CHAPTER 5

Monitoring MPLS VPN Performance

This chapter provides an overview of performance monitoring and data collection tasks. VPN Solutions Center provides three types of performance monitoring:

- MPLS VPN NetFlow Accounting, page 5-2
- Monitoring Performance Through Service Level Agreements, page 5-10
- Using CAR to Monitor Data, page 5-28

Accessing the VPNSC Data Query Tools

The VPN Solutions Center software periodically collects performance data such as Service Assurance Agent (SA Agent) data, Accounting data, and Committed Access Rate (CAR) MIB data; the application then places this data in the Repository. You can access this data through web-based data query tools, as well as through customized reports or through CORBA APIs. The performance data retrieved by the web-based data query tools is saved to a file in XML format.

VPNSC provides the following data query tools:

- SA Agent data
- Accounting data
- CAR MIB data
- Interface statistics

To access the VPNSC Data Query Tools, follow these steps:

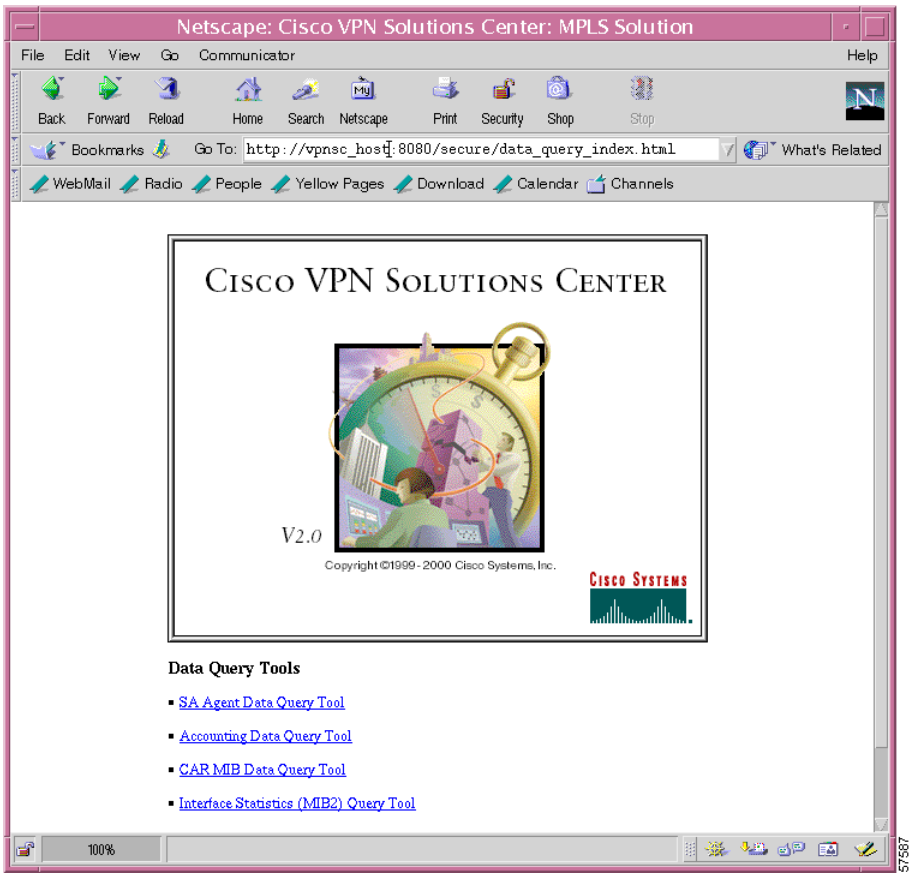
Step 1 From the VPN Console menu, choose **Monitoring > XML Data Query Tool**.

The first time you access the web browser from the VPNSC software, you must log in.

Step 2 In the Netscape Password dialog box, enter your user name and password, then click **OK**.

The VPN Solutions Center Data Query Tools page appears (see Figure 5-1).

Figure 5-1 MPLS Solution Data Query Tools Page



- For information on how to use the Data Query Tools to gather Accounting data, see the "Retrieving Accounting Data with the XML Data Query Tool" section on page 5-8.
- For information on how to use the Data Query Tools to gather SA Agent data, see the "Retrieving SA Agent Data with the XML Data Query Tool" section on page 5-11.
- For information on how to use the Data Query Tools to gather CAR MIB data, see the "Retrieving CAR MIB Data with the XML Data Query Tool" section on page 5-32.
- For information on how to use the Data Query Tools to gather interface statistics data, see the "Retrieving Interface Statistics with the XML Data Query Tool" section on page 5-34.

For additional details, refer to "XML Data Query Tool" in Chapter 8 of the *Cisco VPN Solutions Center: MPLS Solution User Reference*.

MPLS VPN NetFlow Accounting

In the VPN Solutions Center software, accounting data is collected to provide end-to-end usage information on VPN-based network traffic and to provide a complete billing solution. Collected accounting data is used by the Accounting server for various levels of aggregation for accounting reports and API accounting information.

NetFlow Collector (NFC) is the software that gathers flow statistics from Cisco IOS devices. It is used for data collection, filtering and aggregation. The NetFlow data is stored on the NetFlow workstations in binary flat files. Because NetFlow sends data from the router in User Datagram Protocol (UDP) packets, Cisco recommends that the NetFlow Collector 3.0 device be located on a LAN connected directly to the PE or the Management PE (MPE) device.

VPN Solutions Center makes NetFlow "MPLS-aware." Thus, different service provider Customers can use the same IP address space, and VPN Solutions Center can track the traffic flows for each individual VPN and Customer.

To use NetFlow and VPN Solutions Center software to gather flow statistics, you must complete the following tasks:

- Set up the service provider network for NetFlow accounting.
- Make the appropriate settings and configuration elements on each NetFlow Collector device in the service provider network.
- In the VPN Solutions Center software VPN Console, add the NetFlow Collector devices to the service provider network and enable NetFlow accounting.

Setting Up NetFlow Accounting on the Service Provider Network

Before you can use VPN Solutions Center software to provide NetFlow accounting data, complete the following tasks in the service provider network:

1. NetFlow Collector must be running.
2. Issue the following commands once per PE:

   ```
   ip flow-export version 5
   ip flow-export destination ip_address port
   ```

   Note The *Version* and *Port* parameters set on the PEs must be identical to the settings configured in the NetFlow Collector device.

3. 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.
4. On the PE interfaces that face the CEs, enable interfaces with the following command:

   ```
   ip route-cache flow
   ```

5. To confirm that NetFlow is enabled and that traffic flows are being recorded, issue the following command on each NetFlow-enabled PE:

   ```
   show ip cache flow
   ```

   The output for this command shows the size of the packets, types of traffic, which interfaces the traffic enters and exits, as well as the source and destination addresses.

6. NetFlow Collector uses a pre-allocated cache. By default, the NFC cache has 64K entries in which each flow (unidirectional) is assigned one entry. Each entry uses 68 bytes. You can expand the number of NetFlow Collector entries if traffic requirements and machine resources warrant, as follows:

   ```
   ip flow-cache entries #
   ```

The **ip flow-cache entries** command is a global command executed on the PE.

The default size of the NetFlow cache is usually adequate. However, you can increase or decrease the number of entries maintained in the cache to meet the needs of your flow traffic rates. For environments with a high amount of flow traffic (such as an Internet core router), a larger value such as 131072 (128K) is recommended. To obtain information on your flow traffic, use the show ip cache flow command.

The default is 64K flow cache entries. Each cache entry is approximately 64 bytes of storage. Assuming a cache with the default number of entries, approximately 4 MB of DRAM would be required. Each time a new flow is taken from the free flow queue, the number of free flows is checked. If there are only a few free flows remaining, NetFlow attempts to age 30 flows using an accelerated timeout. If there is only one free flow remaining, NetFlow automatically ages 30 flows regardless of their age. The intent is to ensure free flow entries are always available.

Caution Cisco recommends that you do not change the NetFlow cache entries. Improper use of this feature could cause network problems. To return to the default NetFlow cache entries, use the **no ip flow-cache entries** global configuration command.

Configuring the NetFlow Collector Device

Complete the following tasks on each NetFlow Collector device in the service provider network:

1. When you install NetFlow on the NetFlow Collector (NFC) device, configure a local user name and password. VPN Solutions Center software uses this NFC user name and password to communicate with the NFC device.
2. After NetFlow Collector 3.0 is installed, two configuration files must be modified so that VPN Solutions Center software can import traffic data from the NFC device—the *nf.resources* file and the *nfconfig.file*. Both files are located on the NFC device at */opt/CSCOnfc/config*.

- On the NetFlow Collector device, edit the *nf.resources* file as follows:

```
#Set format to Comma Separated for VPNSC:
CSV_FORMAT yes
#Use long file names with dates:
LONG_OUTPUTFILE_SUFFIX yes
```

- On the NetFlow Collector device, edit the *nfconfig.file* file as follows:

```
#Use the Detail Call Record aggregation scheme for VPNSC:
Thread DETCALLREC
Aggregation DetailCallRecord
Period 30
Port 9996
State Active
DataSetPath /opt/CSCOnfc/Data
Binary Yes
Compression No
Max Usage 100
```

Note Without these statements in the *nfconfig.file*, the VPN accounting reports cannot display information.

Configuring NetFlow Accounting in VPN Solutions Center

When NetFlow is set up in the service provider network and the NFC devices themselves, you can then configure NetFlow accounting in VPN Solutions Center software. To do so, you must add the NFC devices to the network definition and enable NetFlow accounting.

1. In order to collect traffic statistics from NetFlow Collector devices, the NFC devices must be configured as a target. For instructions, see the "Adding a NetFlow Collector Device to the Network" section on page 2-47.
2. Enabling NetFlow accounting in VPN Solutions Center software is part of adding a service for a specific PE-CE link. For information on where you enable NetFlow accounting in the product, see the "Specifying VRF Parameters" section on page 4-22.

Specifying the NetFlow Collector Devices in the Network

This procedure allows you to specify the NetFlow Collector devices in the network from which you want VPN Solutions Center to collect accounting data. You also define the data collection schedule. This collection procedure assumes that the NetFlow Collector devices are configured in the network and have already collected data from the network.

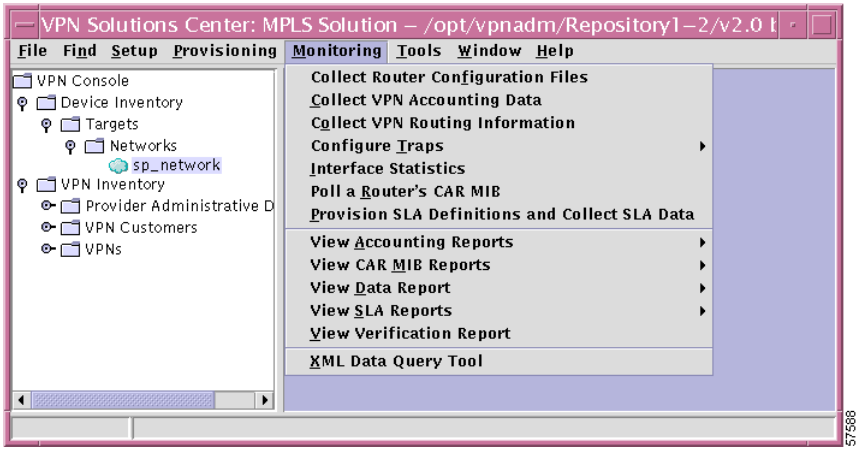
Tips Cisco recommends that you schedule VPN Solutions Center to collect data from the NetFlow Collector devices every three hours.

