myTftpServer** property.

b. Specify the IP address of the VPN Solutions Center workstation.

Step 7 Save your changes and exit from the file.

Setting a Local Solaris Host as a TFTP Server

This section describes how to set up a local Solaris host as a TFTP server. If the VPNSC Network Management Subnet includes one or more Telnet Gateway servers, you must set up the VPN Solutions Center workstation and the Telnet Gateway servers as TFTP hosts.

To set up a local Solaris host as a TFTP server, follow these steps:

Step 1 Open a new terminal window on the local host machine.

Step 2 Log in as the **root** user.

Step 3 With a text editor, open the */etc/inetd.conf* file.

Step 4 Find the following line in the file:

```
#tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

Step 5 To activate the statement, delete the pound symbol (#) at the beginning of the line.

Step 6 Save the change and exit from the *inetd.conf* file.

Step 7 At the terminal window command line, issue the following command to see if *inetd* processes are running:

```
ps -ef | grep inetd
```

The output of this command is as follows:

```
root <pid> 1 0 <date> <time> /usr/sbin/inetd -s
```

where *pid* is the process ID for the inetd process.

Step 8 If the process is running, send the SIGHUP (hang-up) signal to the inetd daemon with this command:

```
kill -1 <pid>
```

If the inetd daemon process is not running, start the inetd daemon.

Step 9 Exit from the terminal window.

Setting Up VPN Solutions Center 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 VPN Solutions Center for collecting router configuration files, implement the following tasks:

- 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

Setting Up Connectivity to a Remote Telnet Gateway Server

When you install the VPN Solutions Center software on the VPNSC workstation, the installation includes a Telnet Gateway server (TGS). The VPN Solutions Center uses TGS for all communication with routers, including downloading and uploading configuration files (with the exception of SNMP communications, which are handled through the poller server).

Service providers can install multiple Telnet Gateway servers, either in the same network that VPN Solutions Center resides in, or on a remote network. However, installing the TGS servers on a remote network requires that TIBCO event connectivity between the VPNSC network and the remote network must be in place.

If you install multiple Telnet Gateway servers on the LAN connected to the VPN Solutions Center workstation (which is called the *VPNSC Network Management Subnet*), no special setup is required. However, if you want to install and use TGS on remote networks, the *TIBCO rvrd* software must be properly configured on both the VPN Solutions Center workstation and on one TGS machine in each remote network.

Note Even if a remote network contains multiple Telnet Gateway servers running on multiple machines, only one instance of TIBCO rvrd needs to run on that network.

Before You Begin the Setup Process

If VPN Solutions Center is currently running, you must bring it down before proceeding with the remote TGS setup procedure.

Step 1 Bring down VPN Solutions Center as described in the "Shutting Down the VPN Solutions Center Software" section on page 3-7.

Step 2 Check to see if the TIBCO software is already running:

```
ps -A | grep rv
```

Step 3 If TIBCO rvd or rvrd processes are running, kill them.

Step 4 Complete the TIBCO connectivity setup procedure on the VPN Solutions Center workstation and on the remote TGS machine as described in the following sections.

Setting Up the VPNSC Workstation for Connectivity to the Remote TGS Host

To set up the VPN Solutions Center workstation to allow TIBCO event connectivity to a TGS host in a remote network, follow these steps.

You must complete this procedure before you start the Watch Dog, bring up the VPN Solutions Center software, and start TGS on the VPN Solutions Center workstation.

Note On the VPN Solutions Center workstation, this is a one-time procedure. If you need to add additional remote TGS server machines, you do not need to repeat this procedure on the VPN Solutions Center workstation.

Step 1 On the VPN Solutions Center workstation, change directories to the */opt/vpnadm/vpn* directory.

Step 2 Issue the following command to source the environment:

```
source vpnenv.csh
```

Step 3 Check to see if the TIBCO software is already running:

```
ps -A | grep rv
```

Step 4 If any **rvd** or *rvrd* processes are running, kill them.

Step 5 Issue the following command:

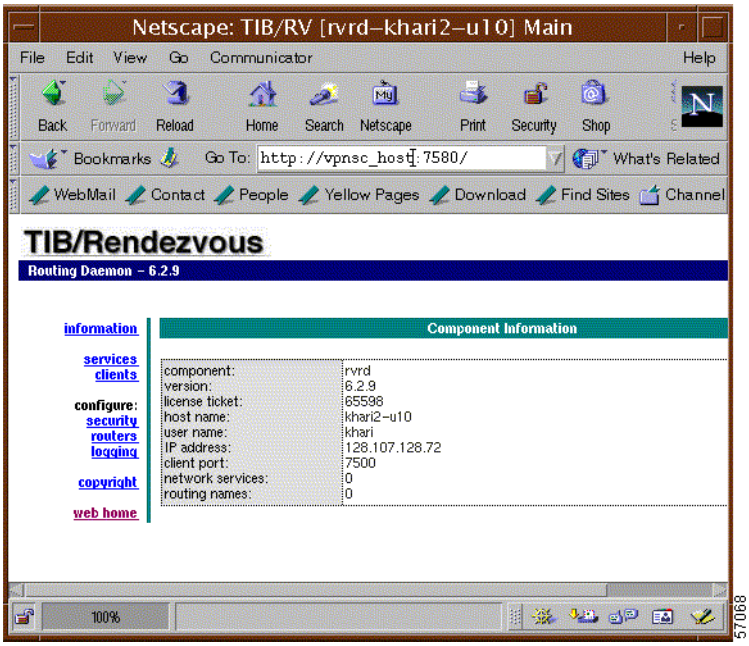
```
rvrd -store rvrd.store
```

Step 6 Start Netscape and go to the following URL, where "*VPNSC_hostname*" is the hostname of the VPN Solutions Center workstation:

http:*VPNSC_hostname***:7580**

The TIB/Rendezvous home page appears (see Figure 2-5).

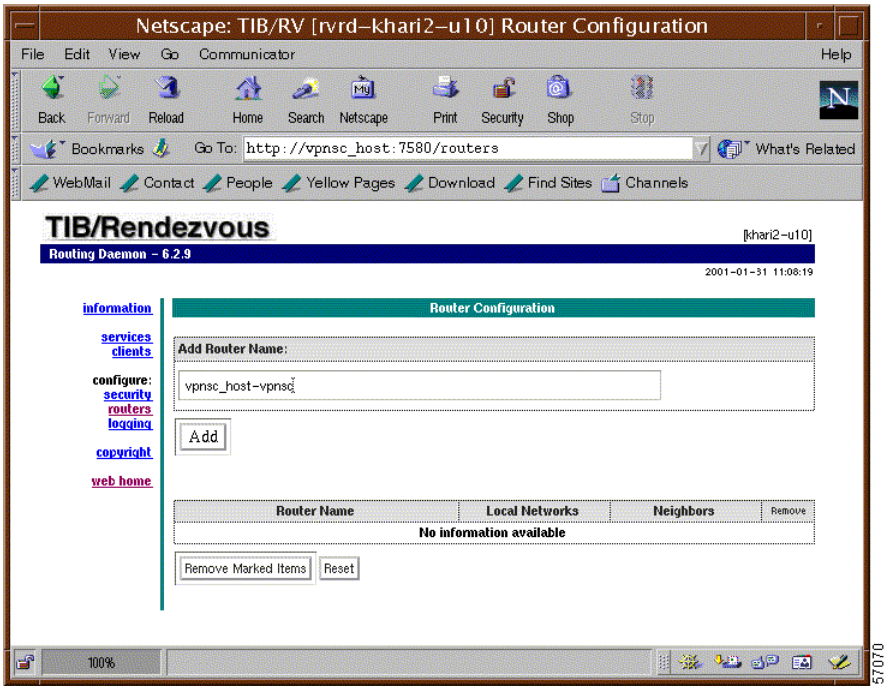
Figure 2-5 TIBCO/Rendezvous Home Page



Step 7 From this page, choose the **routers** link.

The dialog box shown in Figure 2-6 appears.

Figure 2-6 Entering the VPNSC Host Name



Step 8 In the *Add Router Name* field, enter the name of the VPN Solutions Center workstation followed by "**-vpnsc**," as follows: *VPNSC_host*-**vpnsc**.

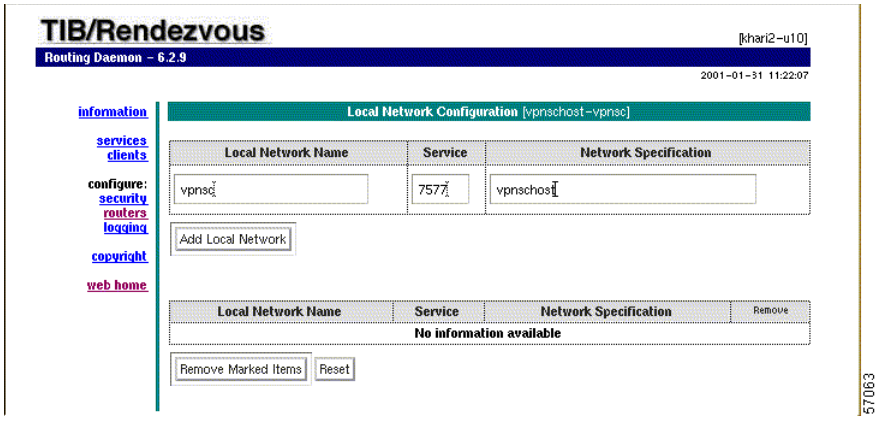
Step 9 Click **Add**.

The value you entered is now displayed in the Router Name column.

Step 10 In the Local Networks column, select the current entry in the field.

The dialog box shown in Figure 2-7 appears.

Figure 2-7 Entering the VPNSC Local Network Information



Step 11 Specify the local VPNSC network with the following values:

a. In the *Local Network Name* field, enter this value:

vpnsc

b. In the *Service* field, enter the TIBCO port number used for this VPN Solutions Center installation.

c. In the *Network Specification* field, enter the name of the VPNSC workstation.

Step 12 When the VPNSC network fields are specified, click **Add Local Network**.

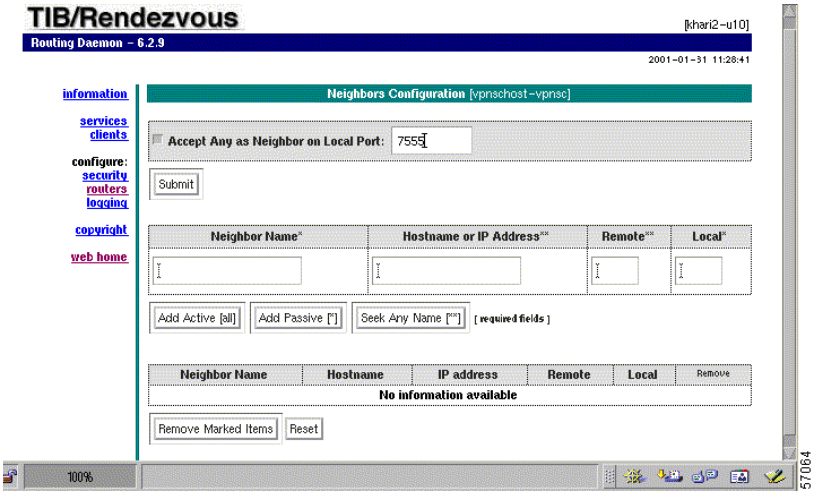
On the lower section of the page, the values you entered are now displayed in the corresponding cells.

Step 13 From the current dialog box, choose the **routers** link.

Step 14 Click the current entry in the Neighbors column.

The dialog box shown in Figure 2-8 appears.

Figure 2-8 Entering the VPNSC Neighbor Information



Step 15 Click the **Accept Any Neighbor on Local Port** option.

Step 16 In the *Local Port* option field, enter the following value:

```
7555
```

Step 17 Click **Submit**.

Step 18 From the current dialog box, choose the **routers** link.

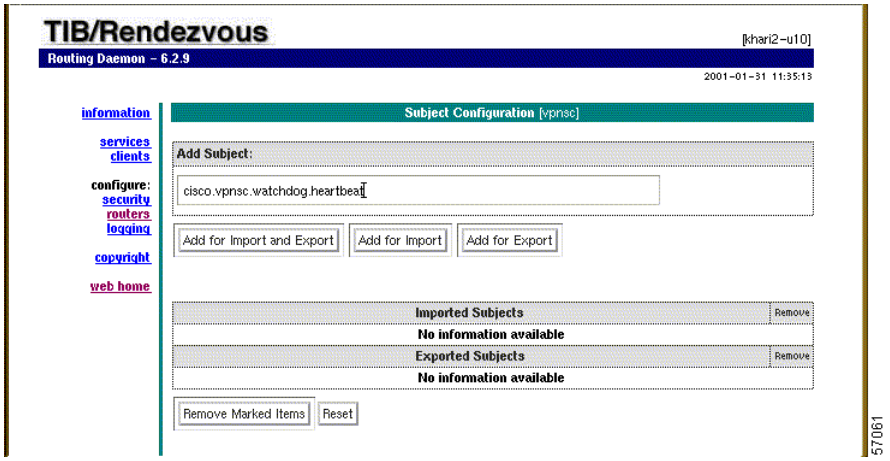
Step 19 Click the current entry in Local Networks column.

The dialog box updates to the screen shown in Figure 2-7 on page 2-16. Notice that "**vpnsc**" is now displayed in the Local Network Name column.

Step 20 In the Local Network Name column, click the **vpnsc** entry.

The dialog box shown in Figure 2-9 appears.

Figure 2-9 Entering the VPNSC Neighbor Information



Step 21 In the *Add Subject* field, enter the following subject for import:

```
cisco.vpnsc.watchdog.heartbeat
```

Step 22 Click **Add for Import**.

The import subject you entered is now displayed in the *Imported Subjects* field.

This completes the procedure for setting up the for connectivity to the remote TGS host from the VPN Solutions Center workstation.

Enabling TIBCO Event Connectivity on the Remote TGS Host

To enable TIBCO event connectivity between a Telnet Gateway Server host on a remote network and the VPN Solutions Center workstation, follow these steps. This procedure assumes that TGS is installed on the Telnet Gateway Server host.

Note You must complete this procedure before you start TGS and before you start the VPN Solutions Center software.

In the following procedure, "*TGS_host*" refers to the hostname of the machine on which you are configuring the TIBCO rvrd software.

Step 1 On the remote Telnet Gateway Server host, change directories to the */opt/vpnadm/vpn* directory.

Step 2 Issue the following command to source the environment:

```
source vpnenv.csh
```

Step 3 Check to see if the TIBCO software is already running:

```
ps -A | grep rv
```

Step 4 If any TIBCO *rvd* or *rvrd* processes are running, kill them.

Step 5 Issue the following command:

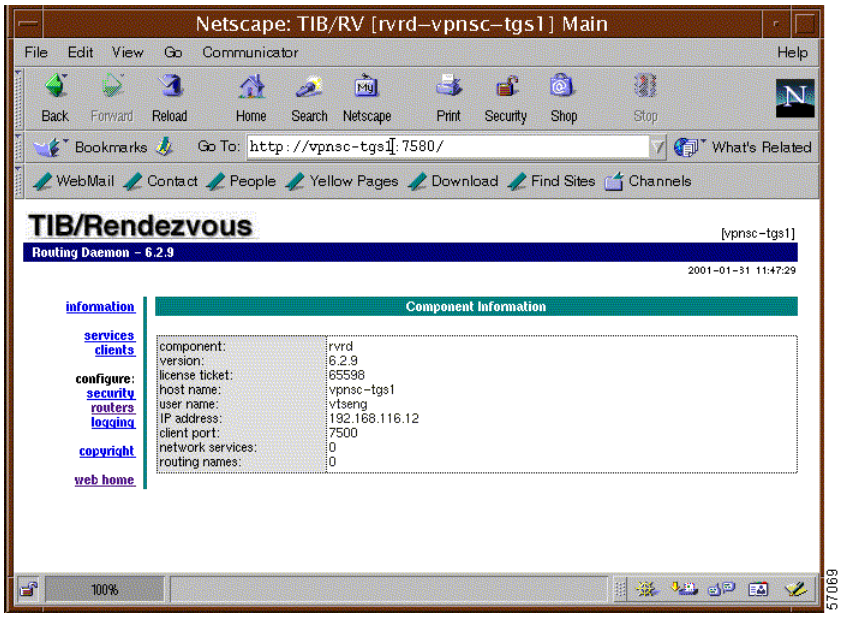
```
rvrd -store rvrd.store
```

Step 6 Start Netscape and go to the following URL, where "*TGS_hostname*" is the hostname of the Telnet Gateway Server installation:

http:*TGS_hostname***:7580**

The TIB/Rendezvous home page appears (see Figure 2-10).

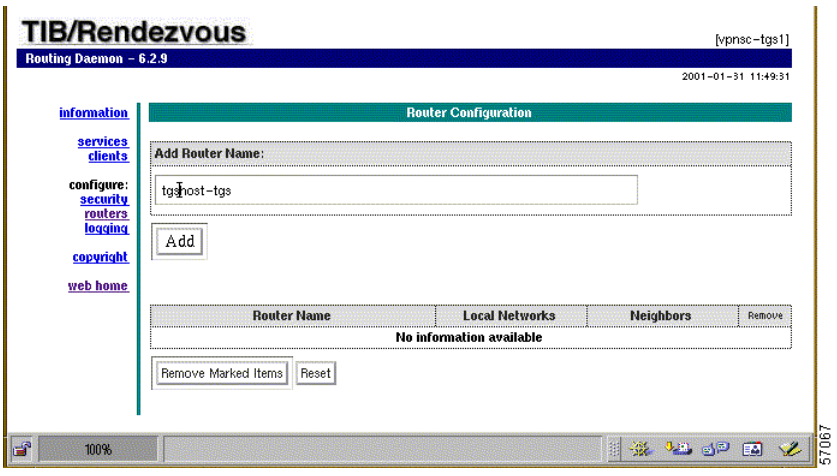
Figure 2-10 TIBCO/Rendezvous Home Page



Step 7 From this page, choose the **routers** link.

The dialog box shown in Figure 2-11 appears.

Figure 2-11 Entering the TGS Host Name



Step 8 In the *Add Router Name* field, enter the name of the TGS host followed by "**-tgs**," as follows: *TGS_host***-tgs**.

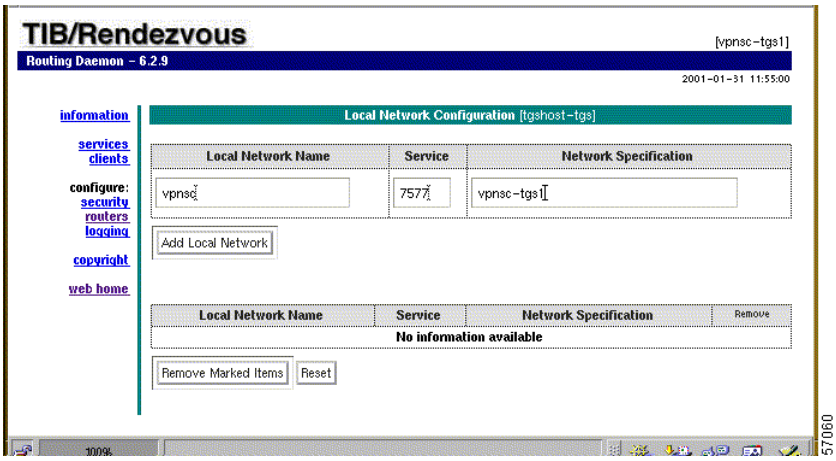
Step 9 Click **Add**.

The TGS host name is displayed in the Router Name column.

Step 10 In the Local Networks column, select the current entry in the field.

The dialog box shown in Figure 2-12 appears.

Figure 2-12 Entering the TGS Local Network Information



Step 11 Specify the local TGS network with the following values:

a. In the *Local Network Name* field, enter this value:

`vpnsc`

b. In the *Service* field, enter the TIBCO port number used for this installation.

The port number entered here should be same TIBCO port number entered in Step 11-b in the previous procedure to set up the VPNSC workstation for connectivity to the remote TGS host (see Figure 2-7 on page 2-16).

c. In the *Network Specification* field, enter the name of the TGS host.

Step 12 When the VPNSC network fields are specified, click **Add Local Network**.

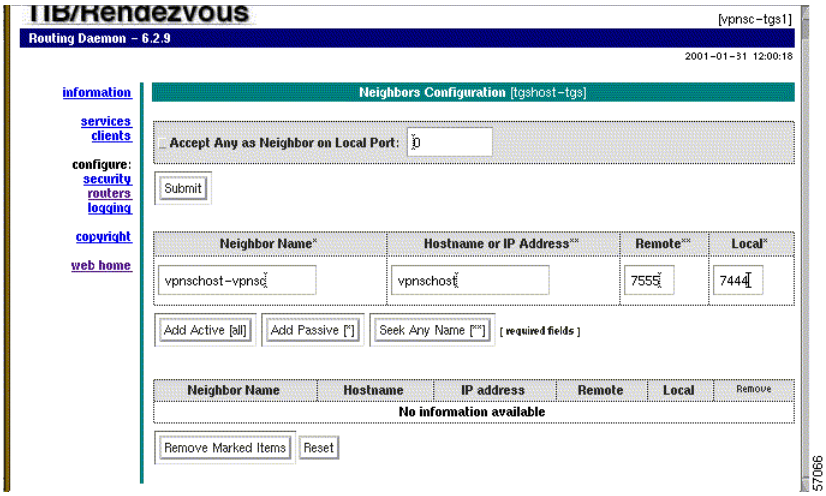
On the lower section of the page, the values you entered are now displayed in the corresponding cells.

Step 13 From the current dialog box, choose the **routers** link.

Step 14 Click the currently displayed entry in the Neighbors column.

The dialog box shown in Figure 2-13 appears.

Figure 2-13 Entering the Telnet Gateway Server Neighbor Information



Step 15 Enter the TGS Neighbor information with these values:

a. In the *Neighbor Name* field, enter the name of the VPNSC workstation, followed by **-vpnsc**: *VPNSC_host***-vpnsc**

b. In the *Hostname or IP Address* field, enter the name of the VPNSC workstation.

c. In the *Remote* field, enter the following value:

7555

d. In the *Local* field, enter the following value:

7444

Step 16 Click **Add Active [all]**.

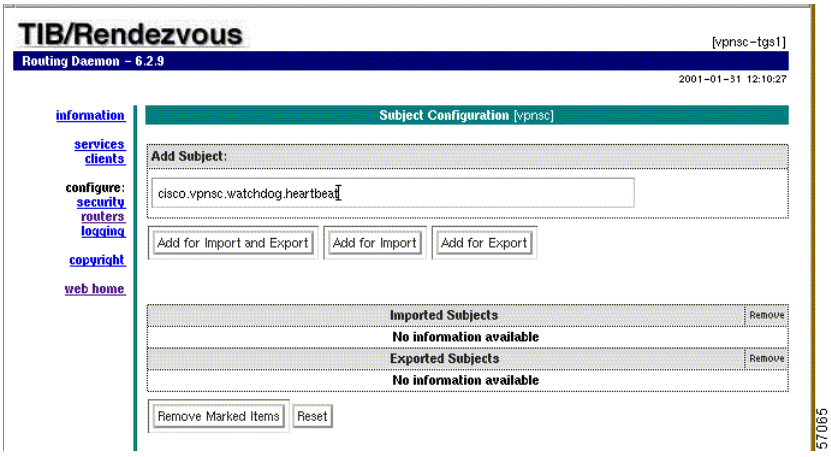
Step 17 From the current dialog box, choose the **routers** link.

Step 18 Click the currently displayed entry in Local Networks column.

Step 19 In the Local Network Name column, click the **vpnsc** entry.

The dialog box shown in Figure 2-14 appears.

Figure 2-14 Entering the Export Object Information



Step 20 In the *Add Subject* field, enter the following subject for export:

```
cisco.vpnsc.watchdog.heartbeat
```

Step 21 Click **Add for Export**.

The export subject you entered is now displayed in the *Exported Subjects* field.

This completes the procedure for setting up the for connectivity to the VPNSC workstation on the remote TGS host.

Step 22 Start the VPN Solutions Center software as described in the "Starting the VPN Solutions Center Software" section on page 2-1.

Step 23 Start the TGS software as described in the "Starting the Telnet Gateway Server Software and the Watch Dog" section in Chapter 3 of the *VPN Solutions Center Installation Guide*.

Modifying Frame Relay LMI Types

Local Management Interface (LMI) is a signalling standard between the router and the Frame Relay switch that provides a Frame Relay management mechanism. The LMI type must match the type used by the network. Changing the LMI type is a global change that affects all service requests (for related information, see the next section, "Applying a Mixed Set of LMI Types").

If a Service Provider or Customer needs to modify the Frame Relay Local LMI types, they can do so by modifying the appropriate property in the *csm.properties* file. Changing the LMI type in this way applies the Frame Relay modification to the Customer Edge router (CE) only.

You can set the LMI type to any one of four values:

LMI Value	Description
ansi	Annex D defined by ANSI standard T1.617
cisco	LMI type defined jointly by Cisco and other companies.
none	This is the default.
q933a	ITU-T Q.933 Annex A

To modify the LMI type in the *csm.properties* file, follow these steps:

Step 1 On the VPN Solutions Center workstation, log in as the **vpnadm** user.

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 line in the *csm.properties* file:

```
netsys.watchdog.server.CVPIMServer.frameRelayLmiType = none
```

Step 5 Change the *none* value to the appropriate LMI type value. For example, to change the LMI type to **cisco**, you would edit the line as follows:

```
netsys.watchdog.server.CVPIMServer.frameRelayLmiType = cisco
```

Step 6 Save your changes and exit the file.

Step 7 Log out (exit) from the **vpnadm** user.

Applying a Mixed Set of LMI Types

Changing the LMI type is a global change that affects all active service requests. To apply a mixed set of LMI types, do the following:

Step 1 Modify the *csm.properties* file to set the desired LMI type as described in the previous section.

Step 2 In the VPN Console, deploy the service requests that are associated with the LMI value set in Step 1.

Step 3 Modify the *csm.properties* file again to set the desired LMI type for the next set of service requests.

Step 4 In the VPN Console, deploy the service requests that are associated with the LMI value set in Step 3.

Specifying the TFTP Server Address for the TGS Host

If the TGS hosts in the VPNSC Network Management Subnet are also TFTP servers, you must set the appropriate property in the *csm.properties* file on those TGS hosts.

Step 1 On the local TGS host, log in as the *vpnadm* administrative user.

Step 2 Go to the */opt/vpnadm/vpn/etc* directory (or wherever the */vpn* directory is installed).

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

Step 4 Find the following line in the *csm.properties* file:

```
netsys.tgs.myTftpServer=
```

Step 5 Enter the IP address of the local TGS host.

Step 6 Save your changes and exit from the file.

Setting Up the Network in the VPN Solutions Center Software

In this product, an MPLS VPN *network* is a unique group of *targets*; a target can be a member of only one network. Thus, an MPLS VPN network allows a provider to partition the working space into manageable segments that are unique and do not overlap other networks.

To use VPN Solutions Center to set up an MPLS VPN network requires the following tasks:

1. Define the target routers—see the next section, "Defining the Target Routers in the MPLS Networks."
2. Define the Provider Administrative Domain —see the "Defining Provider Administrative Domains" section on page 2-51.
3. Create a VPN customer definition for each VPN customer—see the "Creating a VPN Customer Definition" section on page 3-1.
4. Define a VPN—see the "Defining a New VPN in the VPNSC Software" section on page 3-14.
5. If you are using a management VPN to manage your customers' VPNs, define a management VPN—see the "Implementing the Management VPN Technique" section on page 3-23.

Caution Regarding the File Descriptor Setting on the VPN Solutions Center Workstation

Defining the Target Routers in the MPLS Networks

Every device that the VPN Solutions Center software manages must be defined as a *target*. A target is any device from which the VPN Solutions Center software can collect information (a router or Netflow Collector). In most cases, these targets are Cisco routers that function either as a provider edge router (PE) or a customer edge router (CE).

Note When you define target names in the VPN Solutions Center software, the target names you specify must match the actual IOS host names of the corresponding devices.

Note The Simple Network Management Protocol (SNMP) must be configured on each PE router and CE router in the service provider network. To determine whether SNMP is enabled and set the SNMP community strings on a router, see the "Setting Up SNMPv1 and SNMPv2 on the Routers in the Service Provider Network" section on page 2-8 and the "Setting the SNMPv3 Parameters on the Routers in the Service Provider Network" section on page 2-9.

There are two methods for defining targets and organizing them into the appropriate networks (or target groups):

- Importing all the pertinent router configuration files
- Defining individual targets manually

  You can define targets manually when you want to create, edit, or delete targets in a network. See the "Adding a New Router to the Network" section on page 2-36.

Importing Router Configuration Files

Importing your router configuration files into the VPN Solutions Center software is a quick way to define the MPLS VPN networks and the targets in them. This method lets you specify a directory of router configuration files and the network for these routers. The network and the targets in the network are created based on the imported configuration files.

When employing this method, note that not all the necessary information is present after you import the files. You must then proceed to define the additional target information, such as the IP addresses, passwords, and so forth (described later in this document).

When you import router configuration files in VPN Solutions Center, this task does not create new target entries in the Repository—it only adds new datasets for existing targets.

To import router configuration files, follow these steps:

Step 1 Create a directory of configuration files for a given set of devices and copy the appropriate configuration files into the directory.

Device names within each directory must be unique.

A typical set includes Provider and Customer edge routers (PEs and CEs).

Step 2 From the VPN Console menu, choose **Setup > Create Targets From Router Configurations**.

An informational window displays the following information:

This will create targets based on the router configuration files in a specified directory. A network will be created for the new targets.

You will be asked to enter the following information:

- Directory containing the router configuration files

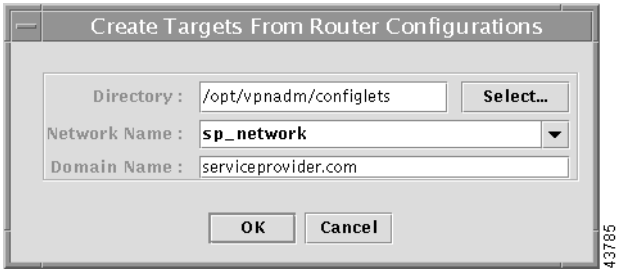
  The default convention for naming configuration files is *device_name.domain_name.com*. But adherence to this nomenclature is not required.
- Network name for the new targets
- Domain name for the targets (optional)

  Specifying the domain name is necessary only if a fully domain-qualified hostname is needed to resolve the IP address of the target (router).

Step 3 Click **OK**.

The Create Targets From Router Configurations dialog box appears (see Figure 2-15 on page 2-25).

Figure 2-15 Creating Targets From Router Configuration Files



Step 4 Enter the directory path, network name, and (optionally) the domain name; then click **OK**.

a. The directory path is the path to the router configuration files.

To browse for the directory path, click **Select** and choose the appropriate directory.

b. The *Network Name* field includes a drop-down list that provides all the currently defined networks. To select the network name from the list, click the **Down Arrow** icon, then select the appropriate network name.

   The network name should reflect the customer's name and the provider's Region that the customer is assigned to. For a discussion of Regions, see the "Defining Provider Administrative Domains" section on page 2-51.

c. The domain name indicates the service provider's domain.

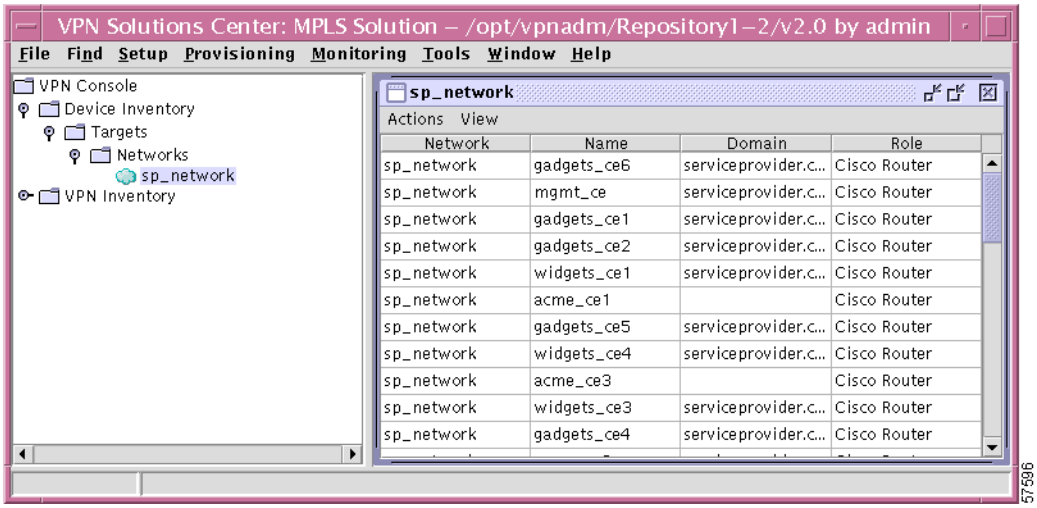
Caution It is important to understand that when you specify both the domain name of a device and the IP address of a device, *the IP address overrides the specified domain name*.

The VPN Solutions Center software imports the router configuration files from the indicated directory. For every valid configuration file, the VPN Solutions Center software creates a target, and defines the target's role as *Cisco router*. A *valid* configuration file is one in which the *hostname statement* is present in the file. If a configuration file does not contain the hostname statement, VPN Solutions Center software regards the file as invalid and does not import the configuration file into the Repository.

Under the Networks folder in the hierarchy pane, the product software adds the network name you specified.

Step 5 To display the window that lists the targets in a network, double-click the network name in the hierarchy pane. The product displays the Network window, as shown in Figure 2-16 on page 2-26.

Figure 2-16 The Network Window



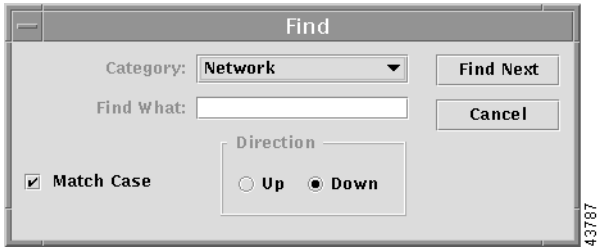
Finding a Specific Network

To find a specific network, follow these steps:

Step 1 From the VPN Console window, choose **Find > Find Network**.

The Find dialog box appears with the category *Network* already selected (see Figure 2-17).

Figure 2-17 Find Network Dialog Box



Step 2 In the *Find What* field, enter the name of the network you want to find.

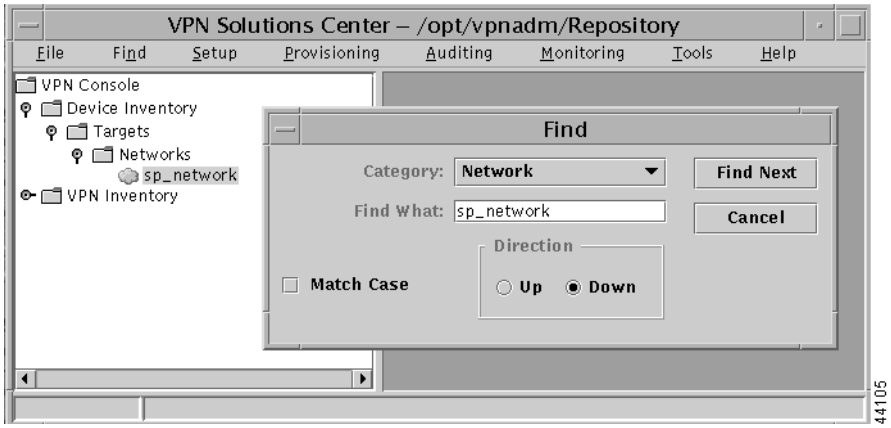
Step 3 If you want the search to match the case of the network name you enter, check the **Match Case** check box.

Step 4 Choose the direction of the search by clicking the **Up** or **Down** radio button.

Step 5 When you have completed the search parameters, click **Find Next**.

The VPNSC software locates the indicated network and highlights it in the hierarchy pane, as shown in Figure 2-18.

Figure 2-18 Network Found in VPNSC Hierarchy Pane



Step 6 Close the Find window.

Completing the Target Information for Multiple Targets

Now that you have imported the router configuration files and assigned them to an MPLS VPN network (*sp_network* in our example), you have completed the initial phase required to define the targets. Now you must enter the rest of the information the product software requires to implement the targets.

Step 1 From the hierarchy pane, click the open-close icon for the Networks folder.

Step 2 Double-click the desired network from the list of networks.

As shown in Figure 2-16 on page 2-26, the Network window appears in the data pane on the right, displaying the name of each router in the selected network, along with its domain name and role (in this case, Cisco Router).

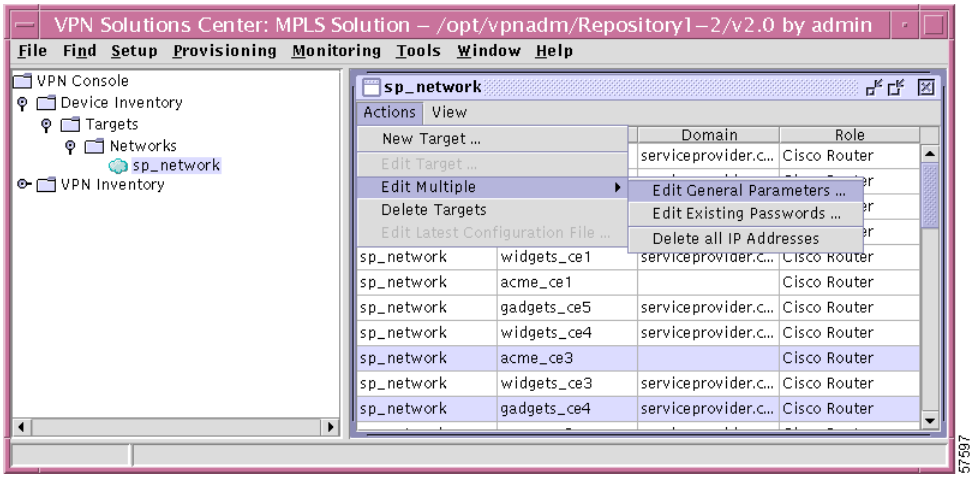
At this point, you have the option to enter information for a single target (router) or multiple targets. If the targets share some characteristics, such as the same login or enable passwords, you can define those parameters once for multiple routers, then return to the Network window to edit individual targets for those parameters that are unique for each router. This is the procedure described in the following steps.

Step 3 Select the routers from the list for which you want to define the common parameters.

To select multiple targets from the list, hold down the **Ctrl** key while you click the desired targets.

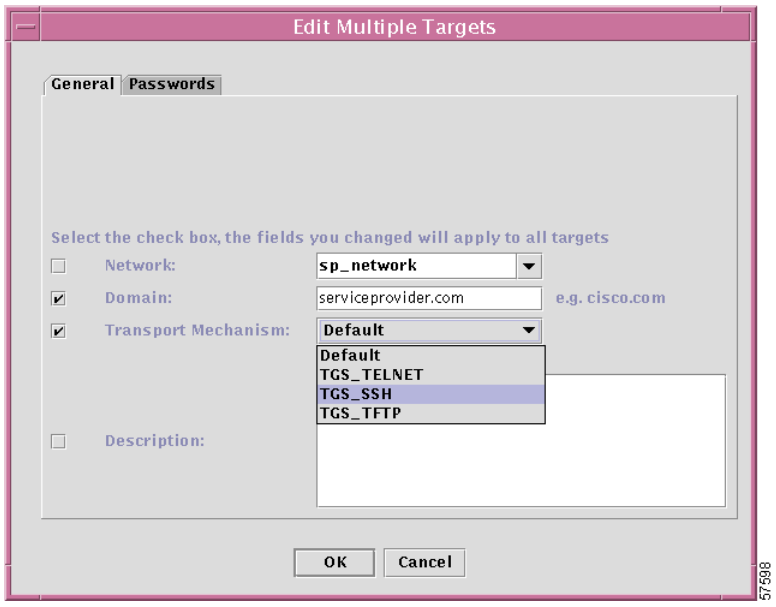
Step 4 From the Network window, choose **Actions > Edit Multiple > Edit General Parameters** (as shown in Figure 2-19 on page 2-28).

Figure 2-19 The Network Window's Action Menu



The General tab for the Edit Multiple Targets dialog box appears (see Figure 2-20).

Figure 2-20 Entering General Information for Multiple Targets



Step 5 In this dialog box, select the check boxes for the fields you want to apply to all the selected targets: *Network*, *Domain*, *Transport Mechanism*, and *Description*. Entering information in the *Description* field is optional (but recommended).

Step 6 Choose the desired network name from the *Network* field drop-down list.

Step 7 Enter the domain name.

Caution When you specify both the domain name of the device and the IP address of a device, *the IP address overrides the specified domain name*.

Specifying the Transport Method

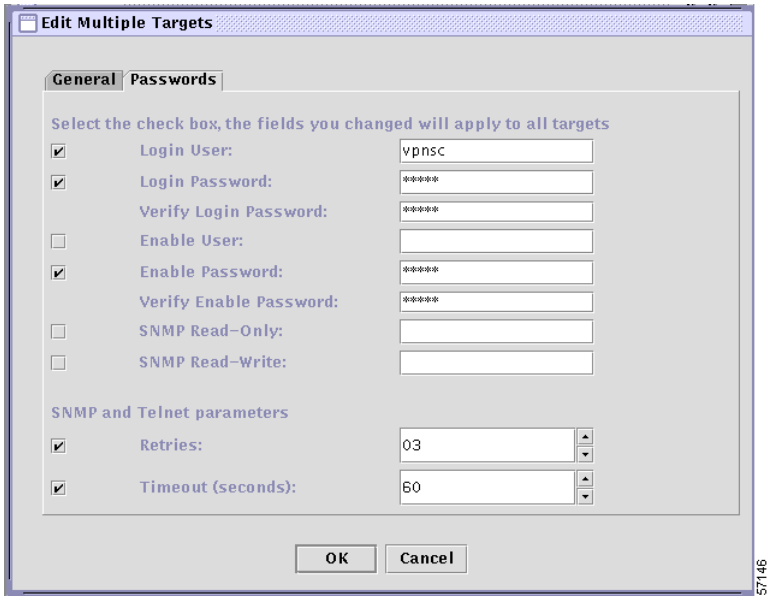
Step 8 From the **Transport** drop down menu, choose the configuration file transport method you are using.

- *TGS_Telnet*: The *TGS_Telnet* option is the default transport method for MPLS VPNs.
- *TGS_SSH*: The configuration file transport method for VPN Solutions Center IPsec mode is *TGS_SSH* (Telnet Gateway Server—Secure Shell).
- *TGS_TFTP*: If you choose TGS_TFTP as the default transport method, be sure to enable TFTP (Trivial File Transfer Protocol) on the VPN Solutions Center workstation and on the target routers.

  For details, see the "Enabling TFTP on the VPN Solutions Center Workstation" section on page 2-11.

Step 9 Choose the **Passwords** tab (as shown in Figure 2-21).

Figure 2-21 Entering Passwords and SNMP Community Strings for Multiple Targets



Step 10 In the Passwords dialog box, click the check boxes for the fields you want to apply to all the selected targets (routers).

In this example, we have not specified a value for the *Login User* field, reserving that value for individual router configuration.

Step 11 Specify the information for the following fields, then click **OK**.

a. *Login Password*

The Login password is the virtual terminal password, which establishes password protection on incoming Telnet sessions.

Caution VPN Solutions Center requires that the PEs and managed CEs in the network have a virtual terminal (login) password. The data collection operation fails if VPN Solutions Center does not find the login password set on a router it is collecting data from.
If you have not yet set the login password on the router and in this dialog box, please do so now.

b. *Enable User*

c. *Enable Password*

d. *SNMP Read-Only* and *SNMP Read-Write* community strings

Note The SNMP community strings must be set on all the PEs and CEs in the service provider's network; the SNMP settings on the routers must match the settings configured here. For related information, see the "Setting Up SNMPv1 and SNMPv2 on the Routers in the Service Provider Network" section on page 2-8 and the "Setting the SNMPv3 Parameters on the Routers in the Service Provider Network" section on page 2-9.

e. *SNMP and Telnet retries*

The recommended setting is three (3) retries.

f. *SNMP and Telnet timeout*

The recommended setting is 30 seconds.

When you click **OK**, you return to the Network window.

Completing the Target Information for Individual Targets

Now that you have defined the parameters that apply to all the selected targets, you can proceed to define the elements that must be defined for each target: user names and IP addresses.

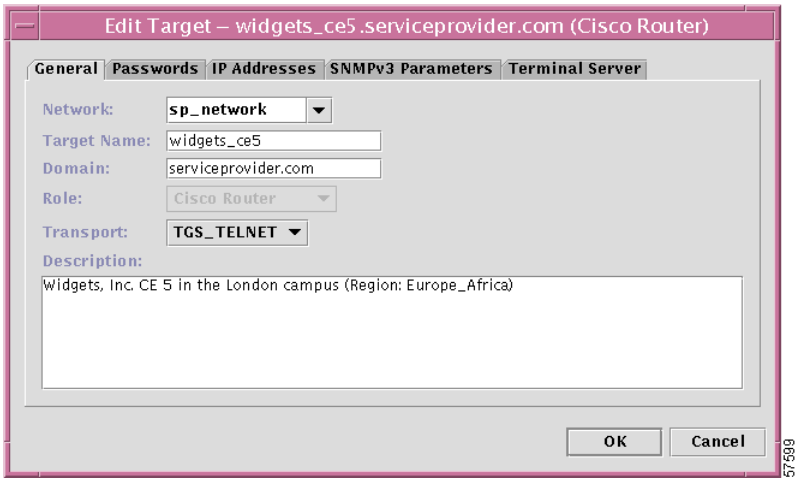
Caution It is important to understand that when you specify both the domain name of the device and the IP address of a device, *the IP address overrides the specified domain name*.

Step 1 From the Network window, select the target you want to edit.

Step 2 Choose **Actions > Edit Target**.

The Edit Target dialog box appears (see Figure 2-22).

Figure 2-22 The Edit Target Dialog Box

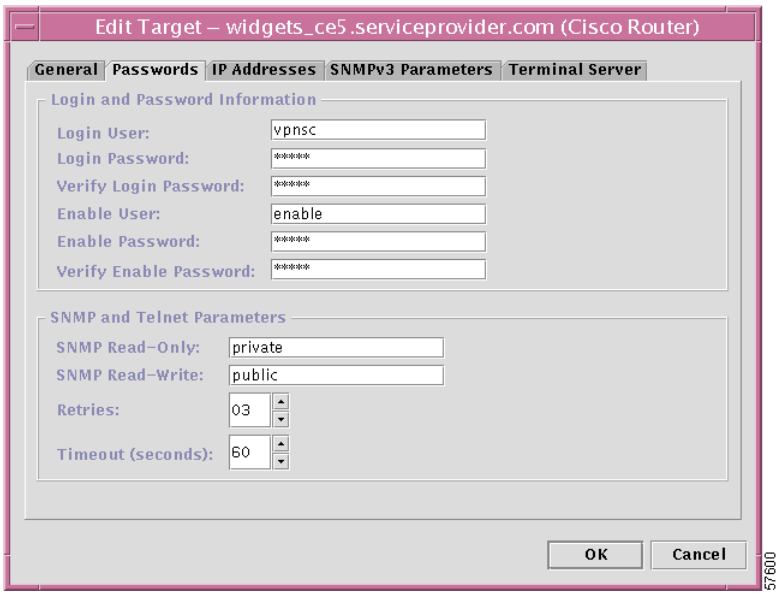


Step 3 If the *Transport* field is not already set to **TGS_TELNET**, set it now.

Defining the Passwords and SNMP Community Strings for Individual Targets

Step 1 From the **General** tab in the Edit Target dialog box, choose the **Passwords** tab (see Figure 2-23).

Figure 2-23 Editing a Target's Password and SNMP Strings Information



As you can see in Figure 2-23, the fields you defined for multiple targets are displayed in the pertinent fields.

Step 2 Enter the information in the fields you need to define for the selected target (router).

Caution VPN Solutions Center requires that the PEs and managed CEs in the network have a virtual terminal (login) password. The data collection operation fails if VPNSC does not find the login password set on a router it is collecting data from.
If you have not yet set the login password on the router and in this dialog box, please do so now.

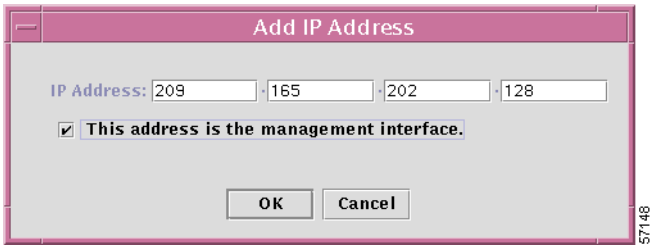
Entering a Target's IP Address Information

Caution When you specify both the domain name of a device and the IP address of a device, the IP address overrides the specified domain name.

Step 1 Choose the **IP Addresses** tab and click **Add**.

The Enter IP Address dialog box appears (see Figure 2-24).

Figure 2-24 Entering the IP Address



Step 2 Enter the IP address for the selected router.

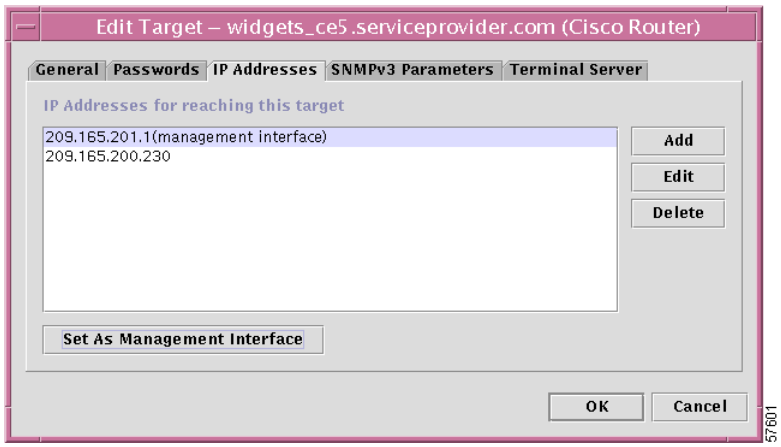
Step 3 If this address is the IP address for the management interface, check the **This address is the management interface** checkbox, then click **OK**.

You return to the IP Addresses tab, where the IP address you entered is now displayed (see Figure 2-25).

Setting the Management Interface

The VPN Solutions Center Network Management Subnet resides inside the service provider network, and communicates with edge routers through an assigned *management interface*. Configuration changes are managed by VPN Solutions Center software and transported to the appropriate edge routers through the management interface.

Figure 2-25 Setting the Management Interface



Step 1 From the displayed list of IP addresses for reaching this target router, choose the IP address that VPN Solutions Center uses to communicate with this router.

Step 2 When the appropriate interface is highlighted, click **Set As Management Interface**.

The selected IP address in the list now displays with the designation “management interface”; for example:

```
192.168.115.85 (management interface)
```

Step 3 If the management interface for this device is set satisfactorily, click **OK**.

The change is added to the VPN Solutions Center Repository.

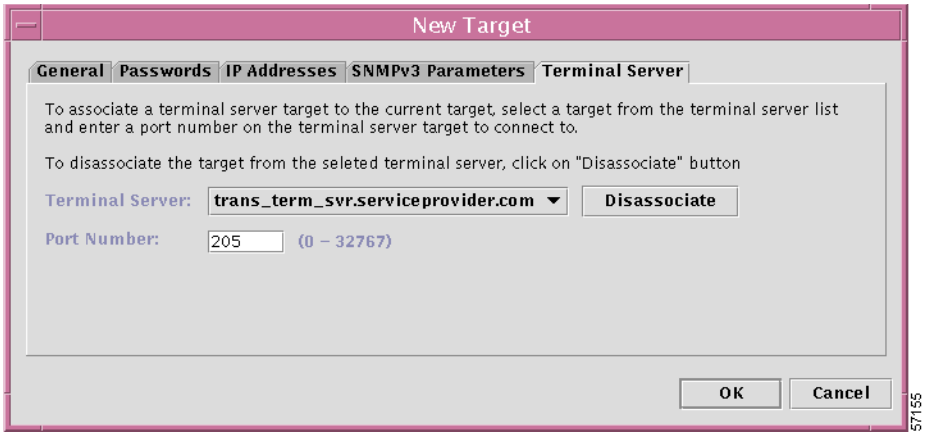
Assigning a Terminal Server to the Current Router

For information on defining a network device as a terminal server, see the "Defining Terminal Servers in VPN Solutions Center Software" section on page 2-41.

To assign a terminal server to the current router, follow these steps:

Step 1 From the Edit Target dialog box, choose the **Terminal Server** tab.

Figure 2-26 Choosing a Terminal Server for the Selected Router



Step 2 From the *Terminal Server* drop-down list, choose the name of the terminal server you want to associate with the current router.

- You can disassociate a terminal server from a device by clicking **Disassociate**.

Step 3 In the *Port Number* field, enter the port number on the terminal server that the server will use to access the router.

Step 4 When set to your satisfaction, click **OK**.

Updating Changed Router Passwords

If you change the passwords on any routers in the MPLS VPN network and you have already defined those passwords in the VPN Solutions Center software, you must update the password information so that they match.

To change the passwords defined for routers in the VPNSC software, follow these steps:

Step 1 From the hierarchy pane, click the open-close icon for the Networks folder.

Step 2 Double-click the desired network from the list of networks.

The Network window appears in the data pane on the right, displaying the name of each router in the selected network, along with its domain name and role (in this case, Cisco Router).

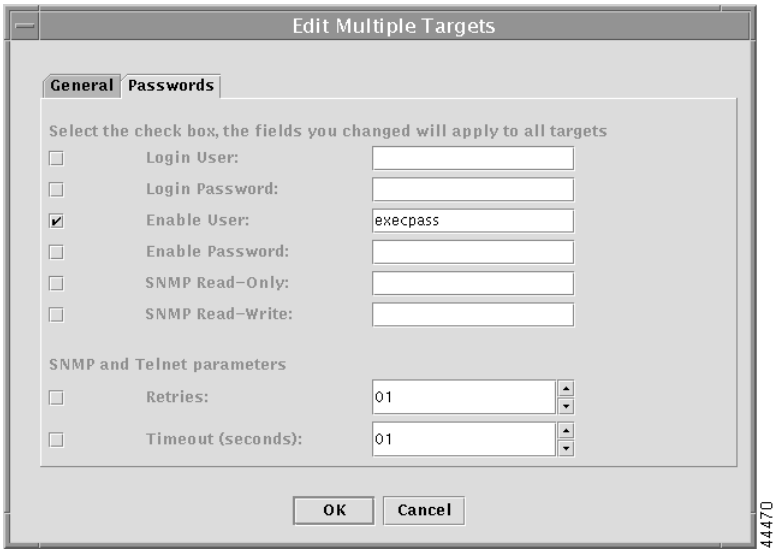
At this point, you have the option to change the passwords for a single target (router) or multiple targets. This procedure describes how to change the passwords for multiple routers at once.

Step 3 Select the routers from the list for which you want to change one or more passwords.

To select multiple targets from the list, hold down the **Ctrl** key while you click the desired targets.

Step 4 From the Network window, choose **Actions > Edit Multiple > Edit Existing Passwords**. The Edit Multiple Targets dialog box appears (see Figure 2-27).

Figure 2-27 Updating Router Passwords



Step 5 Check the checkboxes for the password(s) you want to change, then enter the new passwords.

Step 6 When the changes are complete, click **OK**.

Adding a New Router to the Network

In the event you need to add a new target (router) to an MPLS VPN network, follow these steps:

Step 1 In the VPN Console, open the Networks folder and select the pertinent network.

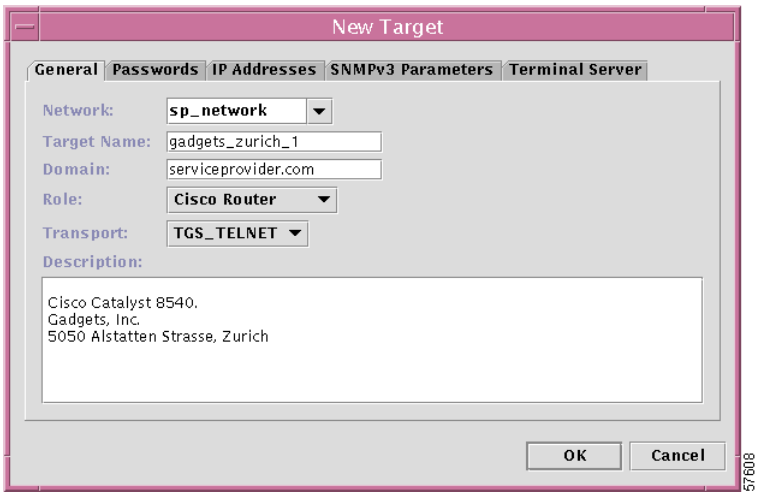
Step 2 Double-click the selected network.

The Network window appears, displaying the names and roles of the devices in the selected network.

Step 3 From the Network window, choose **Actions>New Target**.

The New Target dialog box appears (see Figure 2-28).

Figure 2-28 New Target Dialog Box for a Cisco Router



Enter the General Parameters for the New Target

Step 4 Enter the values for the parameters in the **General** dialog box.

a. From the *Network* drop-down list, select the network name.

b. In the *Target Name* field, specify the name of the router.

c. In the *Domain* field, specify the domain name for the device.

d. In the *Role* field, set the role to **Cisco Router**.

e. In the *Transport* field, choose **TGS_TELNET**.

The *Transport* field configures the method of communication between the VPN Solutions Center workstation and the specified router. The default is **TGS_TELNET** for MPLS operations.

f. In the *Description* field, enter any pertinent information about the router, such as the type of device, its location, and any other information that could be helpful to service provider operators.

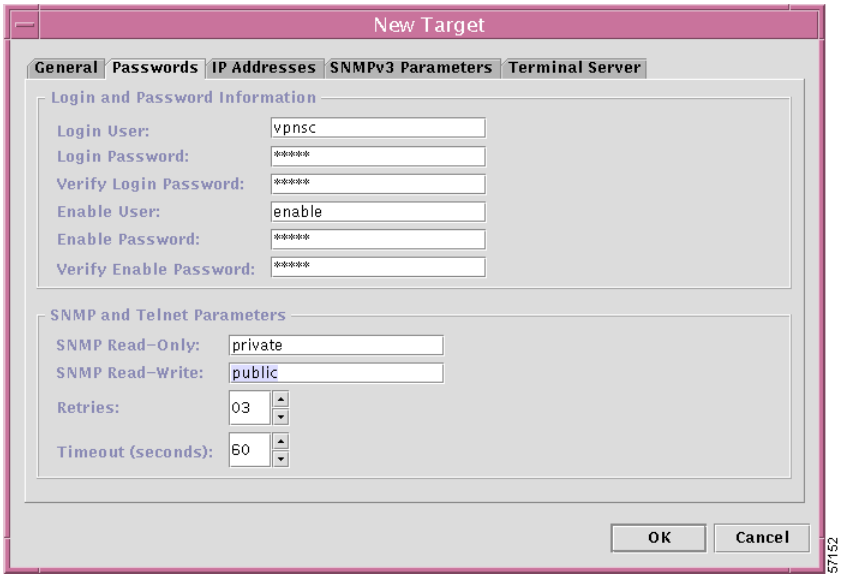
Specifying the Device Passwords and SNMP and Telnet Parameters

Step 1 Choose the **Passwords** tab.

The New Target Passwords dialog box appears (see Figure 2-29).

Note The values set in this dialog box must match the corresponding values set on the actual device.

Figure 2-29 New Target Passwords Dialog Box



Step 2 Enter the appropriate values for the fields in the **Passwords** dialog box.

a. Enter the *Login User* name.

b. Enter the *Login Password* for the device, then verify the password.

c. If the Enable User name exists on the device, enter it in the *Enable User* field.

d. If the Enable Password is set on the device, enter it in the *Enable Password* field.

e. Set the *SNMP Read-Only* and *SNMP Read-Write* community strings in the corresponding fields.

f. Set the SNMP and Telnet *Retries* value.The default is three retries.

g. Set the SNMP and Telnet *Timeout* value (in seconds). The default is 60 seconds.

Specifying IP Addresses and the Management Interface

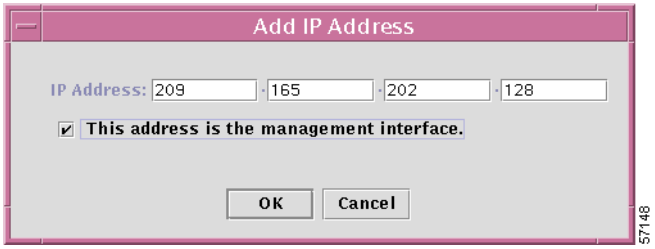
The VPN Solutions Center Network Management Subnet resides inside the service provider network, and communicates with edge routers through an assigned *management interface*. Configuration changes are managed by VPN Solutions Center software and transported to the appropriate edge routers through the management interface.

Step 1 Choose the **IP Addresses** tab.

Step 2 To specify the IP addresses for reaching this router, click **Add**.

The Add IP Address dialog box appears (see Figure 2-30).

Figure 2-30 Add IP Address Dialog Box



Step 3 Enter the IP address for the router.

Step 4 If the IP address you enter here is also the IP address for the management interface on the router, check the **This address is the management interface** option.

You return to the IP Addresses tab. The address you entered is displayed in the "IP Addresses for reaching this target" area (see Figure 2-31).

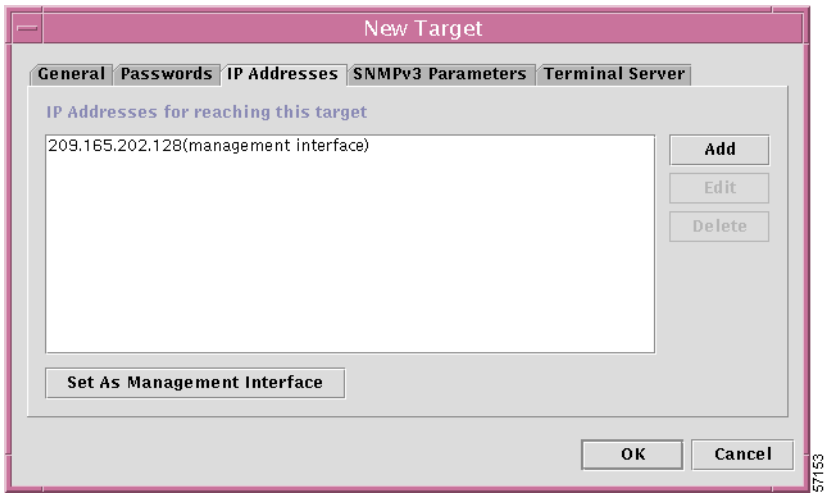
Note that you can also specify an IP address as the management interface from the IP Addresses tab. To do so:

a. Select the appropriate IP address from those listed.

b. Click **Set As Management Interface**.

The IP address is displayed with "(management interface)" appended to the address.

Figure 2-31 New Target IP Addresses Dialog Box



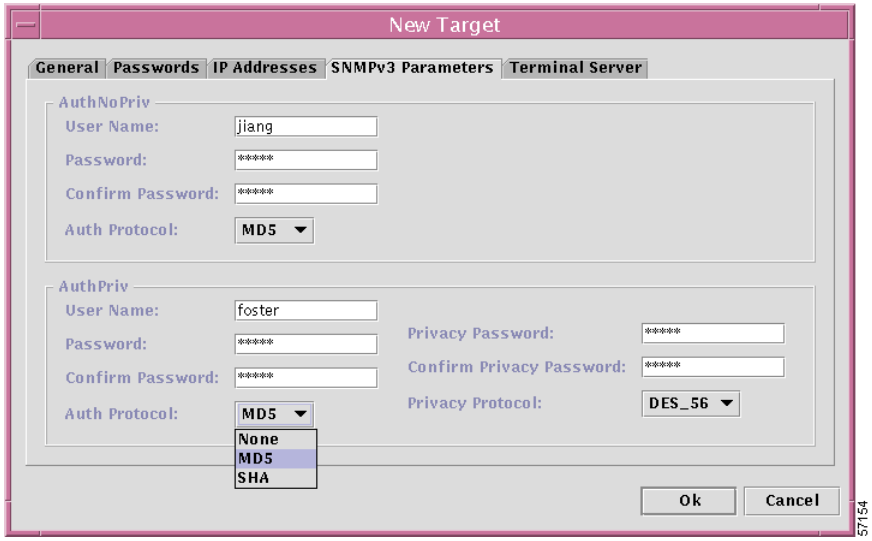
To add additional IP addresses for this device, repeat Steps 8 through 10.

Specifying the SNMPv3 Parameters

Step 1 Choose the **SNMPv3 Parameters** tab.

The SNMPv3 Parameters dialog box appears (see Figure 2-38).

Figure 2-32 SNMPv3 Parameters Dialog Box



Step 2 If appropriate, define the parameters for the *AuthNoPriv* security level.

- *User Name*. The user name configured on the specified edge device router. This user must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request).
- *Password*. The user authentication password.
- *Auth Protocol*. The authentication protocol. The available options are **None**, **MD5**, or **SHA**.

Step 3 If appropriate, define the parameters for the *AuthPriv* security level.

- *User Name*. The user name configured on the specified edge device router. This user must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request).
- *Password*. The user authentication password.
- *Auth Protocol*. The authentication protocol. The available options are **None**, **MD5**, or **SHA**.
- *Privacy Password*. The encryption password.
- *Privacy Protocol*. The encryption protocol. Currently, only **DES-56** is supported.

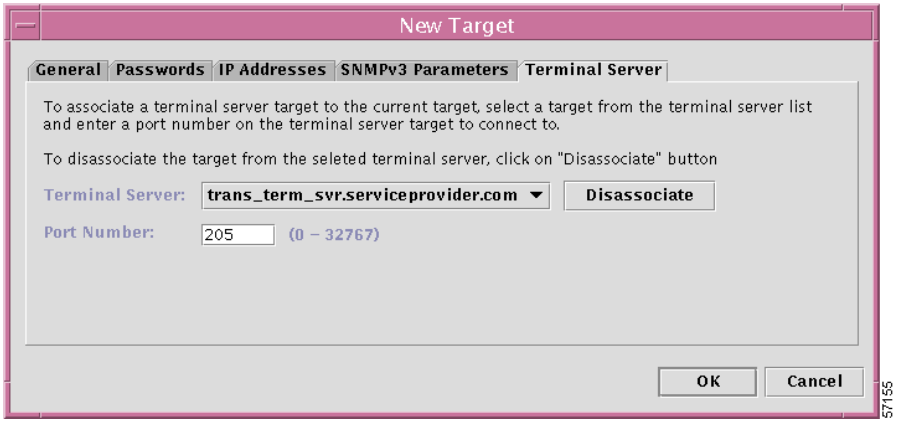
Step 4 When the SNMPv3 parameters are correctly entered, proceed to the next tab, Terminal Server, to associate the terminal server device with an edge device router (as described in the next section).

Assigning a Terminal Server to the Current Router

To assign a terminal server to the current router, follow these steps:

Step 1 From the Edit Target dialog box, choose the **Terminal Server** tab (see Figure 2-33).

Figure 2-33 Choosing a Terminal Server for the Selected Router



Step 2 From the *Terminal Server* drop-down list, choose the name of the terminal server you want to associate with the current router.

- You can disassociate a terminal server from a device by clicking **Disassociate**.

Step 3 In the *Port Number* field, enter the port number on the terminal server that the server will use to access the router.

Step 4 When the parameters are set to your satisfaction, click **OK**.

Defining Terminal Servers in VPN Solutions Center Software

A terminal server is a communications processor that connects asynchronous devices such as terminals, printers, hosts, and modems to a LAN or WAN. In VPN Solutions Center 2.0, terminal servers provide a way to provision edge device routers from a workstation.