To collect VPN accounting data, follow these steps:

Step 1 From the VPN Console, choose **Monitoring**>**Collect VPN Accounting Data**.

The VPN Console Monitoring menu shown in Figure 5-2 provides the menu options from which you can access the performance collection tasks and their corresponding reports.

Figure 5-2 Monitoring Menu



Step 2 The first window is informational. Click **Next** to continue.

The Get Devices dialog box allows you to specify the NetFlow Collector devices from which you wish VPN Solutions Center to collect accounting information.

Step 3 From the Network drop-down menu, select the name of the network that the NetFlow Collector devices are in.

The upper panel displays all the available NetFlow Collector devices in the specified network.

Step 4 Click **Add All**.

The active list of NetFlow Collector devices is displayed in the lower panel.

If you need to remove some of NetFlow Collector devices from the active list, select the appropriate device and click **Remove** to remove a specific device; or click **Remove All** to remove all the NetFlow Collector devices from the active list.

When you are ready to choose the NetFlow Collector devices in the lower panel, click **Next**.

Step 5 Provide a unique task name for the data collection operation, then click **Next**.

The task name you enter here is listed in the Task Manager window and the Task Logs.

Defining the Data Collection Schedule

Step 6 Begin to schedule the task by selecting the **Yes** radio button and clicking **Next**.

Note Do not click **Add** until you have set all the other scheduling information in the Schedule dialog box.

Step 7 To set the collection frequency schedule to once every three hours, click the **Hourly** radio button.

Step 8 In the Start Time fields, set the time you want VPN Solutions Center to start collecting data from the NetFlow Collector devices.

Note Be sure to set the start time no less than fifteen minutes ahead of the current time.

Step 9 In the Every hour(s) drop-down menu, select **3**.

Step 10 Set the duration of the collection task.

- If you want to limit the duration of the collection task, click the End On drop-down menu and specify the desired date you wish to end the collection task.
- If you want to collect data continuously, set the End Time as **No End**.

For detailed information about scheduling, refer to Chapter 12, "Scheduling," in the *Cisco VPN Solutions Center: MPLS Solutions User Reference, Release 2.0*.

Step 11 Click **Next** to initiate and save the accounting collection task.

You are informed that all the steps are done.

Step 12 Click **Close** to close the wizard.

Now that you have collected data for accounting, you can view this data as directed in the next section "Viewing Accounting Reports."

Note Based on the number of data flows, it may take from between fifteen minutes to an hour after you initiate the collection operation before the analyzed data is available through the accounting reports.

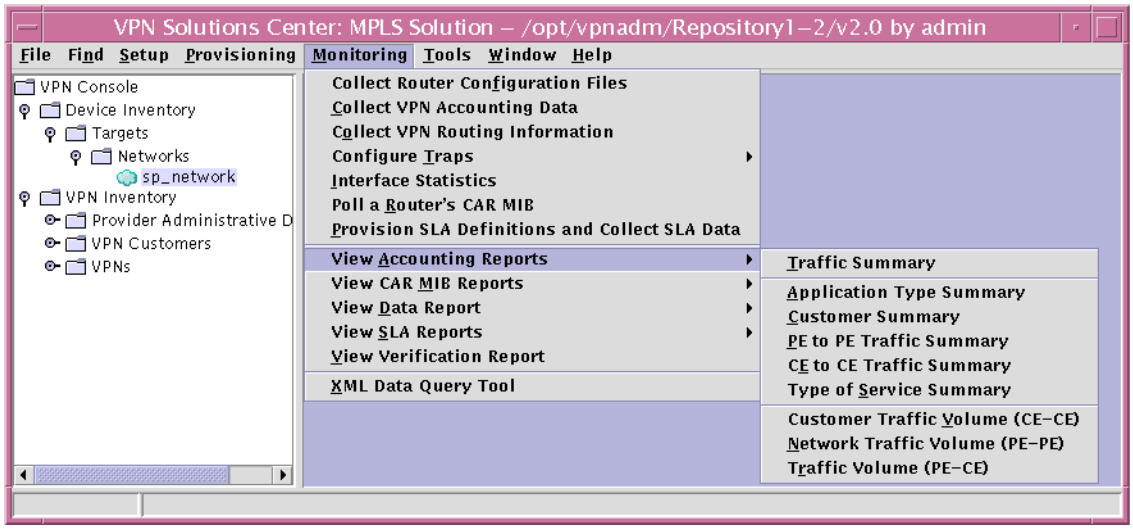
Viewing Accounting Reports

NetFlow data is periodically procured from the NetFlow Collector workstations. VPN Solutions Center analyzes the data to create the accounting reports:

Accounting reports, which are based on processed accounting data, provide network usage and planning information. Billing systems can get the traffic usage from the Accounting Server, which leverages collected accounting data and provides complete billing services to customers.

After collecting VPN accounting data, choose **Monitoring** > **View Accounting Reports**, then select the specific type of report you require (as shown in Figure 5-3).

Figure 5-3 Accounting Reports Menu



The accounting reports are as follows:

- Traffic Summary Report

  Displays total packets and total KB for traffic that can be mapped to the VPN (VPN Traffic) and otherwise to Unmappable Traffic.

- Application Type Summary Report

  Provides total packets and total K bytes for each application type.

- Customer Summary Report

  Provides total packets and total KB for each customer plus additional reports for customer site and application type.

- PE to PE Traffic Summary Report

  Reports on all traffic between PE to PE, plus additional reports for the following: 1) PE to connected CE, 2) PE to remote CE, 3) PE traffic, and 4) PE to CE.

- CE to CE Traffic Summary Report

  Reports on all traffic between CE to CE.

- Type of Service Summary Report

  Provides total packets and total KB for each type of service.

- Customer Traffic Volume (CE-CE) Report

  Provides information on all traffic volume for a specific customer between CE to CE in packets or KB (by type of service).

- Network Traffic Volume (PE-PE) Report

  Provides information on all traffic volume between PE to PE in packets or KB (by type of service).

- Traffic Volume (PE-CE) Report

  Provides information on all traffic between PE to CE (by TOS).

Note For more detail about the data provided in the reports and how to get to the specific information that you require, refer to "View Accounting Reports" in Chapter 9 of the *Cisco VPN Solutions Center: MPLS Solutions User Reference. Release 2.0*.

Retrieving Accounting Data with the XML Data Query Tool

VPN Solutions Center periodically collects Accounting performance data and places this data in the Repository. You can access the Accounting data through web-based data query tools, as well as through customized reports or through CORBA APIs. The performance data retrieved by the web-based data query tools is saved to a file in XML format that includes a Document Type Definition (DTD).

The Accounting data query can specify the exact time period and time interval for the data. With the Advanced query, you can organize the data by application type or service request; you can also retrieve the Accounting data for a specific application or class of service.

You can retrieve Accounting statistics by specifying the source and destination of the traffic. The source and destination can be any one of the following network elements: PE, CE, Customer, or Customer Site. To query the traffic traversing between two CEs requires that both CEs belong to the same Customer; likewise, to query the traffic traversing between two sites requires that both sites belong to the same Customer.

To access the Accounting Data Query Tools, follow these steps:

Step 1 From the VPN Console menu, choose **Monitoring > XML Data Query Tool**.

The first time you access the web browser from the VPNSC software, you must log in.

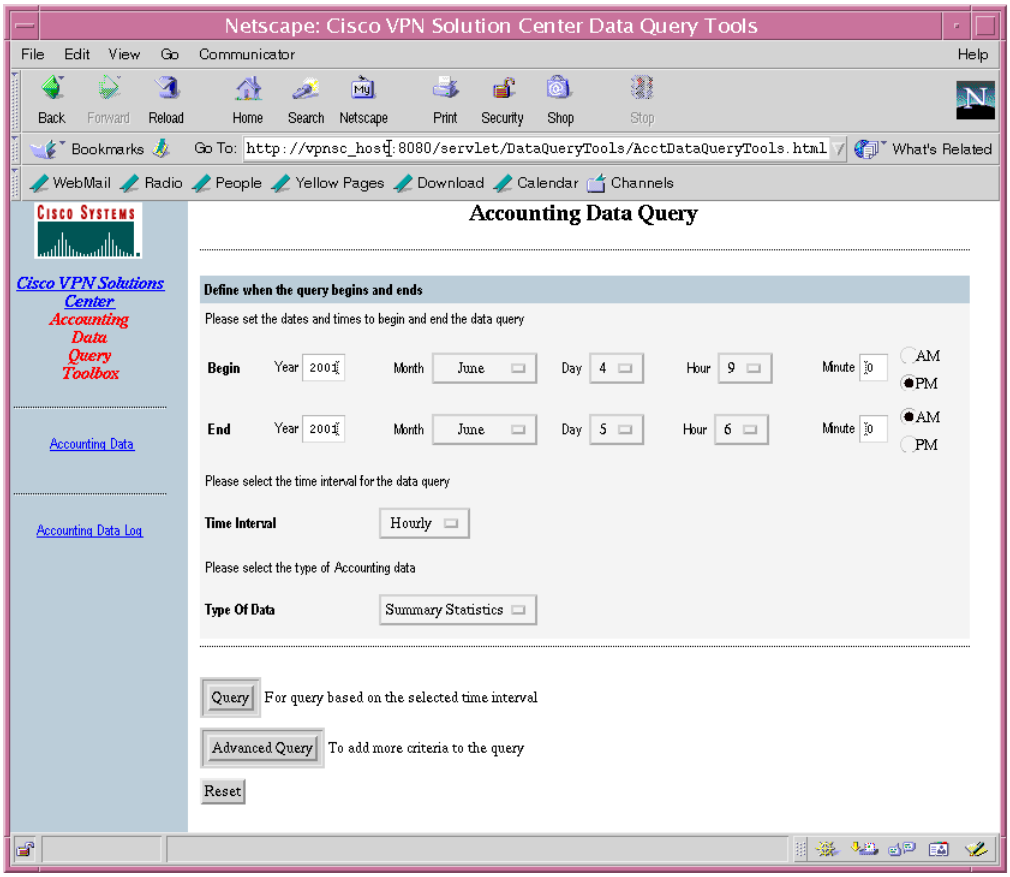
Step 2 In the Netscape Password dialog box, enter the username and password for the VPN Solutions Center workstation, then click **OK**.

The VPN Solutions Center Data Query Tools page appears.

Step 3 Choose **Accounting Data Query Tool**. The Accounting Data Query Tool page appears.

Step 4 From this page, choose **Accounting Data**.

Figure 5-4 Accounting Data Query Page



Step 5 In the *Begin* area, set the following parameters:

- **a.** Year to start the Accounting data query
- **b.** Month to start
- **c.** Day to start
- **d.** Hour to start
- **e.** Minute to start
- **f.** A.M. or P.M.