The VPN Solutions Center workstation is connected on a LAN to the terminal server device (typically a Cisco 2500 Series router). Each of the terminal server device's ports have a port number. Each serial line can be connected to an edge device router's console port. In this way, a VPN Solutions Center operator can communicate directly with an edge device router.

In the VPN Solutions Center software, you first define a target as a terminal server, and then associate that terminal server device with a particular edge device router.

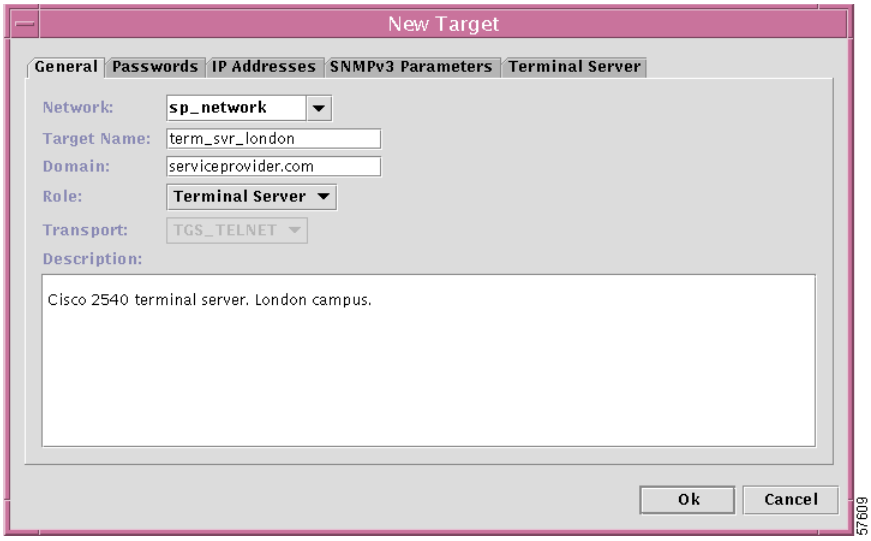
Defining a Target as a Terminal Server

To define a target as a terminal server in VPN Solutions Center software, follow these steps:

Step 1 From the Networks window, choose **Actions > New Target**.

The New Target dialog box appears (see Figure 2-34).

Figure 2-34 New Target Dialog Box



Step 2 Enter the values for the parameters in the **General** dialog box.

a. From the *Network* drop-down list, specify the network name.

b. In the *Target Name* field, specify the name of the terminal server device.

c. In the *Domain* field, specify the domain name for the device.

d. In the *Role* field, set the role to **Terminal Server**.

When you set the Role to Terminal Server, the *Transport* field is automatically set to *Telnet*, which configures the method of communication between the VPN Solutions Center workstation and the terminal server device.

e. In the *Description* field, enter any pertinent information about the terminal server device, such as the type of device and its location.

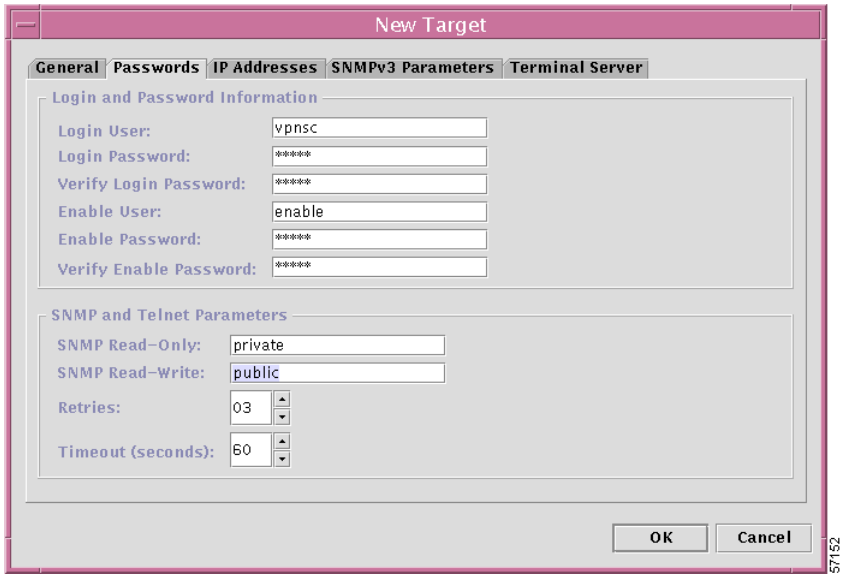
Specifying the Device Passwords and SNMP and Telnet Parameters

Step 3 Choose the **Passwords** tab.

The New Target Passwords dialog box appears (see Figure 2-35).

Note The values set in this dialog box must match the corresponding values set on the actual device.

Figure 2-35 New Target Passwords Dialog Box



Step 4 Enter the appropriate values for the fields in the **Passwords** dialog box.

a. Enter the *Login User* name.

b. Enter the *Login Password* for the device, then verify the password.

c. If the Enable User name exists on the device, enter it in the *Enable User* field.

d. If the Enable Password is set on the device, enter it in the *Enable Password* field.

e. Set the *SNMP Read-Only* and *SNMP Read-Write* community strings in the corresponding fields.

f. Set the SNMP and Telnet *Retries* value.The default is three retries.

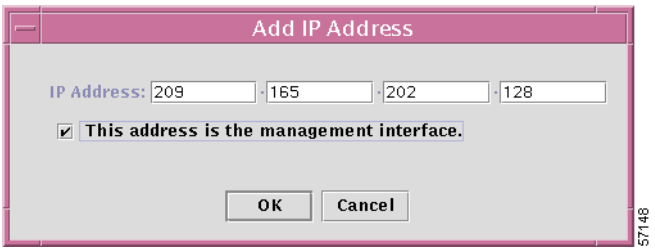
g. Set the SNMP and Telnet *Timeout* value (in seconds). The default is 60 seconds.

Step 5 Choose the **IP Addresses** tab.

Step 6 To specify the IP addresses for reaching this terminal server device, click **Add**.

The Add IP Address dialog box appears (see Figure 2-36).

Figure 2-36 Add IP Address Dialog Box

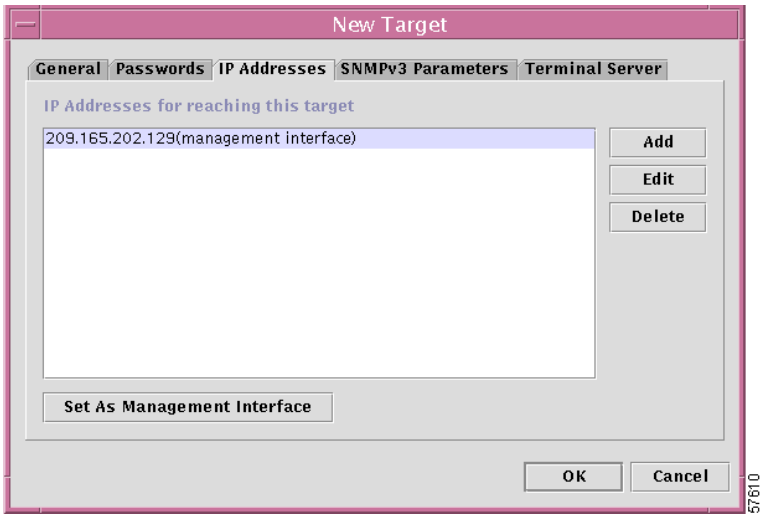


Step 7 Enter the IP address for the terminal server device, then click **OK**.

The address you entered is displayed in the "IP Addresses for reaching this target" area (see Figure 2-37).

For information about the management interface, see the "Setting the Management Interface" section on page 2-33.

Figure 2-37 New Target IP Addresses Dialog Box



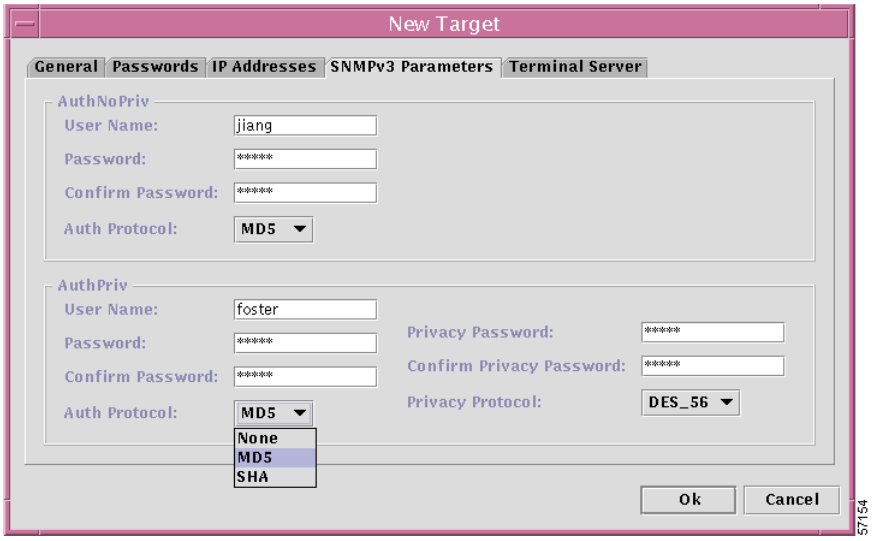
To add additional IP addresses for this device, repeat Step 6 and Step 7.

Specifying the SNMPv3 Parameters

Step 8 Choose the **SNMPv3 Parameters** tab.

The SNMPv3 Parameters dialog box appears (see Figure 2-38).

Figure 2-38 SNMPv3 Parameters Dialog Box



Step 9 If appropriate, define the parameters for the *AuthNoPriv* security level.

- *User Name*. The user name configured on the specified edge device router. This user must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request).
- *Password*. The user authentication password.
- *Auth Protocol*. The authentication protocol. The available options are **None**, **MD5**, or **SHA**.

Step 10 If appropriate, define the parameters for the *AuthPriv* security level.

- *User Name*. The user name configured on the specified edge device router. This user must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request).
- *Password*. The user authentication password.
- *Auth Protocol*. The authentication protocol. The available options are **None**, **MD5**, or **SHA**.
- *Privacy Password*. The encryption password.
- *Privacy Protocol*. The encryption protocol. Currently, only **DES-56** is supported.

Step 11 When the SNMPv3 parameters are correctly entered, proceed to the next tab, Terminal Server, to associate the terminal server device with an edge device router (as described in the next section).

Associating a Terminal Server with an Edge Device Router

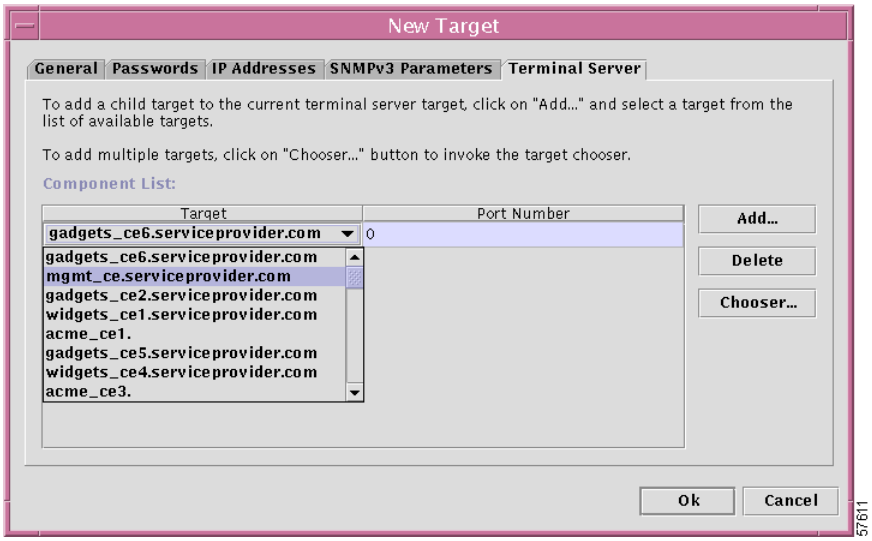
When a terminal server device is defined in VPN Solutions Center software, you can then associate that terminal server device with one or more edge device routers in the network. Then a workstation connected to the terminal server device can communicate with all of the routers associated with the terminal server.

To associate a terminal server with an edge device router, follow these steps:

Step 1 In the New Target window, choose the **Terminal Server** tab.

The Terminal Server dialog box appears (see Figure 2-39).

Figure 2-39 Terminal Server Dialog Box



This dialog box provides a procedure for adding access from the terminal server to a single edge router device or adding access to multiple edge router devices.

Adding Terminal Server Access to a Single Device

Step 2 To assign terminal server access to a single router device, click **Add**.

A new row appears in the window. If there are multiple targets in the Repository, the Target field displays a drop-down list (as shown in Figure 2-39).

Step 3 In the *Target* field, click the down arrow to see a list of targets (as shown in Figure 2-39).

Step 4 Select the name of the device you want terminal server access to.

The cursor appears in the *Port Number* field.

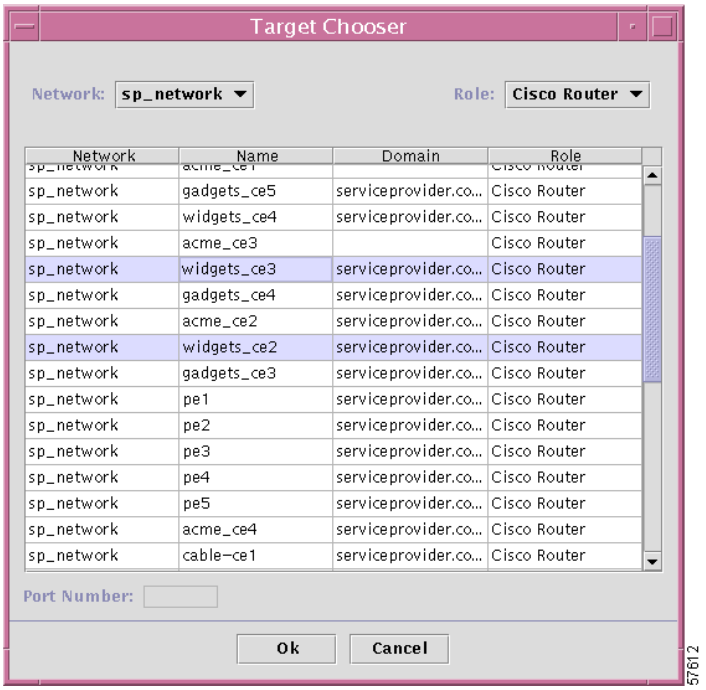
Step 5 Enter the terminal server port number for access to the selected router.

Adding Terminal Server Access to Multiple Devices

Step 1 To assign terminal server access to multiple router devices, click **Chooser**.

The Target Choose dialog box appears (see Figure 2-40).

Figure 2-40 Selecting Multiple Devices for Terminal Server Access



Step 2 From the list of devices listed in the Target Chooser, select the routers for which you want access from the terminal server.

To select multiple items in a list, press **Ctrl+Click**.

Note that when you select multiple routers from the list, the *Port Number* field is grayed out.

Step 3 When you finish selecting the routers that are to be accessible from the selected terminal server, click **OK**.

You return to the Terminal Server dialog box, where the routers that you selected are added to the list of targets for the terminal server.

Step 4 In the *Port Number* field for each new router, enter the appropriate terminal server port numbers for access to the selected routers, then click **OK**.

You have now completed defining a device as a terminal server and configured terminal server access to the routers.

Adding a NetFlow Collector Device to the Network

When you install NetFlow on the NetFlow Collector (NFC) device, configure a local username and password. The username and password is used by VPN Solutions Center software to communicate with the NFC.

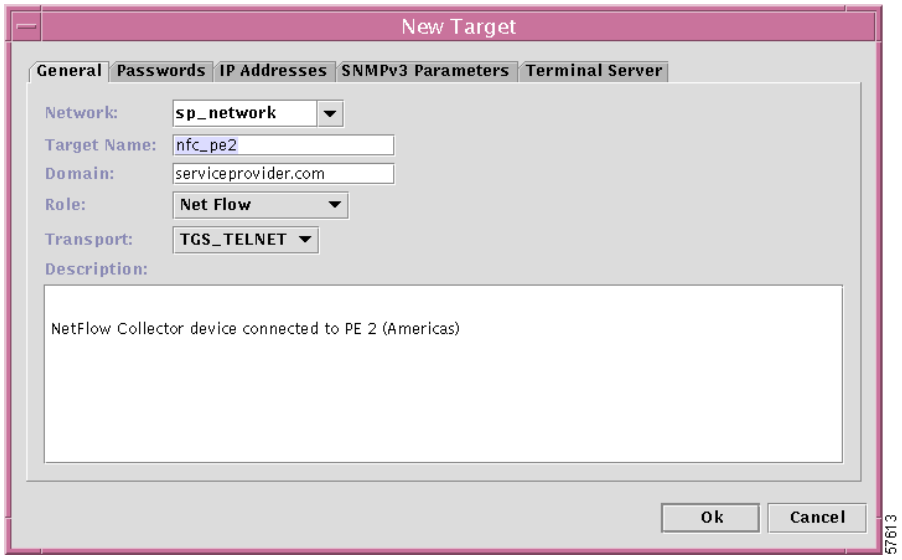
In order to collect traffic statistics from NetFlow Collector devices, these devices must be configured as a target. To do so, follow these steps:

Step 1 Double-click the desired network from the Networks list.

The Network window appears, displaying the names of all the devices in the selected network.

Step 2 From the Network window, choose **Actions > New Target**. The New Target dialog box appears (see Figure 2-41).

Figure 2-41 New Target Dialog Box for NetFlow Collector Device



Step 3 Enter the values for the parameters in the **General** dialog box.

a. From the *Network* drop-down list, specify the network name.

b. In the *Target Name* field, enter the UNIX host name of the NetFlow Collector device (NFC).

Note When you define target names in VPN Solutions Center software, it is important that the target names you specify match the actual IOS host names of the corresponding devices.

c. In the *Domain* field, specify the domain name for the device.

Caution It is important to note that when you specify both the domain name of a device and the IP address of a device, *the IP address overrides the specified domain name*.

d. In the *Role* field, set the role to **NetFlow**.

e. In the *Transport* field, choose **TGS_TELNET**.

The *Transport* field configures the method of communication between the VPN Solutions Center workstation and the NFC device. The default is **TGS_TELNET** for MPLS operations.

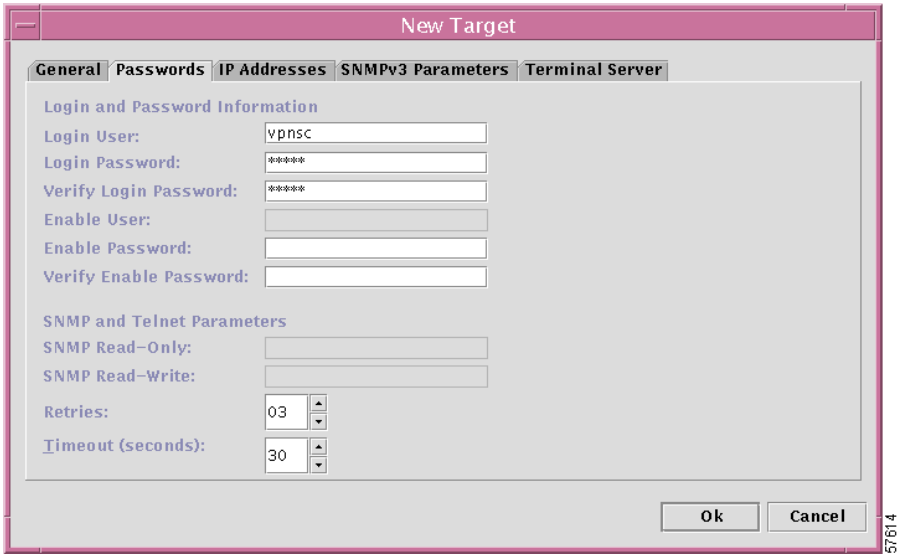
f. In the *Description* pane, enter any pertinent information about the NFC device, such as the type of device, its location, and any other information that could be helpful to service provider operators.

Specifying the NFC Device Passwords

Step 4 Choose the **Passwords** tab.

The New Target Passwords dialog box appears (see Figure 2-42).

Figure 2-42 Passwords Tab for NetFlow Collector Device



Step 5 Complete the Passwords dialog box fields as necessary.

a. Enter the *Login User* and *Login Password* fields as necessary.

VPN Solutions Center uses the username and Login password specified here to communicate with the NFC device. The Login password is a required password—this password must be set both on the NFC device and in VPN Solutions Center software.

The Enable user, Enable Password, and SNMP and Telnet parameter information is not necessary on an NFC device, so these fields are not accessible.

b. Complete the *Retries* and *Timeout* fields as necessary.

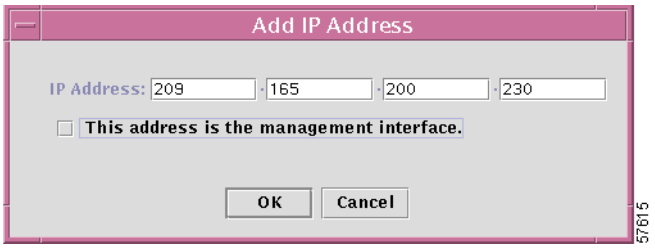
The recommended value for *Retries* is **4**; the recommended value for *Timeout* is **30** seconds.

Step 6 Choose the **IP Addresses** tab, then click **Add**.

The Add IP Address dialog box appears (see Figure 2-43).

Caution It is important to understand that when you specify both the domain name of the device and the IP address of the device, *the IP address overrides the specified domain name*.

Figure 2-43 Add the IP Address for the NetFlow Collector Device



Step 7 Enter the IP address for the selected NFC device, then click **OK**.

You return to the IP Addresses tab, where the IP address you entered is now displayed.

Specifying the SNMPv3 Parameters

Step 8 Choose the **SNMPv3 Parameters** tab.

The SNMPv3 Parameters dialog box appears (see Figure 2-38 on page 2-44).

Complete the fields as necessary as described in "Specifying the SNMPv3 Parameters" section on page 2-39.

When defining an NFC device, you cannot configure terminal server access to the NFC device; therefore, the Terminal Server tab is not enabled.

This completes the procedure for adding an NetFlow Collector device to the network.

Viewing Devices in the Network by Their Role

You can view lists of the existing devices in a network by the role assigned to them as either Cisco routers or NetFlow Collector devices.

To view devices by their role, follow these steps:

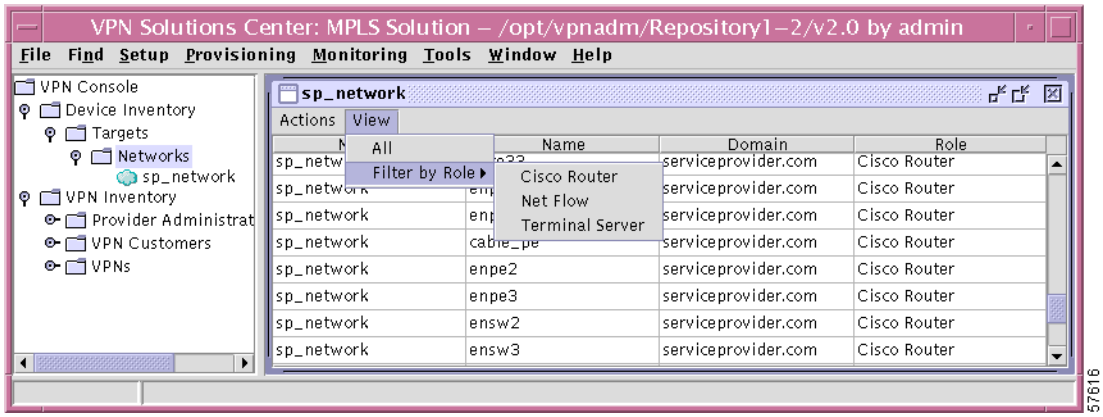
Step 1 From the VPN Console hierarchy pane, select the desired network and double-click.

The Network window appears in the data pane. By default, all the routers in the selected network are listed in the Network window.

Step 2 From the Network window, choose **View > Filter by Role**.

As shown in Figure 2-44, a submenu appears with three options: **Cisco Router**, **NetFlow**, and **Terminal Server**.

Figure 2-44 Network Window View Menu



- To view all the devices—routers and NFC devices—in the network, choose **View > All**.
- To view all the *Cisco routers* in the network, choose **View > Filter by Role > Cisco Routers**.
- To view all the *NetFlow Collector devices* currently defined in the network, choose **View > Filter by Role > NetFlow**.
- To view all the terminal servers in the network, choose **View > Filter by Role > Terminal Server**.

Defining Provider Administrative Domains

The VPN Solutions Center software allows you to define as many *Regions* within a Provider Administrative Domain (PAD) as you need. PADs are divided into Regions in much the same way that customers are divided into sites. A Region can be considered to be a group of provider edge routers (PEs) within a single BGP autonomous system. The primary objective for defining Regions is to allow a provider to employ unique IP address pools in large Regions, such as Europe, Asia Pacific, and so forth.

Note that a provider can also assign PEs to these Regions, thereby simplifying the PE selection process (for example, only presenting PEs in the European Region when adding service to a European customer edge router).

Tips Cisco recommends that providers create one Provider Administrative Domain and then define the Regions within the PAD.

Before you begin this procedure, have the following information at hand:

- The BGP autonomous system (AS) number

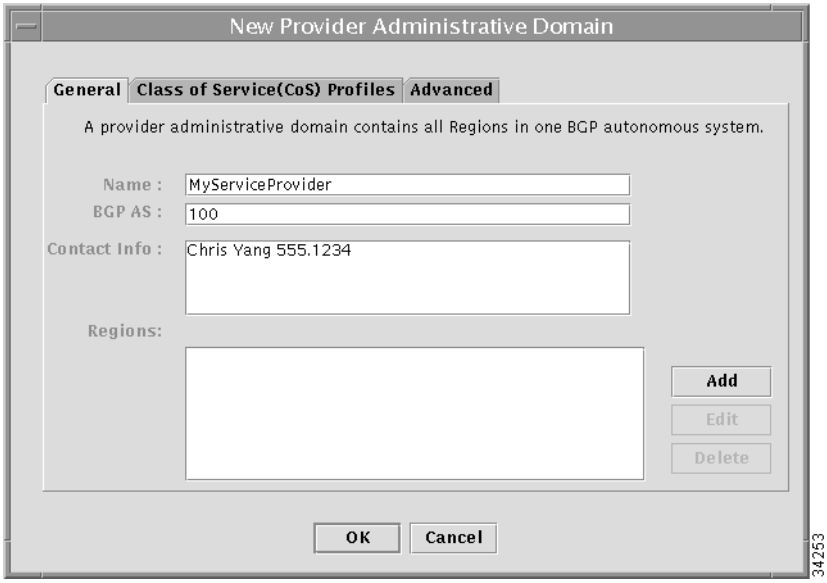
  There is generally one BGP AS number per Provider Administrative Domain.
- The names of the PE routers within the Region
- The IP address pools for point-to-point links (that is, the IP numbered links)
- The IP address pools for loopback links (that is, the IP unnumbered links)

To define a new Provider Administrative Domain, follow these steps:

Step 1 From the VPN Console menu, choose **Setup>New Provider Administrative Domain**.

The New Provider Administrative Domain dialog box appears (see Figure 2-45).

Figure 2-45 The New Provider Administrative Domain Dialog Box



Step 2 Enter the name of the PAD and the BGP Autonomous System (AS) number in the appropriate fields.

Each autonomous system is assigned a unique 16-bit number by the same central authority that assigns IP network numbers.

The contact information is optional, but it is a good idea to provide it.

The Regions pane on the dialog box shown in Figure 2-45 on page 2-51 is where existing Region names are displayed. Regions must have a name, assigned PEs, and their corresponding IP address pools.

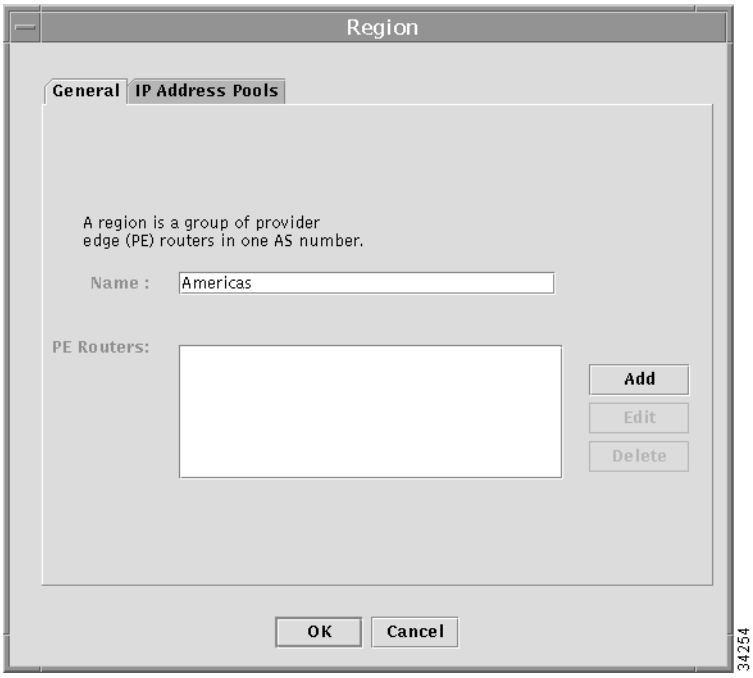
Defining a New Region in a PAD

A Region can be considered to be a group of provider edge routers (PEs) within a single BGP autonomous system.

Step 3 To begin defining a new Region, from the New Provider Administrative Domain dialog box, click **Add**.

The Region dialog box appears (see Figure 2-46).

Figure 2-46 Defining a New Region



Step 4 Enter the name of the Region.

The next step in creating a Region is to assign the provider edge routers that are in the Region.

Assigning the Provider Edge Routers to a Region

To assign the provider edge routers for the Region, follow these steps:

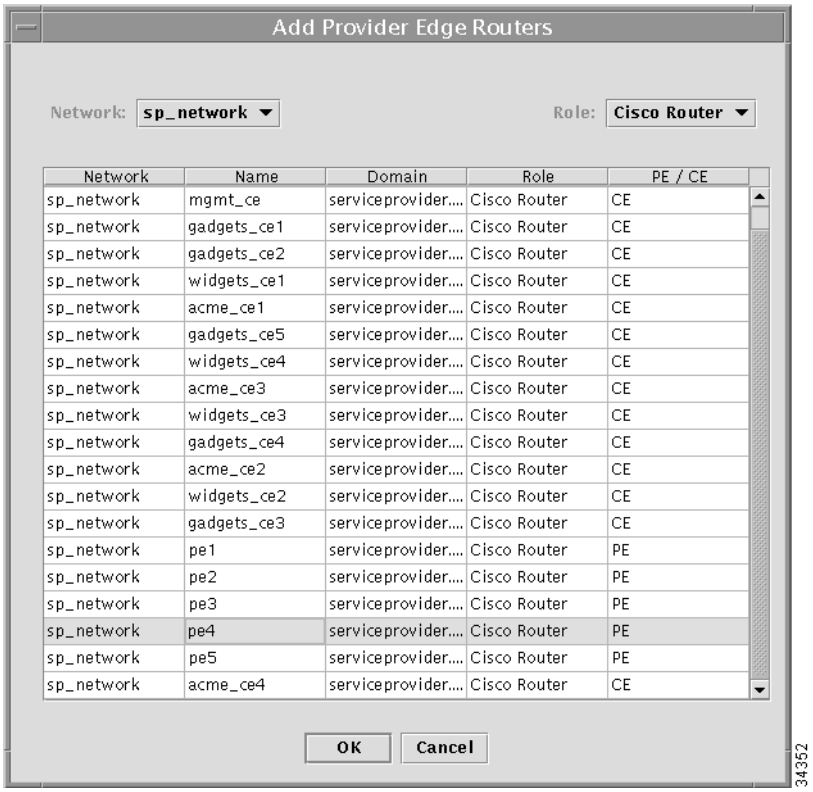
Step 1 From the New Region dialog box, click **Add**.

When you select the **Add** button from the Region dialog box, the Add Provider Edge Routers dialog box appears.

Step 2 From the dialog box's Network drop-down list, select the appropriate service provider network name (or a network that contains provider devices).

The names of the targets (routers) in the selected service provider network are displayed (see Figure 2-47).

Figure 2-47 Assigning Provider Edge Routers



Step 3 From the list of routers, select a router to be assigned as a PE, then click **OK**.

You return to the Region dialog box. The name of the router you selected is now displayed in the list of PE Routers.

Step 4 Repeat this procedure to add additional PEs to the Region as required.

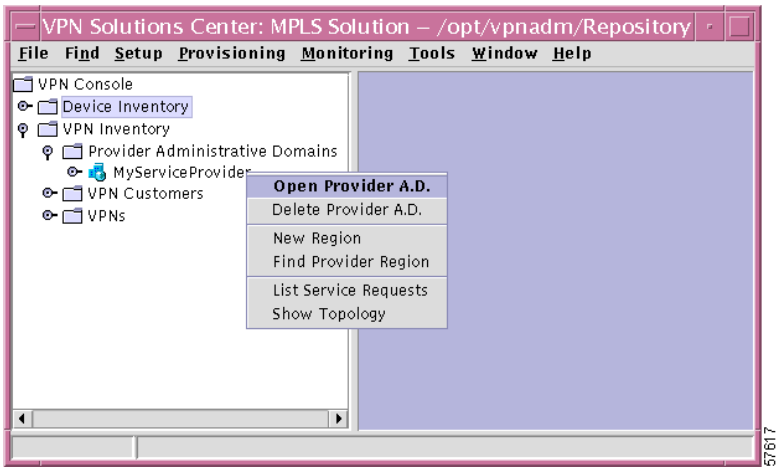
When all the provider edge routers for a Region are assigned, the next task is to assign the IP address pool for the Region (see the "Defining the IP Address Pools for a Region" section on page 2-57).

Adding Provider Edge Routers to a Region

You can add only PEs that are not already assigned to a Region. To add PEs to a Region, follow these steps:

Step 1 In the VPN Console hierarchy pane, select the name of the Provider Administrative Domain (PAD), then **right-click**. The Provider Administrative Domain menu appears (see Figure 2-48).

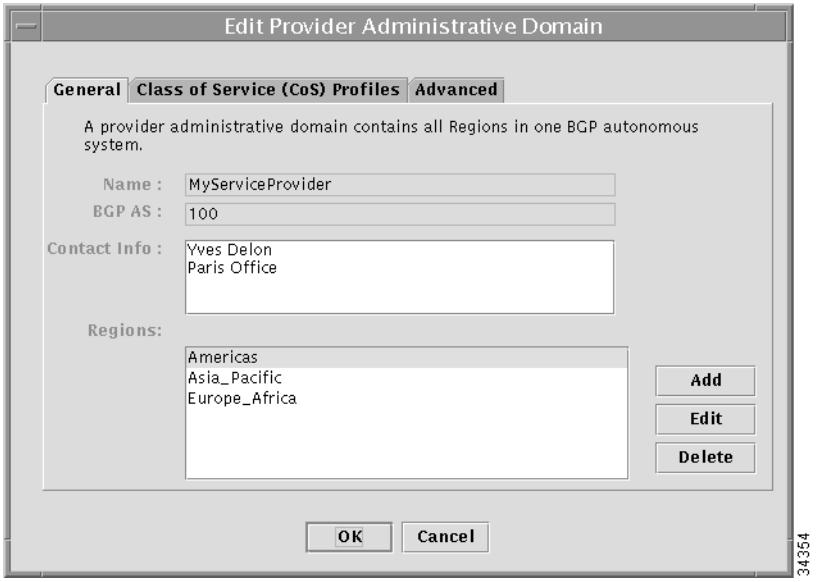
Figure 2-48 The Provider Administrative Domain Menu



Step 2 From the Provider Administrative Domain menu, choose **Open Provider A.D.**

The Edit Provider Administrative Domain dialog box appears (see Figure 2-49).

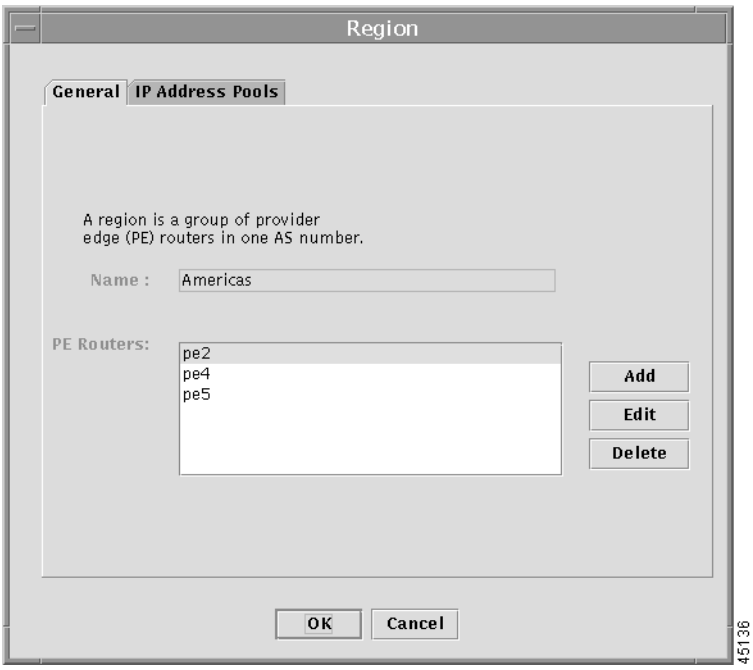
Figure 2-49 Edit Provider Administrative Domain Dialog Box



Step 3 From the list of Regions, choose the Region to which the PE is to be added.

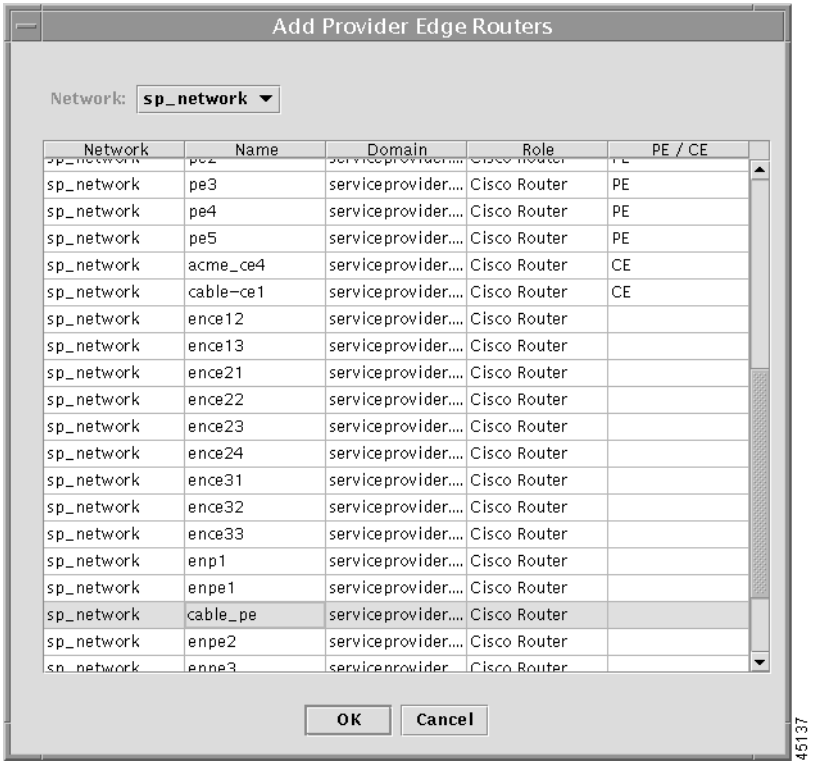
Step 4 Click **Edit**. The Region dialog box appears (see Figure 2-50).

Figure 2-50 The Region Dialog Box



Step 5 From the Region dialog box, click **Add**.

Figure 2-51 Selecting the PE to Be Added to the Region



Step 6 In the Add Provider Edge Routers dialog box, do the following:

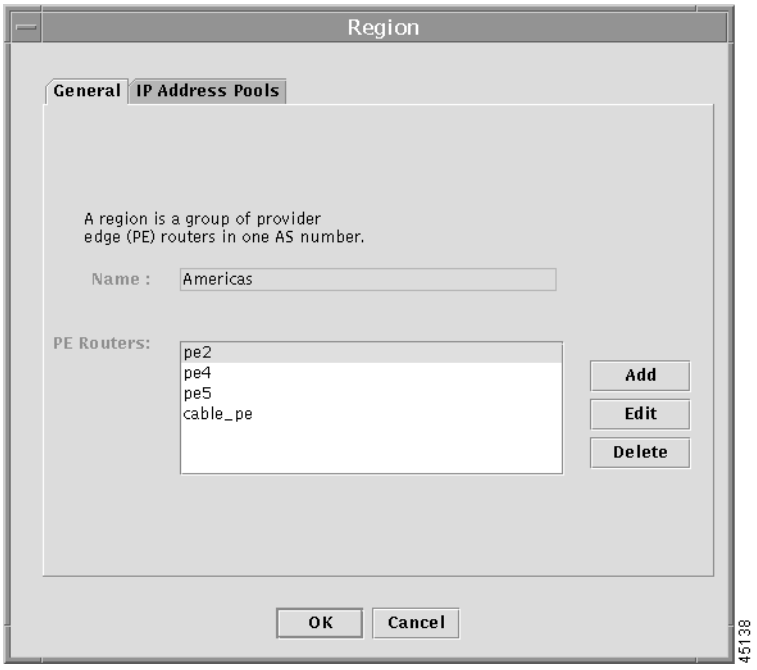
a. From the Network drop-down list, choose the network.

b. From the list of devices, choose the name of the router you want to add as a PE.

c. Click **OK**.

You return to the Region dialog box, where you can see, as shown in Figure 2-52, that the selected router has been added to the list of PE Routers in the Region.

Figure 2-52 The PE Is Added to the Region



Step 7 To complete the operation, click **OK**. You return to the Edit Provider Administrative Domain dialog box. Click **OK** again to return to the VPN Console.

Finding a Specific VPN Service Provider