Step 6 In the *End* area, set the same parameters outlined in Step 5 to indicate when you want the Accounting data query to end.

Step 7 In the *Time Interval* area, select the appropriate interval for the query: *Hourly*, *Daily*, *Weekly*, *Monthly*, or *Annually*.

You have the option of proceeding with the data query by clicking the **Query** button or adding additional criteria to the data query by clicking the **Advanced Query** button.

Step 8 In the *Type of Data* area, select either **Summary Statistics** or **Detailed Statistics**.

Step 9 To initiate the Accounting query with the current query parameters, click **Query**.

You receive the following message:

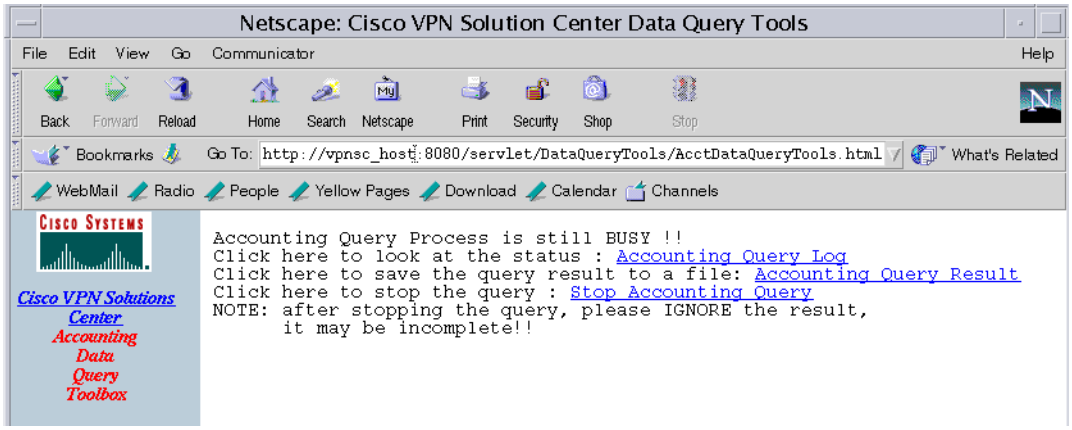
```
Accounting Data Query is starting; it may take some time. Do you really want to continue?
```

Step 10 Click **OK** to start the data query.

To cancel the query, click **Cancel**.

If you click **OK**, the page shown in Figure 5-5 appears

Figure 5-5 Choosing the Accounting Query Options



This page provides the following options:

- To view the query status, choose the **Accounting Query Log** link.
- To save the query result to a file, choose the **Accounting Query Result** link.
- To stop the query process, choose the **Stop Accounting Query** link.

Step 11 Choose the desired option to proceed.

Monitoring Performance Through Service Level Agreements

VPN Solutions Center software monitors performance through the service-level agreement (SLA) server. An SLA defines a service provided by a service provider to any customer. VPN Solutions Center monitors the service related performance criteria by provisioning and monitoring SLAs on routers that support the Service Assurance Agent (SA Agent) management information base (MIB). To provision the SLAs and to collect statistics for each SLA, the process of creating an SLA and collecting the data requires some user input, as described in this section.

The SLA server collects the relevant performance data, stores it persistently, and presents useful reports. The SLA server is based on the Service Assurance Agent (SA Agent) MIB. The MPLS VPN Solution software leverages the SA Agent MIB to monitor SLA performance. Service providers can monitor network traffic using any of the following protocols:

- Internet Control Message Protocol Echo (ICMP Echo)
- Transmission Control Protocol Connect (TCP Connect)
- User Datagram Protocol Echo (UDP Echo).
- Jitter (voice jitter)
- Dynamic Host Configuration Protocol (DHCP)
- Hyper text Transfer Protocol (HTTP)
- Domain Name System (DNS)

About the Service Assurance Agent Feature

The Service Assurance Agent (SA Agent) feature allows you to monitor network performance, network resources, and applications by measuring response times and availability. With this feature you can perform troubleshooting, problem notifications, and preventive analysis based on Service Assurance Agent statistics.

The SA Agent router uses the Cisco Round Trip Time Monitor (RTTMON) MIB. For more information on the RTTMON MIB, refer to the *Cisco MIB User Quick Reference*.

You can use the Service Assurance Agent feature to troubleshoot problems by checking the time delays between devices (such as between two CEs in a VPN) and the time delays on the path from the source device to the destination device at the protocol level.

You can use this feature to perform preventive analysis by scheduling the Service Assurance Agent and collecting the results as history and accumulated statistics. You can then use the statistics to model and predict future network topologies.

About SA Agent Traps

You can configure SA Agent traps per SLA probe. SA Agent can send three types of traps:

- *Connection Loss traps*. VPN Solutions Center sends a Connection Loss trap when an SLA probe detects a lost connection for a connection-oriented protocol. VPNSC sends a resolution trap the next time the operation is completed successfully.
- *Timeout traps*. When an operation delay exceeds the timeout value specified, VPNSC sends a Timeout trap.
- *Threshold traps*. When an operation delay meets a falling threshold value, VPNSC sends a Threshold trap.

The traps configuration encapsulates all three types of SA Agent traps.

In VPN Solutions Center, you can set traps per SLA either when you create an SLA or on an actively running SLA probe. When you configure traps during SLA creation, the traps are set before the SLA operation activates. In this case, VPNSC sends a trap in the event of a connection loss, a timeout, or threshold violation. When you configure a trap on an SLA probe that is already running, VPNSC does not send a trap after the first operation that triggers the trap until it sends the resolution trap.

An indication as to whether traps are sent on each SLA is recorded in the Repository. When a router reboots, VPNSC recreates the SLA and configures the traps according the data in the Repository.

Retrieving SA Agent Data with the XML Data Query Tool

VPN Solutions Center periodically collects Service Assurance Agent (SA Agent) performance data and places this data in the Repository. You can access the SA Agent data through web-based data query tools, as well as through customized reports or through CORBA APIs. The performance data retrieved by the web-based data query tools is saved to a file in XML format.

For related information regarding the retrieval of SLA definitions on SA Agent routers, see the "Retrieving SLA Data with the XML Data Query Tool" section on page 5-26.

To access the SA Agent Data Query Tools, follow these steps:

Step 1 From the VPN Console menu, choose **Monitoring > XML Data Query Tool**.

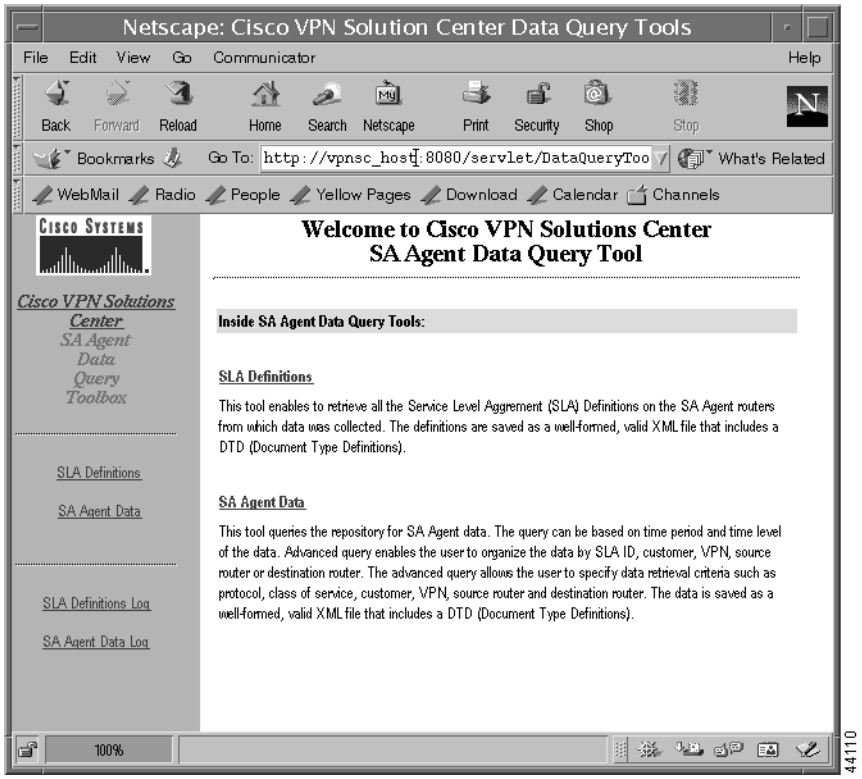
The Netscape browser comes up. The first time you access the web browser from the VPNSC software, you must log in.

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

The VPN Solutions Center Data Query Tools page appears.

Step 3 Choose **SA Agent Data Query Tool**. The SA Agent Data Query Tool page appears (see Figure 5-6).

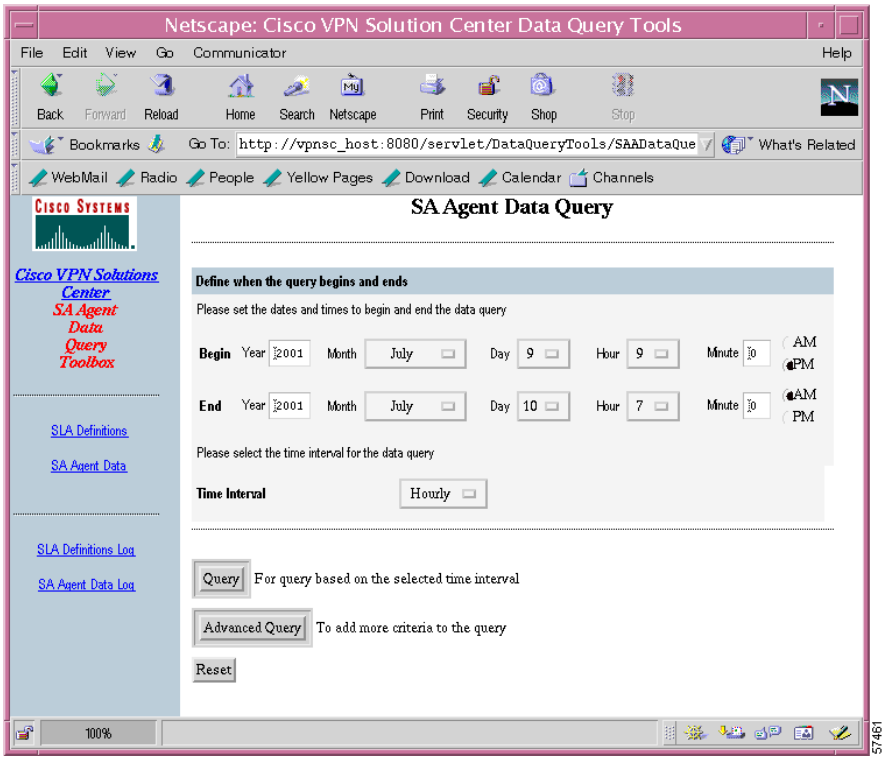
Figure 5-6 SA Agent Data Query Tool Page



Step 4 Choose **SA Agent Data**.

The SA Agent Data Query page appears (see Figure 5-7).

Figure 5-7 SA Agent Data Query Page



Step 5 In the *Begin* area, set the following parameters:

- **a.** Year to start the SA Agent data query
- **b.** Month to start
- **c.** Day to start
- **d.** Hour to start
- **e.** Minute to start
- **f.** A.M. or P.M.