To find a specific VPN service provider, follow these steps:

Step 1 From the VPN Console window, choose **Find > Find VPN Provider**.

The Find dialog box appears with the category *VPN Provider* already selected, as shown in Figure 2-53.

Figure 2-53 The Find VPN Provider Dialog Box

Step 2 In the *Find What* field, enter the name of the VPN Provider you want to find.

Step 3 If you want the search to match the case of the VPN Provider name you enter, check the **Match Case** check box.

Step 4 Choose the direction of the search by clicking the **Up** or **Down** radio button.

Step 5 When you have completed the search parameters, click **Find Next**.

The VPNSC software locates the indicated VPN Provider and highlights it in the hierarchy pane.

Defining the IP Address Pools for a Region

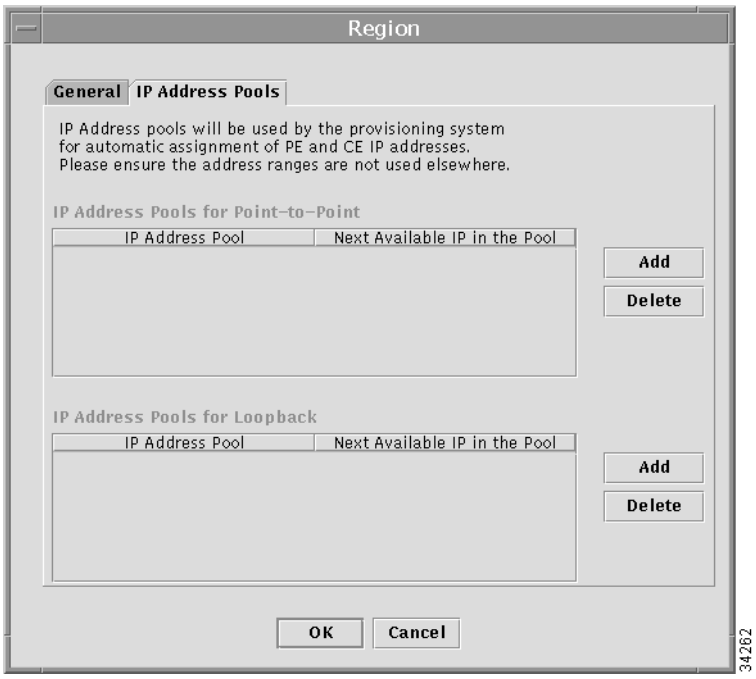
The VPN Solutions Center software uses IP address pools to automatically assign IP addresses to PEs and CEs. Each Region has an IP address pool to use for IP numbered addresses (point-to-point address pool) and a separate IP address pool for IP unnumbered address (loopback address pool).

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

Caution Due to security and maintenance issues, Cisco does not recommend using customer IP addresses on the PE-CE link.

Step 1 From the Region dialog box, choose the **IP Address Pools** tab (see Figure 2-54).

Figure 2-54 Defining a Region's IP Address Pool



From this dialog box, you can add IP address pool information for point-to-point (IP numbered) links or loopback (IP unnumbered) links.

Step 2 Choose which type of address pool you are defining and click **Add**. The New IP Address Pool dialog box appears (see Figure 2-55).

Figure 2-55 Entering a New IP Address Pool

Step 3 Enter the address for the IP address pool and click **OK**.

You return to the IP Address Pools dialog box, where the new IP address pool information is displayed.

Step 4 Click **OK**.

You return to the New Provider Administrative Domain dialog box, where the new Region name is displayed in the *Regions* field.

Customizing the Route Distinguisher and Route Target Values

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

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

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

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

VPN Solutions Center software sets the route distinguisher and route target values, but you can assign your own values if you choose (as described in this section).

You can also override the default RD value set by the VPN Solutions Center software. For instructions, see the "Overriding the Default VRF Name and Route Distinguisher Values" section on page 4-23.

Note You can change the RD and RT values with the VPN Solutions Center software for a given Provider Administrative Domain (PAD) *only* when creating a new PAD. You cannot edit the RD and RT values once they are initially set.

By default, the product software assigns the RD values as follows:

- CEs with hub connectivity use `bgp_AS:`*value*.
- CEs with spoke connectivity use `bgp_AS:`*value* `+ 1`

Each spoke uses its own RD value for proper hub and spoke connectivity between CEs; therefore, the VPN Solutions Center software implements a new RD for each spoke that is provisioned.

To assign the Route Distinguisher or Route Target values, follow these steps:

Step 1 From the New Provider Administrative Domain dialog box (see Figure 2-45 on page 2-51), choose the **Advanced** tab.

The New PAD Advanced dialog box appears (see Figure 2-56 on page 2-60), which allows you to alter the default Route Distinguisher and Route Target values.

Figure 2-56 Setting the Route Distinguisher and Route Target Values

Step 2 In the *Start Route Distinguisher Values At <BGP AS#>* field, enter the new Route Distinguisher value.

Step 3 In the *Start Route Target Values At <BGP AS#>* field, enter the new Route Target value.

Step 4 Click **OK**.

Adding a Region to an Existing Provider Administrative Domain

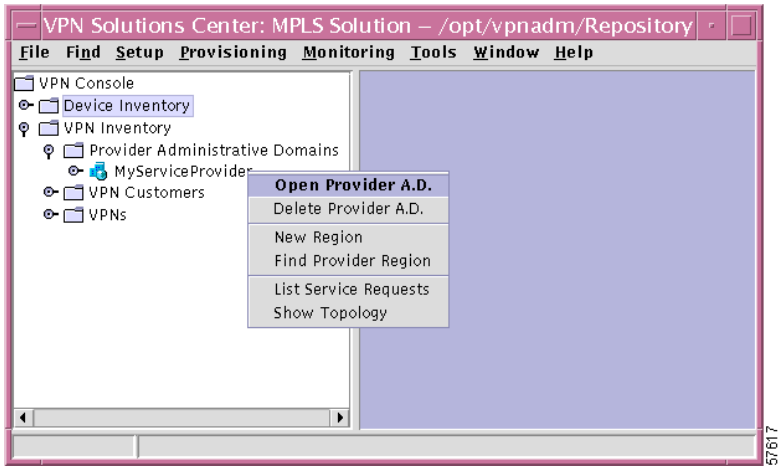
To add a Region to an existing Provider Administrative Domain, follow these steps:

Step 1 From the VPN Console hierarchy pane, click the open-close icon for the Provider Administrative Domain folder.

The list of Provider Administrative Domains is displayed.

Step 2 Select the desired Provider Administrative Domain, then **right-click**. The PAD menu appears (see Figure 2-57).

Figure 2-57 Accessing the PAD Menu



Step 3 From the PAD menu, choose **New Region**. The Region dialog box appears, as shown in Figure 2-46 on page 2-52.

Step 4 Complete the procedures as described in the previous sections, "Assigning the Provider Edge Routers to a Region" and "Defining the IP Address Pools for a Region."

Deleting a Region

Only a Region without any active service requests associated with that Region can be deleted.

To delete a Region from a Provider Administrative Domain, follow these steps:

Step 1 From the VPN Console hierarchy pane, click the open-close icon for the Provider Administrative Domain folder.

Step 2 Click the desired Provider Administrative Domain's open-close icon.

The list of Regions is displayed.

Step 3 Select the desired Region, then **right-click**.

Step 4 From the Regions menu, choose **Delete Region**.

A confirmation window appears with the message, "Are you sure you want to delete this Region?"

Step 5 Click **Yes**.

The Region is deleted and removed from the VPN Console display.

Finding a Specific Provider Region

To find a specific region, follow these steps:

Step 1 From the VPN Console window, choose **Find > Find Provider Region**.

The Find dialog box appears with the category *Provider Region* already selected, as shown in Figure 2-58).

Figure 2-58 Find Provider Region Dialog Box

Step 2 In the *Find What* field, enter the name of the Region you want to find.

Step 3 If you want the search to match the case of the Region name you enter, check the **Match Case** check box.

Step 4 Choose the direction of the search by clicking the **Up** or **Down** radio button.

Step 5 When you have completed the search parameters, click **Find Next**.

The VPNSC software locates the indicated Region and highlights it in the hierarchy pane.

Step 6 Close the Find dialog box.

Showing the Topology for a Provider Administrative Domain

This section provides an overview of main features for viewing the Provider Administrative Domains topology. This section does not describe all the topology features in detail. For details on each of the menus and options available from the Topology window, refer to "Topology" in Chapter 10 of the *VPN Solutions Center: MPLS Solution User Reference*.

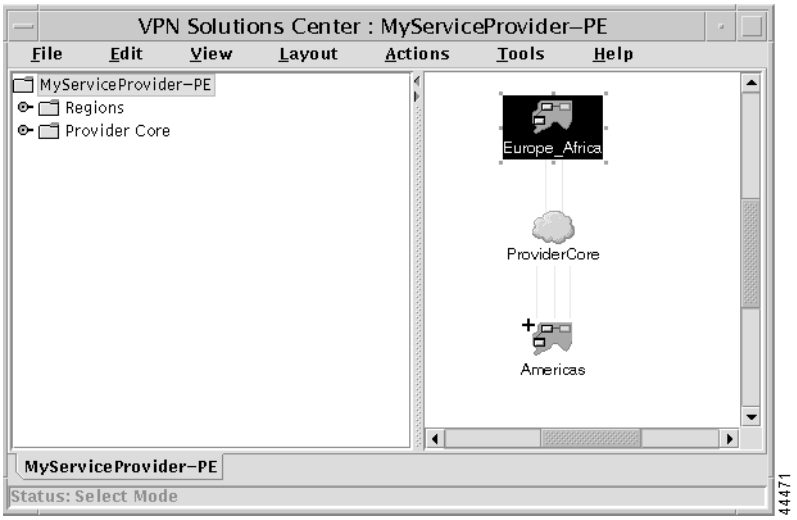
To display the topology for a particular Provider Administrative Domain, follow these steps:

Step 1 In the hierarchy pane of the VPN Console, select the name of the Provider Administrative Domain, then **right-click**. The PAD menu appears (see Figure 2-57 on page 2-60).

Step 2 From the PAD menu, choose **Show Topology**.

The VPNSC software displays the current top-level topology for the selected Provider Administrative Domain (see Figure 2-59).

Figure 2-59 Top-Level Topology Display for the PAD

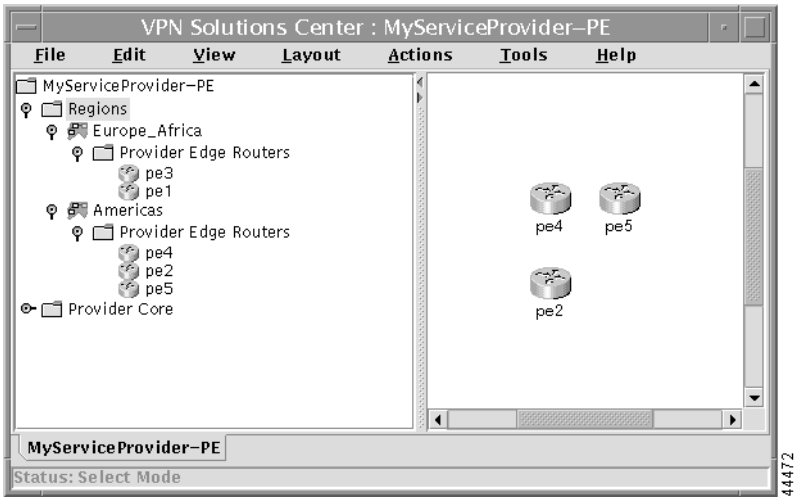


Step 3 Use the functions and features in the Topology windows to view various aspects of the PAD topology.

Viewing the List of Regions and PEs in Each Region

When you open the folders in the hierarchy pane, you can see the names of the PEs, the Regions, and the Service Provider with whom they are associated (see Figure 2-60).

Figure 2-60 Viewing the Elements in the PAD

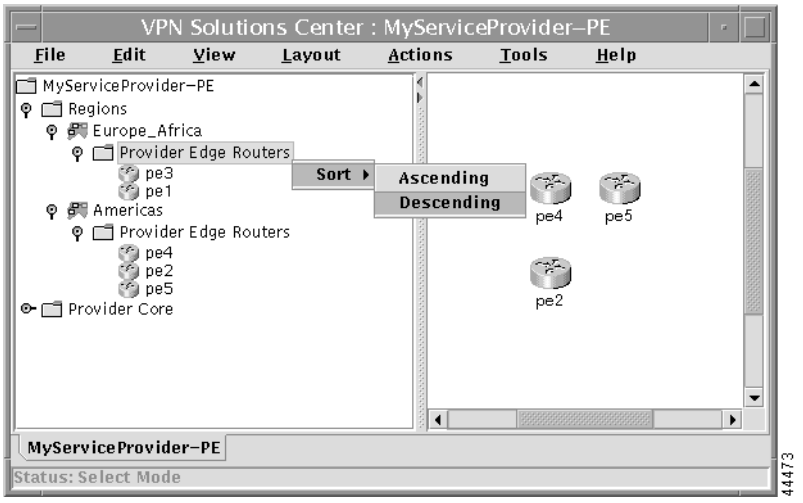


Sorting the Regions and PEs

Step 1 You can sort the display of Regions and Provider Edge Router. To do so, select either the Regions or Provider Edge Routers folder, then **right-click**. The Sort menu appears (see Figure 2-61).

Step 2 To sort the list in ascending order, choose **Sort > Ascending**; to sort the list in descending order, choose **Sort > Descending**.

Figure 2-61 The Topology Sort Menu

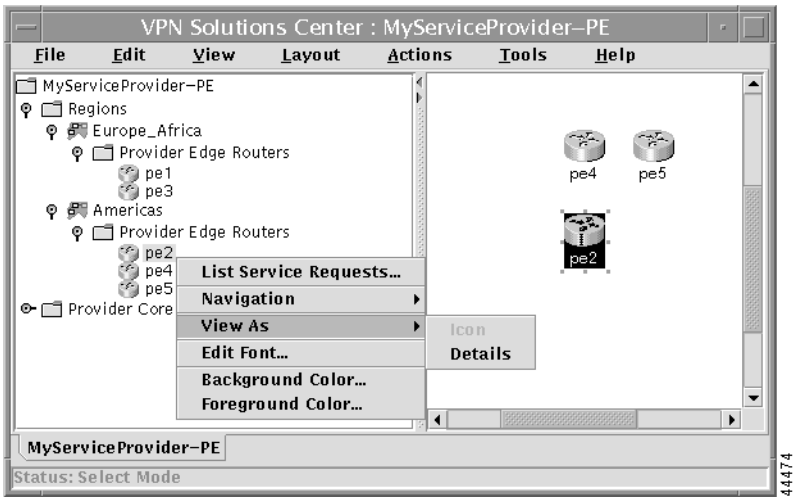


Retrieving Region and PE Details

You can view and retrieve various details concerning the Regions and PEs in a specific PAD.

Step 1 To do so, select the name of a Region or the name of a specific PE. The Node menu appears (see Figure 2-62).

Figure 2-62 Viewing Details with the Node Menu Options

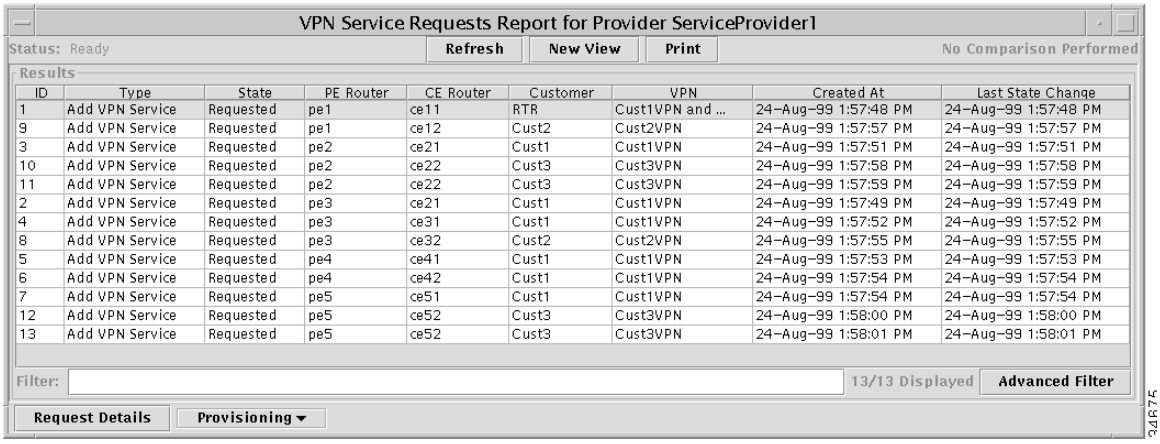


The Node menu presents the following options:

- List Service Requests

  Choose **List Service Requests** to generate the VPN Service Requests Report that lists the service requests associated with the selected Region or PE.

Figure 2-63 The VPN Service Requests Report



- Navigation