Step 6 In the *End* area, set the same parameters outlined in Step 5 to indicate when you want the SA Agent data query to end.

Step 7 In the *Time Interval* area, select the appropriate interval for the query: *Hourly*, *Daily*, *Weekly*, *Monthly*, or *Annually*.

You have the option of proceeding with the data query by clicking the **Query** button or adding additional criteria to the data query by clicking the **Advanced Query** button.

Step 8 To initiate the SA Agent query with the current query parameters, click **Query**.

You receive the following message:

SA Agent Data Query is starting; it may take some time. Do you really want to continue?

Step 9 Click **OK** to start the data query.

To cancel the query, click **Cancel**.

If you click **OK**, the another page appears that provides the following options:

- To view the query status, choose the **Query SA Agent Log** link.

- To save the query result to a file, choose the **Query SA Agent Result** link.
- To stop the query process, choose the **Stop SA Agent Query** link.

Step 10 Choose the desired option to proceed.

Before You Create SLAs in VPN Solutions Center Software

Before you create SLAs in VPN Solutions Center software, you must enter some configuration changes on each CE and PE from which you want to collect performance data. To set up the CEs for SLAs, make sure the following conditions are met:

1. SNMP must be enabled and the SNMP read-only and read-write community strings must be set on all the PEs and CEs in the service provider's network. For instructions, 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.
2. The *rtr responder* software must be enabled on the CEs configured as SA Agent CEs. The rtr responder is automatically enabled when VPN Solutions Center software provisions a CE that is running SA Agent. Also see the "Enabling SA Agent on Edge Device Routers" section on page 2-11.

   Note The command syntax does not reflect the current terminology for the SA Agent. The terms "rtr" and SA Agent are equivalent.

   To enable the rtr responder software, enter the following command on each CE router that is running the SA Agent:

   ```
   rtr responder
   ```

3. To enable a UDP Echo SLA, enter the following command on the SA Agent CE router:

   ```
   service udp-small-servers
   ```

4. PEs and CEs in the Customer's VPN must be able to communicate with the HTTP server in the service provider network.
5. Verify that the targets are assigned and the IP addresses are populated into the Device Inventory Repository (see the next section for details).

Verifying SA Agent Targets and IP Addresses in the Repository

You must verify that the targets are assigned and the IP addresses are populated into the Device Inventory Repository for each target that is a source or destination for an SLA probe.

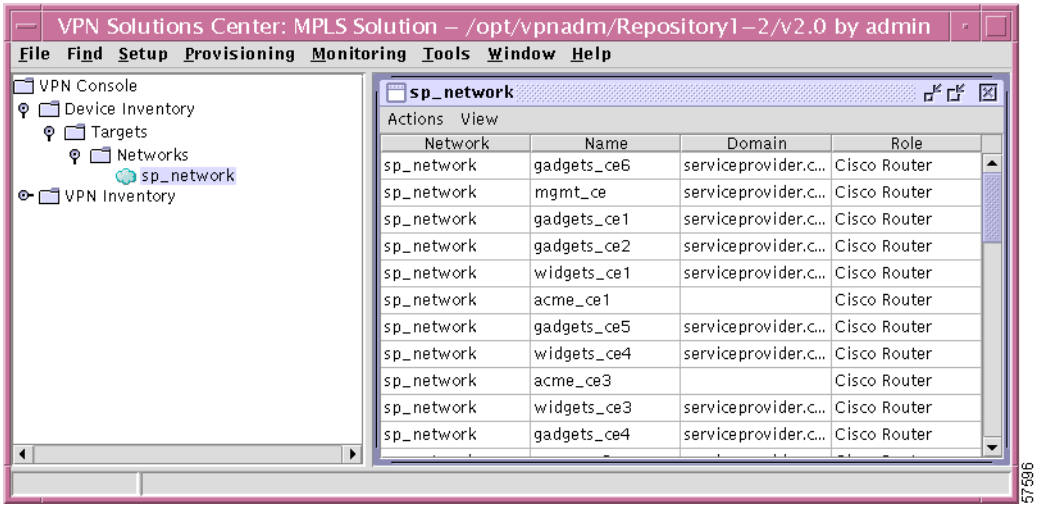
Tips The SA Agent can gather performance information from CEs only when they are managed CEs. Make sure that when you add a CE to VPN Customer that the CE is configured as a *managed CE* with either *Regular SA Agent* status or *Shadow SA Agent* status enabled. For information on modifying an existing CE definition to enable SA Agent, see the "Editing Customer Site and Site CE Definitions" section on page 3-8.

To verify router targets and IP addresses in the Device Inventory Repository, follow these steps:

Step 1 Bring up the VPN Console. In the hierarchy pane under the Device Inventory, double-click the name of the desired network listed in the Networks folder.

The Network window is displayed, as shown in Figure 5-8.

Figure 5-8 Network Window



Step 2 Select a row that lists the target router.

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

Step 4 Choose the **IP Addresses** tab.

A complete list of all currently populated IP addresses for the selected target (router) is displayed.

Populating IP Address Information to the Device Inventory Repository

If all IP addresses are not listed, you must populate the IP addresses in the Device Inventory Repository database as follows:

Step 1 From the VPN Console, choose **Monitoring** > **Configure Traps** > **Populate interface information for Cisco Router Targets**.

Step 2 Step through the Populate Interface Information wizard.

This wizard sets up a scheduled task that polls for information about router interfaces. It extracts the interface name, index number, and IP address and subnet mask for each interface. The collected interface information is stored with each router definition.

Step 3 If only a few IP address are missing, you can individually add IP addresses and click the **Add** button for each addition.

Refer to “Adding a New Router to the Network” section on page 2-36 for the steps to do this.

Creating an SLA

Each Service Level Agreement (SLA) is associated with a customer, the source and destination addresses on the target CEs, the protocol used for the SA Agent probe, and the threshold for delay. Before you can create an SLA, the SA Agent CE router must be:

- Assigned to the appropriate Customer(s)
- Configured for a valid VPN

When you create an SLA, VPN Solutions Center software creates an SA Agent probe on the target CE router. To create an SLA, follow these steps:

Step 1 From the VPN Console, choose **Monitoring** > **Provision SLA Definitions and Collect SLA Data.**

Step 2 The first wizard window is informational. Click **Next** to continue.

The Specify SLA Operation dialog box appears (see Figure 5-9).

Figure 5-9 Specifying the SLA Operation

As shown in Figure 5-9, you can create an SLA, delete an SLA, or collect data for SLA monitoring.

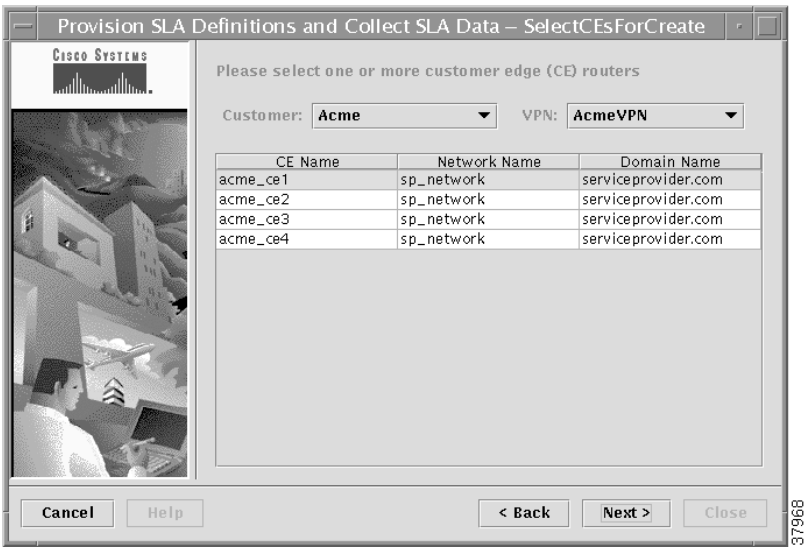
You can also enable or disable traps. For more information, see “About SA Agent Traps” section on page 5-11.

For information on creating, selecting, and deleting SLAs for APIs by using the command line interface, see the *Cisco VPN Solutions Center: MPLS Solution API Programmer Guide*.

Step 3 To create an SLA in VPN Solutions Center, choose **Create SLA**, then click **Next.**

The dialog box shown in Figure 5-10 directs you to select the source CE (or CEs)—that is, the CE you select here sends the SLA probe.

Figure 5-10 Selecting the Source CE(s) for the SLA Probe



Step 4 Select one or more source CEs for the SLA probe.

a. From the Customer drop-down list, choose the name of the customer.

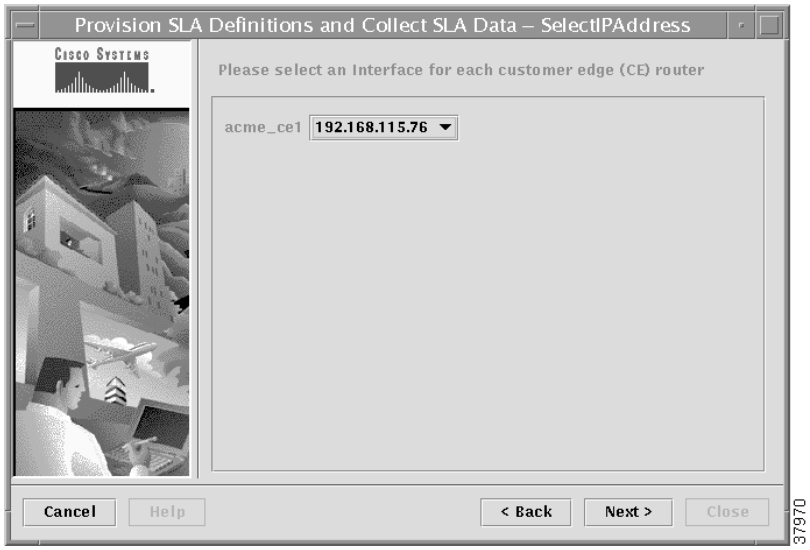
b. From the VPN drop-down list, choose the name of the VPN.

c. Select one or more source CEs for the SLA probe, then click **Next**.

To select multiple CEs from the list, hold down the **Ctrl** key, then click the additional router names.

The next dialog box directs you to indicate the source IP address for the source CE.

Figure 5-11 Select Source IP Address for SLA Probe

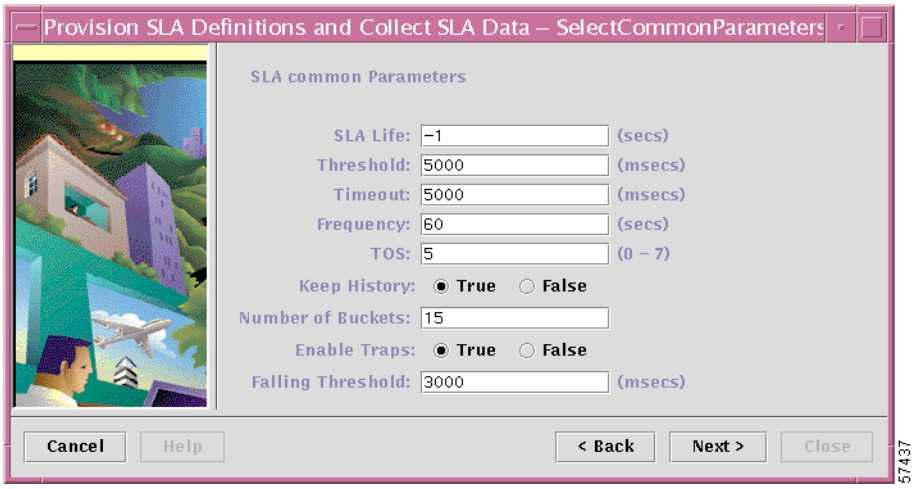


Step 5 From the drop-down list, choose the IP address for the appropriate interface on the source CE. The name of the selected CE is displayed to the left of the IP address.

When finished, click **Next**.

The next dialog box directs you to specify the common parameters for the SLA.

Figure 5-12 Specify SLA Common Parameters



Step 6 Enter the pertinent values for the SLA parameters common to each of the SLA protocols, then click **Next**.

The fields in the SLA Common Parameters dialog box are as follows:

- *SLA Life* is the number of seconds that the probe will be active (with the maximum value of a 32-bit integer in seconds). If the value is set to **-1**, the typical value, the probe is active indefinitely. The default value is **-1**.
- *Threshold* is an integer that defines the threshold limit in milliseconds. The maximum value is the maximum value of a 32-bit integer. If the SA Agent operation time exceeds this limit, the threshold violation is recorded by the SA Agent. The default value is **5000**.
- *Timeout* is the duration in milliseconds to wait for an SA Agent operation completion. The value for *Timeout* must be less than the value for *Frequency*. The default value is **5000**.
- *Frequency* is the duration in seconds between initiating each SA Agent operation. The default value is **60**.
- *TOS* is an integer (ranging from **0** to **7**) that represents the type of service (ToS) bits in an IP header. The default value is **0**. Table 5-1 defines the *TOS* values.

Table 5-1 Meanings of TOS Values in SLA Parameters

ToS Value	Binary Value	Meaning
7	111	In contract, best class
6	110	In contract, second best class
5	101	In contract, third best class
4	100	In contract, worst class
3	011	Out of contract, best class
2	010	Out of contract, second best class

Table 5-1 Meanings of TOS Values in SLA Parameters (continued)

ToS Value	Binary Value	Meaning
1	001	Out of contract, third best class
0	000	Out of contract, worst class

Step 7 Set the next set of SLA parameters as necessary:

a. *Keep History*

The VPN Solutions Center history table records the round trip time (that is, the delay) of operations in milliseconds. The history table does not apply to the jitter and http SLA probes.

The statistics table, which is unrelated to the history table, records the sum of the round trip times, calculates averages, and records the minimum and maximum delay values.

When you set the *Keep History* parameter to **True**, it configures the SLA probe to keep both the history table and statistics table.

b. *Numbered Buckets*

The *Numbered Buckets* parameter determines the number of samples saved for each operation. This parameter indicates the number of history delay values retained in the history table.

c. *Enable Traps*

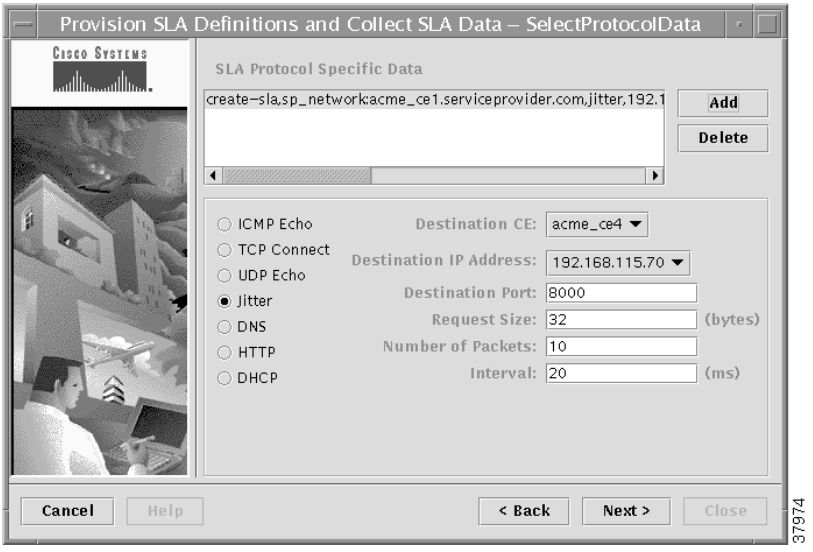
When you set *Enable Traps* for a new SLA probe, the traps are set before the SLA operation activates. VPN Solutions Center sends a trap in the event of a timeout, a connection loss, or threshold violation (see also "About SA Agent Traps" section on page 5-11).

d. *Falling Threshold*

If you enable traps for the SLA, you must specify the *Falling Threshold* value, which triggers a threshold resolution trap. The default is 3000 milliseconds.

The next dialog box (see Figure 5-13) directs you to specify the type of SLA protocol and set its corresponding parameters.

Figure 5-13 Select SLA Protocol Data Parameters



Step 8 Select one or more SLA protocols and enter the values for the fields associated with them.

- Internet Control Message Protocol Echo (ICMP Echo)
- Transmission Control Protocol Connect (TCP Connect)
- User Datagram Protocol Echo (UDP Echo).
- Jitter (voice jitter)
- Dynamic Host Configuration Protocol (DHCP)
- Hyper text Transfer Protocol (HTTP)
- Domain Name System (DNS)

Step 9 Be sure to select the appropriate *Destination CE* and the corresponding *Destination IP Address*. Then complete the other fields as necessary.

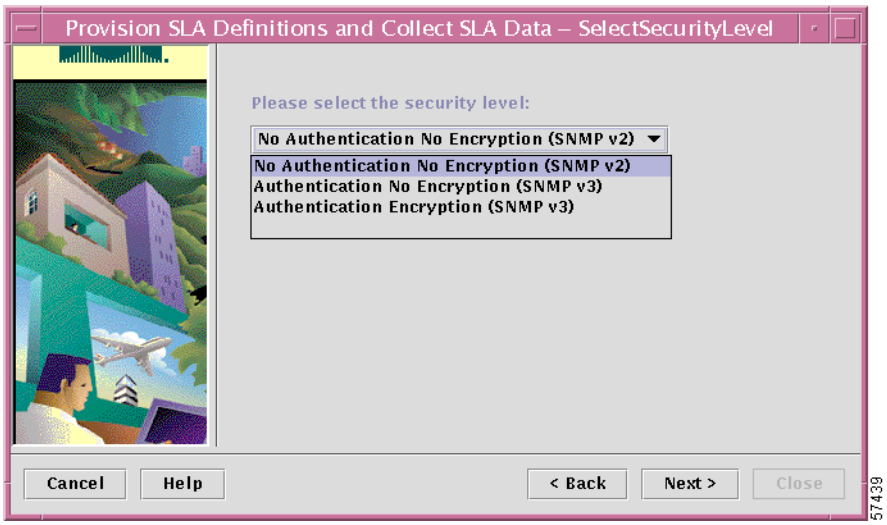
You can add additional protocols as desired.

Step 10 When finished specifying the SLA protocol probes, click **Add**. Then click **Next**.

For details on the parameters and values for each SLA protocol listed here, refer to "Provision SLA Definitions and Collect SLA Data" in Chapter 9 of the *Cisco VPN Solutions Center: MPLS Solution User Reference*.

The dialog box shown in Figure 5-14 directs you to select the SNMP security level for the SLA.

Figure 5-14 Specifying the SNMP Security Level



Step 11 From the drop-down list, choose the appropriate SNMP security level:

- *No Authentication, No Encryption (SNMPv2)*
- *Authentication, No Encryption (SNMPv3)*
- *Authentication, Encryption (SNMPv3)*

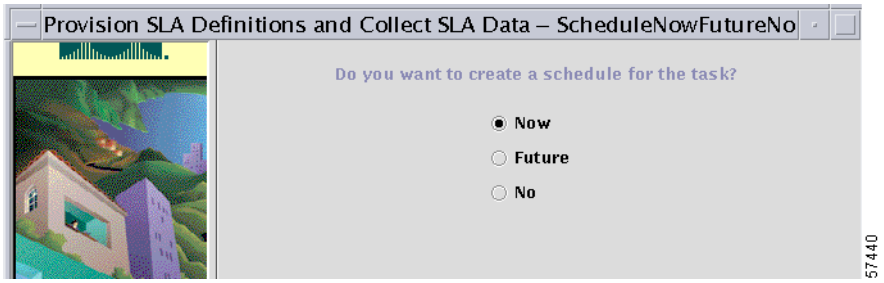
When you have selected the SNMP security level for this SLA, click **Next**.

Step 12 Enter a unique task name, then click **Next**.

To help you specify a unique task name, the Task Name drop-down list shows the list of existing task names.

The dialog box shown in Figure 5-15 asks if and when you want to schedule the task.

Figure 5-15 Specifying When to Run the Task



You have three options:

- *Now*. The task is scheduled to run immediately.
- *Future*. The Schedule dialog box appears.
- *No*. The SLA task is canceled.

Step 13 Choose **Now** to run the task now; or choose **Future** to schedule the task, then click **Next**.

Step 14 If you choose to schedule the task for some time in the future, from the Schedule dialog box, set all the pertinent scheduling information, then click **Add**.

The SLA is added to the Schedule List (and displayed in the upper pane).

Step 15 Click **Next** twice, then click **Close**.

Configuring VPN Solutions Center to Collect SA Agent Data for an SLA

When you collect data for SLA monitoring, VPN Solutions Center software downloads SLA statistics collected over the last hour from one or more specified routers. The specified routers must have the SA Agent probes configured on them. For information on defining a CE as a router running SA Agent, see the "Defining the Customer Sites" section on page 3-2.

Note When you initially create an SLA, you must wait at least sixty minutes before attempting to collect SLA data. If you try to collect SLA data before sixty minutes elapses, the data will not yet be available and the SLA reports will be empty.

To collect SA Agent data for SLAs, follow these steps:

Step 1 From the VPN Console, choose **Monitoring** > **Provision SLA Definitions and Collect SLA Data.**

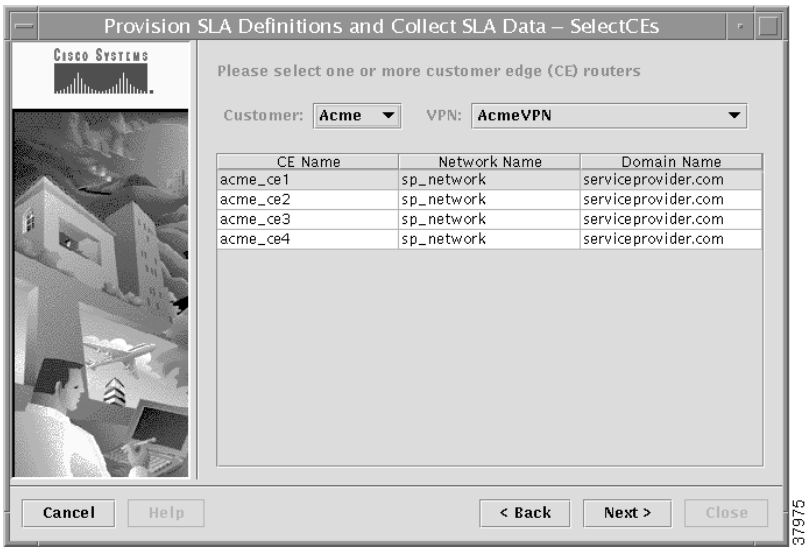
Step 2 The first wizard window is informational. Click **Next** to continue.