  An element displayed with a + (plus) sign indicates that more information is available. The **Navigation** option offers two options: **Go to Child Graph** and **Show Child Graph**.

- View As

  The **View As** option provides two options: **Icon** and **Details**.

- Edit Font

  Choosing the **Edit Font** option brings up the Choose Font dialog box. From this dialog box, you can choose the font type and size for the topology display.

- Background Color

  Choosing the **Background Color** option brings up the Choose Color dialog box. From this dialog box, you can choose the background color for the topology display.

- Foreground Color

  Choosing the **Foreground Color** option brings up the Choose Color dialog box. From this dialog box, you can choose the foreground color for the topology display.

Step 2 Choose the options you need from the Node menu.

About Class of Service with VPN Solutions Center Software

As part of their VPN services, service providers may wish to offer premium services defined by Service Level Agreements (SLAs) to expedite traffic from certain customers or applications. Quality of Service (QoS) and its implementation through Class of Service (CoS) mechanisms in IP networks gives devices the intelligence to preferentially handle traffic as dictated by network policy.

About QoS

Quality of Service (QoS) is typically used to describe a situation in which the network provides preferential treatment to certain types of traffic, but the term is not specific about exactly which mechanisms are used to provide these services.

QoS is not a device feature, it is an end-to-end system architecture. A robust QoS solution includes a variety of technologies that interoperate to deliver scalable, media-independent services throughout the network, with system-wide monitoring capabilities.

QoS is defined as those mechanisms that give network managers the ability to control the mix of bandwidth, delay, jitter, and packet loss in the network.

The actual deployment of QoS in a network requires a division of labor for greatest efficiency. Because QoS requires intensive processing, the Cisco model distributes CoS duties between edge and core devices. Edge devices, such as provider edge routers (PEs), do most of the processor-intensive work, performing application recognition to identify flows and classify packets according to unique customer policies. Edge devices also provide bandwidth management. Core devices expedite forwarding while enforcing CoS levels assigned at the edge.

About CoS

Class of Service (Cos) is distinguished by providing *differentiated* classes of service. Before you can provide a higher quality of service to a customer, application, or protocol, you must classify the traffic into classes, and then determine the way in which to handle the various traffic classes as traffic moves through the network.

When differentiation is performed, it is done to identify traffic by a unique criteria and classify incoming traffic into classes. Each of the traffic classes must be recognized by the classification mechanisms at the network ingress point, as well as farther along in the network topology.

CoS differentiation is usually performed as a method of identifying traffic as it enters the network or a method that ensures that traffic is classified appropriately so that it is forced to conform with the desired user-defined policy or service-level agreement (SLA).

VPN Solutions Center software provisions Class of Service on the ingress PE interfaces and the egress CE interfaces. VPN Solutions Center offers the following features for Class of Service (CoS) provisioning between a CE and a PE:

- Shaping

  Shaping is a method of mapping traffic into separate output queues to provide predictable network behavior. In MPLS VPNs, shaping is configured on either the CE's or PE's egress interfaces. For shaping, the product uses Generic Traffic Shaping (GTS) that includes an optional feature that handles Frame Relay Backward Explicit Congestion Notification (BECN) responses.

- Policing

  Takes place into a PE from a CE and configured on the CE's or PE's egress interfaces. The product uses Committed Access Rate (CAR) for policing.

- Congestion Management

  Congestion management is a scheme that provides preferential treatment to certain classes of traffic when the network is congested. In the context of MPLS VPNs, congestion management is put in place to manage heavy traffic from a PE as it moves to a CE. The product employs both GTS and (D)WRED.

  GTS for congestion management is not a full-featured technique because it cannot preferentially queue and drop packets based on precedence. However, the ideal solution—Class-Based Weighted Fair Queueing—is not currently available.

  GTS still has the powerful property of protecting other customers' SLAs, which are supported on shared fabric between the PE and CE. That is, if one customer suddenly converges all his traffic towards one CE, GTS shapes this load so that the shared medium is not saturated, hence preventing failure on all SLAs in the vicinity.

  The other choice, Distributed Weighted Random Early Detection ((D)WRED) is simple to configure, although not particularly precise. (D)WRED is configured on the PE's egress interfaces.

  VPN Solutions Center over-specifies the inputs for congestion management, even though the current configuration uses only the bandwidth total.

All three techniques rely on existing IP precedence values in all packets. Policing may change these values, but the values to differentiate the service classes must have already been set before exiting from the CE. The setting of initial IP precedence values is called *painting* or *marking*.

Defining a Class of Service Profile

A Class of Service (CoS) profile represents a set of CoS configurations offered by a provider to its customer. Each CoS profile consists of a set of CoS classes that record information on how traffic shaping and policing are configured.

The VPN Solutions Center software requires that you create a Class of Service (CoS) Profile only if you want the product to provision CoS on the PE-CE link. You can add additional CoS profiles at any time. This procedure only defines the CoS Profile—until you invoke it when you activate a service request, the CoS Profile has no effect.

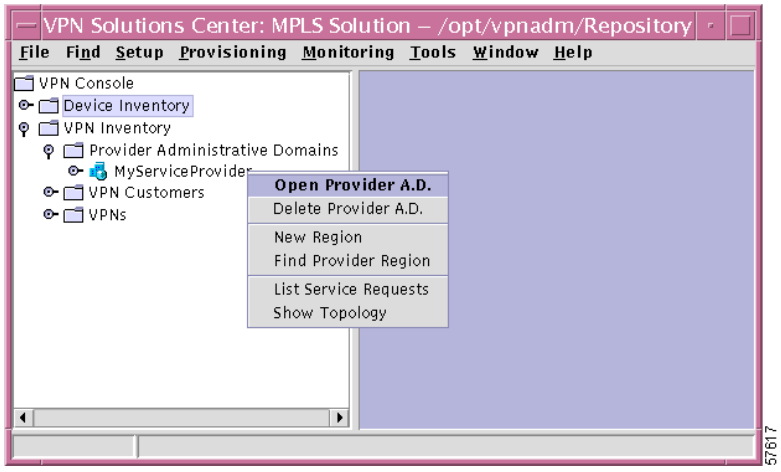
Class of Service Profiles are applied to the Provider Edge Router (PE), but the CoS definition is enforced across the PE-CE link on both the PE and CE.

To define a Class of Service Profile, follow these steps:

Step 1 From the VPN Console hierarchy pane, select the name of the pertinent Provider Administrative Domain, then **right-click**.

The PAD menu appears (see Figure 2-64).

Figure 2-64 The PAD Menu



The PAD menu lets you open (that is, edit) the current settings for the administrative domain, define a new Region, list the service requests active for this administrative domain, and view the current topology for that domain.

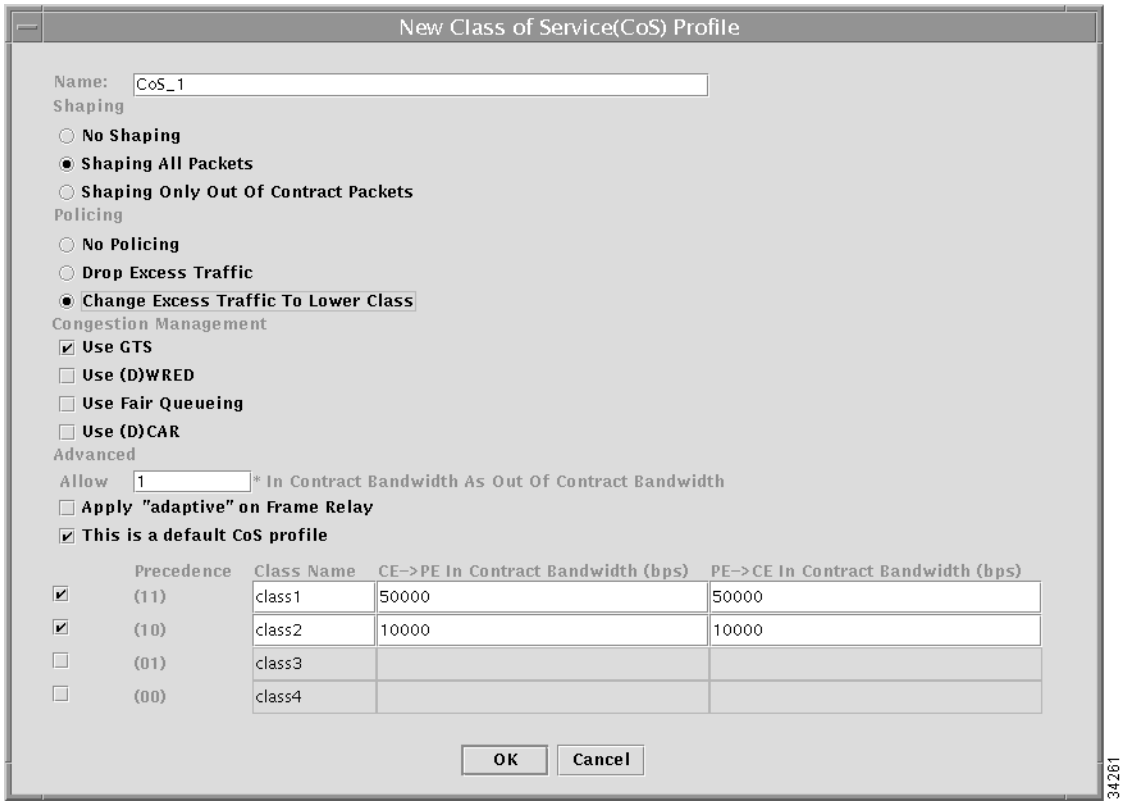
Step 2 Choose **Open Provider A.D**.

The Edit Provider Administrative Domain dialog box appears.

Step 3 Choose the **Class of Service (CoS) Profiles** tab, then click **Add**.

The New Class of Service Profile dialog box appears (see Figure 2-65).

Figure 2-65 Defining a Class of Service Profile



Step 4 Complete the Class of Service profile, then click **OK**.

Valid input for the in-contract bandwidth is a range from **8,000 to 2,000,000,000** (in *bits per second*).

The PE can rate limit traffic to the subscribed bandwidth and mark the traffic that is within the specified bandwidth as *in-contract*, and mark traffic above the specified bandwidth as *out-of-contract*.

Marking a packet as in-contract or out-of-contract is done by setting the first bit of the precedence bits in the IP header. The appropriate class is indicated by the remaining two precedence bits (see Table 2-2 on page 2-69). Traffic that exceeds any class is marked as out-of-contract, and this traffic can be dropped or mapped to a lower class of service.

The out-of-contract bandwidth is initially set to the in-contract bandwidth, but you can set this to the values appropriate for the customer.

Table 2-2 Mapping IP Precedence to Class of Service

IP Precedence	Contract Status	Class of Service
111	In-contract	Class 1
110	In-contract	Class 2
101	In-contract	Class 3
100	In-contract	Class 4
011	Out-of-contract	Class 1
010	Out-of-contract	Class 2
001	Out-of-contract	Class 3
000	Out-of-contract	Class 4

The customer can initially "paint" the packets that leave the customer edge router (the PE is the destination router), and VPN Solutions Center allows policing or repainting of packets that enter the provider edge router.

For more information, see the "Quality of Service and Class of Service" section on page 1-25.