The Specify SLA Operation dialog box is displayed. From this dialog box, you can choose to create an SLA, delete an SLA, or collect data for SLA monitoring.

Step 3 Choose **Collect Data for SLA Monitoring**, then click **Next**.

The dialog box shown in Figure 5-16 appears and directs you to select the source CE for the SLA probe (or CEs). The CE you select here sends the SLA probe to the routers that have SA Agent enabled.

Figure 5-16 Select Source CE for SLA Probe



a. Choose the appropriate Customer from the Customer drop-down list.

b. Choose the appropriate VPN from the VPN drop-down list.

c. Select one or more CEs from which you want to collect SLA data, then click **Next**.

Step 4 Provide a unique task name, then click **Next.**

To help you specify a unique task name, the Task Name drop-down list shows the list of existing task names.

The next dialog box asks if and when you want to schedule the task. You have three options:

- *Now.* The task is scheduled to run immediately.
- *Future*. The Schedule dialog box appears.
- *No*. The SLA task is canceled.

Step 5 Choose **Now** to run the task now; or choose **Future** to schedule the task, then click **Next**.

Step 6 If you choose to schedule the task for some time in the future, from the Schedule dialog box, set all the pertinent scheduling information, then click **Add**.

The SLA is added to the Schedule List (and displayed in the upper pane).

For detailed information about scheduling, refer to Chapter 13, "Scheduling," in the *Cisco VPN Solutions Center: MPLS Solutions User Reference*.

Step 7 To save the SA Agent collection task, click **Next**.

If you chose to schedule the SA Agent collection task, that will also occur.

You are informed that all steps are done.

Step 8 Click **Close** to close the wizard.

When you have collected data for SLAs, you can view the data (see the "Viewing SLA Reports" section on page 5-25).

Deleting an SLA

Deleting an SLA from VPN Solutions Center deletes an SA Agent probe from the source CE router.

Step 1 From the VPN Console, choose **Monitoring > Provision SLA Definitions and Collect SLA Data.**

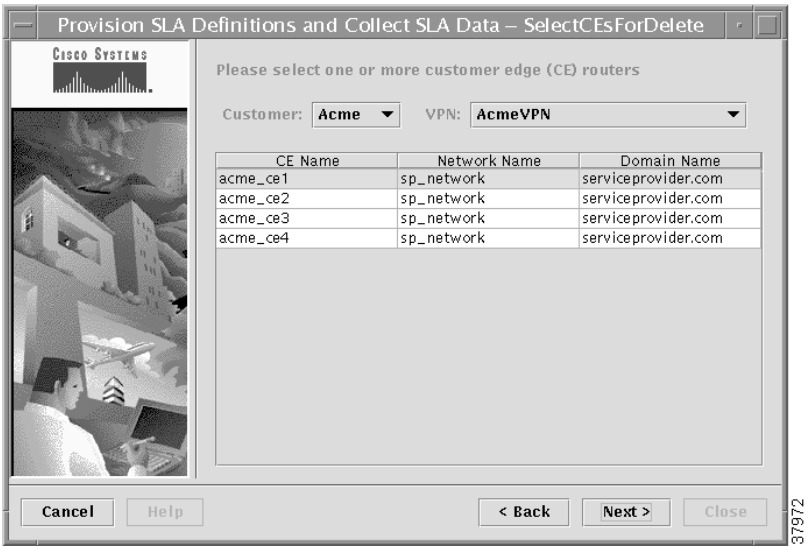
Step 2 The first wizard window is informational. Click **Next** to continue.

The Specify SLA Operation dialog box is displayed (as shown in Figure 5-9).

Step 3 To delete an SLA in VPN Solutions Center, choose **Delete SLA**, then click **Next**.

The dialog box shown in Figure 5-17 appears.

Figure 5-17 Select Source CE of SLA



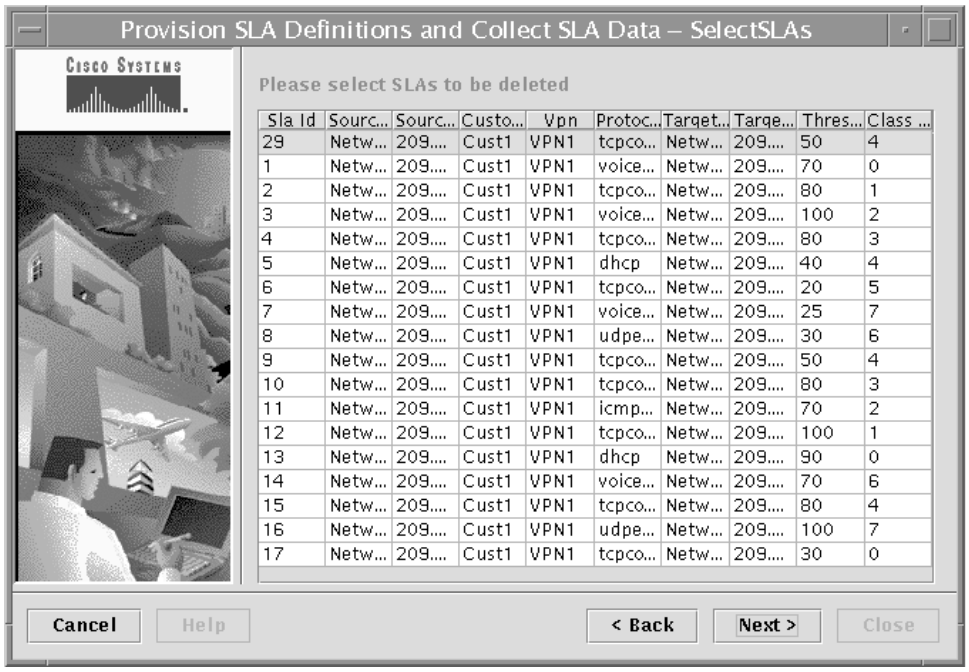
Step 4 In the **Customer** and **VPN** drop-down lists, select the pertinent Customer name and VPN name.

The CE pane lists all the CEs in the selected VPN that are running SA Agent.

Step 5 Select the name of the source CE for the SLA probe you want to delete, then click **Next**.

The next dialog box directs you to select the SLA you want to delete.

Figure 5-18 Select SLAs to Delete



Step 6 Click the appropriate lines in the list to select the SLAs you want to delete, then click **Next**.

To select multiple items, hold down the **Ctrl** key and click each item you want to add.

Step 7 Enter a unique task name, then click **Next**.

Step 8 Choose the default (**Yes**) to proceed to schedule the task, then click **Next**.

Step 9 From the Schedule dialog box, set all the pertinent scheduling information, then click **Add**.

The SLA deletion request is added to the Schedule List (and displayed in the upper pane).

Step 10 Click **Next** twice, then click **Close**.

Viewing SLA Reports

After collecting SA Agent data for SLA, choose **Monitoring**>**View SLA Reports**, then select the specific type of report you require.

Note For details on each type of SLA report, refer to "View SLA Reports" in Chapter 9 of the *Cisco VPN Solutions Center: MPLS VPN User Reference*.

The specific report types are as follows:

- Summary Report

  These reports are time-based reports that show the following parameters: *Connectivity* as a percentage, *Maximum Delay* in milliseconds, and *Threshold Violation* as a percentage. These parameters are available in annual, monthly, weekly, daily, and hourly reports. For each parameter, you can generate detailed reports that show more related parameters. The reports can be organized by source router (the source CE of the SLA), SLA identifier, customer name, or VPN name.

- Jitter Report

  Displays statistics that are measured only by Voice Jitter SLAs originated in a selected router. The reports are time-based. They show hourly, daily, weekly, monthly, and annual data and can be organized by SLA ID, destination router, VPN, Customer, or Unspecified.

- HTTP Report

  Displays statistics that are measured only by HTTP SLAs. The reports are time-based, and they show data in the following time increments: hourly, daily, weekly, monthly, and annually. Data can be organized by SLA ID, source router, VPN, or Customer.

  The Summary HTTP Report displays the connectivity, maximum delay, and threshold violation (as in the Summary Report). The Stages HTTP Report displays the round trip time, timeouts, and the error distribution among different HTTP stages: DNS lookup, TCP connect, and Transaction.

- Customer Packet Drop (CE-CE) Report

  Shows the packet drop percentage among CEs of a specific customer. This information is measured only for the SLAs with the jitter protocol. The reports are organized by class of service. The reports are annually, monthly, weekly, daily, and hourly. You can navigate along the time scale.

- Customer Round Trip Delay (CE-CE) Report

  Shows the maximum, minimum, and average round-trip time (in milliseconds) among the CEs of a specific customer. The statistics are for all the probe types. The reports are organized by class of service. The reports are annually, monthly, weekly, daily, and hourly. You can navigate along the time scale.

- Network Packet Drop (PE-PE) Report

  Shows the packet drop percentage among all the shadow SA Agent CEs in the network. The network packet drop between PEs is measured by the shadow SA Agent CEs that are connected to the PEs. This information is measured only for the SLAs with the jitter protocol. The reports are organized by class of service. The reports are annually, monthly, weekly, daily, and hourly. You can navigate along the time scale.

- Network Round Trip Delay (PE-PE) Report

  Shows the maximum, minimum, and average round-trip time among shadow SA Agent CEs in the network. The statistics are for all the probe types. The reports are aggregated by class of service. The reports are annually, monthly, weekly, daily, and hourly. The user can navigate along the time scale.

- SLA Definition Report

  Shows all the SLAs on the SA Agent routers from which data was collected. The SLA Definition report shows the SLA ID given to each SLA. SLAs in the report may have been deleted but are kept in the SLA Definition to match the old collected data.

Retrieving SLA Data with the XML Data Query Tool

VPN Solutions Center allows you to retrieve Service Level Agreement (SLA) definitions on the Service Assurance Agent (SA Agent) routers from which data has been collected. You can either retrieve all the SLA definitions on the SA Agent routers, or only the SLA definitions that are currently active.

You can access the SLA data through web-based data query tools, as well as through customized reports or through CORBA APIs. The data retrieved by the web-based data query tools is saved to a file in XML format that includes a Document Type Definition (DTD).

To access the interface statistics Data Query Tools, follow these steps:

Step 1 From the VPN Console menu, choose **Monitoring > XML Data Query Tool**.

The first time you access the web browser from the VPNSC software, you must log in.

Step 2 In the Netscape Password dialog box, enter your user name and password, then click **OK**.

The VPN Solutions Center Data Query Tools page appears.

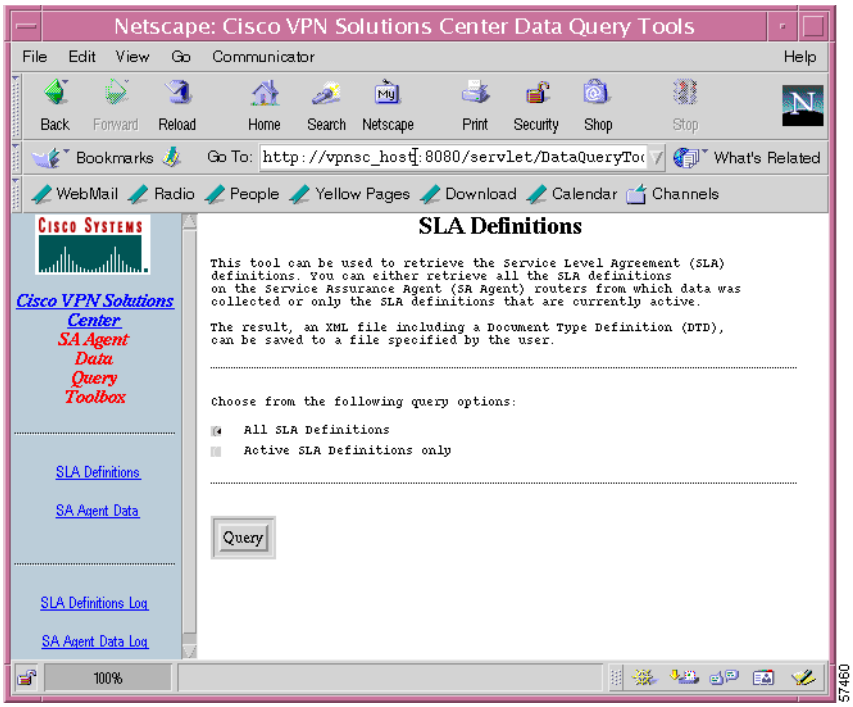
Step 3 Choose **SA Agent Data Query Tool**.

The SA Agent Query Tools page appears. This page provides two options: **SLA Definitions** and **SA Agent Data**.

Step 4 From this page, choose **SLA Definitions**.

The SLA Definitions Query page appears (see Figure 5-19).

Figure 5-19 SLA Definitions Query Page



Step 5 Choose one of the following query options:

- **All SLA Definitions**
- **Active SLA Definitions only**

Step 6 Click **Query**.

You receive the following message:

SLA Definitions Data Query is starting. Do you really want to continue?

Step 7 Click **OK** to start the data query.

To cancel the query, click **Cancel**.

The next page that appears gives you the following options:

- To view the query status, choose **SA Agent Query Log**.
- To save the query result to a file, choose **Save Result**.

Step 8 Choose the desired option to proceed.

Using CAR to Monitor Data

Committed Access Rate (CAR) is the underlying software base for both packet classification and access rate-limiting functionality. CAR provides the status for each interface on each router configured with CAR. CAR controls IP traffic transmission rates into the network during periods of network congestion. CAR achieves this control through rate limiting (with burst capabilities), and classifies and marks packets using IP precedence and QoS group settings.

CAR provides several fundamental capabilities:

- *Traffic matching*

  CAR can identify traffic of interest for limiting access rate or setting the precedence (or both). Rate policies can be associated with one of the following:

  – All IP traffic
  – IP precedence (defined by a rate-limit access list)
  – QoS group
  – MAC address (defined by a rate-limit access list)
  – IP access list (standard and extended)

- *Traffic measurement*

  CAR utilizes a token bucket measurement mechanism. Tokens are inserted into the bucket at the committed rate. The depth of the bucket is the burst size. When traffic arrives at the bucket, if sufficient tokens are available, the traffic is said to conform and the corresponding number of tokens are removed from the bucket. If sufficient tokens are not available, the traffic is said to exceed. Note that unlike leaky bucket implementations, the token bucket does not delay the traffic.

- *Configurable action policies*

  The network operator can specify policies to be executed for traffic, which either conforms to or exceeds a specified rate limit.

Rate-Limiting Functionality

CAR's rate-limiting functionality provides the network operator with the means to define Layer 3 aggregate or granular access or egress bandwidth rate limits and to specify traffic handling policies when the traffic either conforms to or exceeds the specified rate limits. Aggregate access means matching all of the packets on an interface or subinterface. Granular access means matching a particular type of traffic based on precedence, MAC address, or other parameters.

You can specify CAR rate-limiting policies based on criteria including physical port, packet classification, IP address, MAC address, application flow, or other criteria specifiable by access lists or extended access lists. CAR rate limits can be implemented either on input or output interfaces or subinterfaces including frame relay and ATM subinterfaces.

CAR utilizes a token bucket; thus CAR can pass temporary bursts that exceed the rate limit as long as tokens are available. CAR does not smooth or shape the traffic and thus does no buffering (and adds no delay). CAR provides managed discard between the excess burst and extended excess burst parameters and CAR is highly optimized to run on high-speed links.

CAR also includes a new set of algorithms that provide highly efficient execution of aggregate rate limits (matching all traffic on an interface or subinterface), as well as rate limits that match specific IP precedence values and MAC addresses.

Setting Up the Service Provider Network for CAR

Setting up the service provider network in preparation for generating and collecting CAR data requires the following steps:

1. Configure each PE and CE in the network.
2. Populate the router's interface information to the Repository.

   This task is performed in VPN Solutions Center software.
3. Poll each router's CAR MIB.

   This task is performed in VPN Solutions Center software.

Platform and Cisco IOS Support

CAR does not run on all Cisco routers. At this time, CAR is supported on the following platforms:

- Cisco 2600 Series
- Cisco 3600 Series
- Cisco 4500 Series
- Cisco 4700 Series
- Cisco 7200 Series

CAR requires Cisco IOS 12.0(7) or later.

Distributed CAR (DCAR) is supported on Cisco 7000 series routers with a route switch processor-based RSP7000 interface processor or a Cisco 7500 series router with a Versatile Interface Processor-based VIP2-40 or greater interface processor.

CAR and DCAR can be configured on an interface or subinterface. However, CAR and DCAR are not supported on Fast EtherChannel, tunnel, or PRI interfaces, nor on any interface that does not support Cisco Express Forwarding (CEF). CEF must be enabled on the interface before configuring CAR or DCAR.

Note Cisco assumes that a service provider network administrator is responsible for configuring CAR on the network's PEs and managed CEs.

CAR reports are organized by both the Network and the Customer. You can generate Customer reports only if CAR is configured the CEs and data has been collected from the CEs. To generate Customer-based reports, CEs collecting CAR data must be managed CEs.

Simple CAR Configuration Example

The following configuration example illustrates how to configure a basic CAR policy that allows all IP traffic.

In the example, assume the network operator delivered a physical T3 link to the customer, but offered a less expensive 20 MBPS subrate service. The customer pays only for the subrate bandwidth, which can be upgraded with additional access bandwidth.

The CAR policy configured here limits the traffic rate available to the customer and delivered to the network to the agreed upon rate limit, plus providing the ability to briefly burst over the limit.

```
interface hssi 0/0/0
rate-limit output 200000000 24000 3200 conform-action transmit exceed-action drop
ip address 209.165.200.225 255.255.255.0
```

To verify the configuration and monitor CAR statistics, use the **show interfaces rate-limit** command:

```
Router# show interfaces hssi 0/0/0 rate-limit
```

Setting Up CAR Data Collection in VPN Solutions Center

To gather and view CAR data in VPN Solutions Center software, you must complete two tasks:

- Populate the router interface information to the Device Inventory Repository.
- Poll the routers' CAR MIB.

Populating Interface Information to the Device Inventory Repository

Prior to polling a router's CAR MIB, you must populate the router interfaces.

To populate the interface information for all managed devices in the Device Inventory Repository, follow these steps:

Step 1 From the VPN Console, choose **Monitoring**>**Configure Traps** > **Populate interface information for Cisco Router Targets**.

Step 2 Step through the Populate Interface Information wizard.

This wizard sets up a scheduled task that polls for information about router interfaces. It extracts the interface name, index number, and IP address and subnet mask for each interface. The collected interface information is stored with each router definition.

Polling a Router's CAR MIB

To poll a router's CAR MIB, follow these steps:

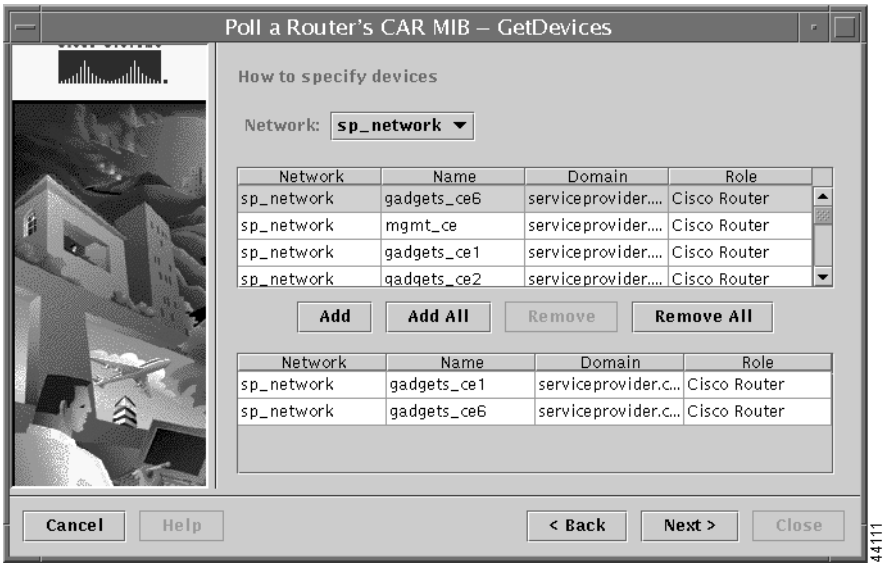
Step 1 From the VPN Console, choose **Monitoring > Poll a Router's CAR MIB**.

This wizard creates a task to poll the selected Cisco routers for data from the CAR MIB.

Step 2 Click **Next** twice to step through the introductory windows.

The next dialog box (see Figure 5-20) allows you to specify which devices to poll for CAR information.

Figure 5-20 Specifying CAR Devices



Step 3 From the Network drop-down list, choose the pertinent network.

This dialog box has two panels. The upper panel displays the routers in the selected network. The lower panel will display the routers you want to be polled for CAR data.

Step 4 From the upper panel, select the routers you want to be polled for CAR data.

- If you want all the routers to be polled, click **Add All**.
- If you want some routers, but not others, to be polled, select each router, then click **Add**.

When you click **Add** or **Add All**, the selected routers are displayed in the lower panel.

If you need to remove any of the routers from the lower panel, click **Remove** to remove individual routers; or click **Remove All** to remove the entire list from the lower panel.

Step 5 When finished defining the list of routers to be polled, click **Next**.

Step 6 Enter a unique task name, then click **Next**.

Step 7 Choose the default (**Yes**) to proceed to schedule the task, then click **Next**.

Step 8 From the Schedule dialog box, set all the pertinent scheduling information, then click **Add**.

Tips Cisco recommends that you schedule the polling task to occur every fifteen minutes. This requires four separate tasks to be scheduled, each starting fifteen minutes apart and reoccurring every hour.

Note You may discover that you need to increase the frequency of polling for CAR data, depending on the speed of the device interfaces and the volume of traffic on the router that is being polled.

The polling request is added to the Schedule List (displayed in the upper pane).

Step 9 Click **Next** twice, then click **Close**.

Viewing CAR MIB Reports

The CAR MIB status data is collected in the Repository. The report data is organized first by *Customer* and *Network*. Each of these reports can be generated on an hourly, daily, weekly, monthly, and yearly basis.

Step 1 To view the data, choose **Monitoring > View CAR MIB Reports**.

Step 2 From the menu, choose either **By Customer** or **By Network**.

- If you choose **By Customer**, the CAR MIB Report by Customer appears.
- If you choose, **By Network**, the CAR MIB Report by Network appears.

For detailed information on these reports, refer to "View CAR MIB Reports" in Chapter 9 of the *Cisco VPN Solutions Center: MPLS Solution User Reference, Release 2.0.*

Retrieving CAR MIB Data with the XML Data Query Tool

VPN Solutions Center periodically collects CAR MIB performance data and places this data in the Repository. You can access the CAR MIB data through web-based data query tools, as well as through customized reports. The performance data retrieved by the web-based data query tools is saved to a file in XML format.

The CAR MIB Data Query Tool queries the Repository for CAR MIB status data. The data is saved in an XML file that includes a Document Type Definition (DTD). CAR MIBs provide the status for the token bucket parameters and their associated access list. You can retrieve the status data for the following categories:

- The managed CEs that belong to the Customer
- The managed CEs that belong to the Customer Site
- The PEs in the specified network
- Routers

To access the CAR MIB Data Query Tools, follow these steps:

Step 1 From the VPN Console menu, choose **Monitoring > XML Data Query Tool**.

The first time you access the web browser from the VPNSC software, you must log in.

Step 2 In the Netscape Password dialog box, enter your user name and password, then click **OK**.

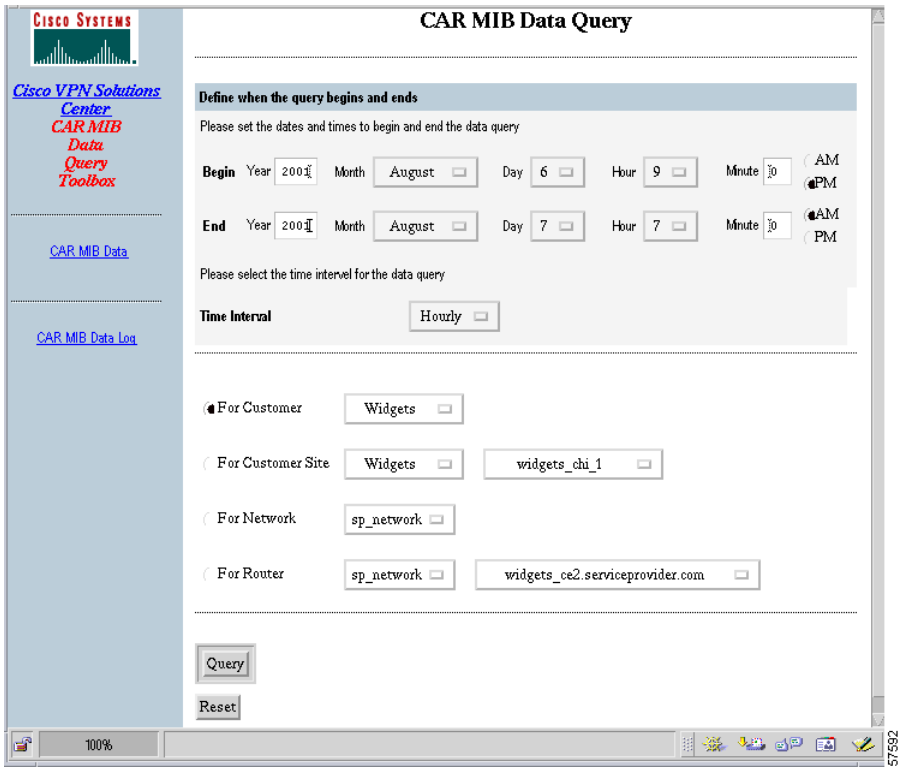
The VPN Solutions Center Data Query Tools page appears.

Step 3 Choose **CAR MIB Data Query Tool**. The CAR MIB Data Query Tool page appears.

Step 4 From this page, choose **CAR MIB Data**.

The CAR MIB Data Query page appears (see Figure 5-21).

Figure 5-21 CAR MIB Data Query Page



Step 5 In the *Begin* area, set the following parameters:

- **a.** Year to start the CAR MIB data query
- **b.** Month to start
- **c.** Day to start
- **d.** Hour to start
- **e.** Minute to start
- **f.** A.M or P.M.

Step 6 In the *End* area, set the same parameters outlined in Step 5 to indicate when you want the CAR MIB data query to end.

Step 7 In the *Time Interval* area, select the appropriate interval for the query: *Hourly*, *Daily*, *Weekly*, *Monthly*, or *Annually*.

Step 8 To initiate the CAR MIB query with the current query parameters, click **Query**.

You receive the following message:

CAR MIB Data Query is starting; it may take some time. Do you really want to continue?

Step 9 To start the data query, click **OK**.

To cancel the query, click **Cancel**.

If you click **OK** to start the query, the next page that appears gives you the following options:

- To view the query status, choose **CAR MIB Query Log**.

- To save the query result to a file, choose **CAR MIB Query Result**.
- To stop the query operation, choose **Stop CAR MIB Query**.

Step 10 Choose the desired option to proceed.

Retrieving Interface Statistics with the XML Data Query Tool

VPN Solutions Center periodically collects interface statistics data and places this data in the Repository. You can access the interface statistics data through web-based data query tools. The data retrieved by the web-based data query tools is saved to a file in XML format that includes a Document Type Definition (DTD).

The data query tool collects and saves the interface statistics by router. The statistics include packet counters for router interfaces. You must identify the interfaces by *index number*, which is a unique and constant number, at least from one initialization of the router's network management system to another. The counters are wrapped around numbers with a maximum value of 2 to the power of 32 minus 1.

To access the interface statistics Data Query Tools, follow these steps:

Step 1 From the VPN Console menu, choose **Monitoring > XML Data Query Tool**.

The first time you access the web browser from the VPNSC software, you must log in.

Step 2 In the Netscape Password dialog box, enter your user name and password, then click **OK**.

The VPN Solutions Center Data Query Tools page appears.

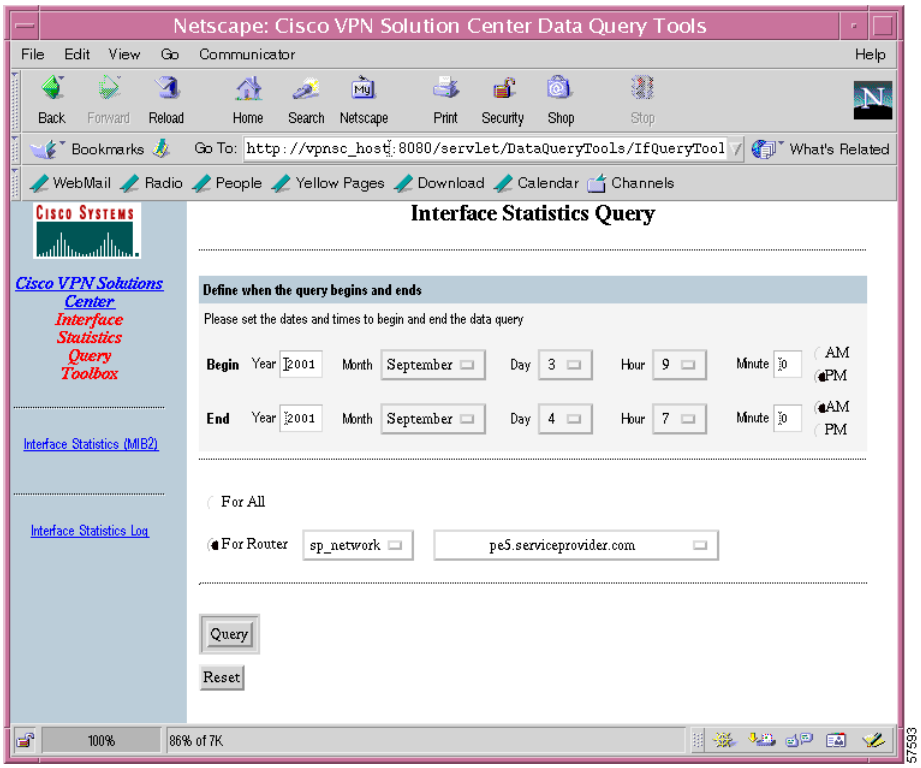
Step 3 Choose **Interface Stats (MIB2) Query Tool**.

The Interface Stats (MIB2) Query Tool page appears.

Step 4 From this page, choose **Interface Statistics**.

The Interface Statistics Query page appears (see Figure 5-22).

Figure 5-22 Interface Statistics Query Page



Step 5 In the *Begin* area, set the following parameters:

a. Year to start the Accounting data query

b. Month to start

c. Day to start

d. Hour to start

e. Minute to start

f. A.M. or P.M.

Step 6 In the *End* area, set the same parameters outlined in Step 5 to indicate when you want the Accounting data query to end.

Step 7 In the *Time Interval* area, select the appropriate interval for the query: *Hourly, Daily, Weekly, Monthly,* or *Annually.*

Step 8 You have the option of retrieving interface statistics for all the routers in the network or for a specific router.

- To retrieve interface statistics for all the routers, choose the **For All** radio button.
- To retrieve interface statistics for a specific router, choose the **For Router** radio button, then specify the network and router name.

Step 9 To initiate the interface statistics query, click **Query**.

You receive the following message:

```
Interface Statistics Query is starting; it may take some time. Do you really want to
continue?
```

Step 10 To start the data query, click **OK**.

To cancel the query, click **Cancel**.

If you click **OK**, the next page that appears gives you the following options:

- To view the query status, choose **Interface Statistics Query Log**.
- To save the query result to a file, choose **Interface Statistics Query Result**.
- To stop the query process, choose **Stop Interface Statistics Query**.

Step 11 Choose the desired option to proceed.

Collecting Only Changed Configuration Files

Router configuration files are usually collected at regular intervals and then examined for changes that affect the way the routers function. While the routers whose configuration files have changed are the only ones that need to be collected, the normal collection process does not separate the routers whose configuration files have changed from the routers whose configuration files have not. SmartCollector finds the routers whose configuration files have changed and puts them in a group to have their configuration files collected.

With SmartCollector, VPN Solutions Center creates a task and schedules it to be run once. When the task executes, all the targeted routers are instructed to advise the VPN Solutions Center software that uses the Simple Network Management Protocol (SNMP) of any change to their configuration files. MPLS VPN Solution, through the trapcatcher daemon, notes these traps and keeps track of the routers whose configuration files have changed, and thus need to be collected. The purpose of configuring traps (through SmartCollector) is to efficiently collect router configuration files from a set of routers that can belong to more than one network.

An example of the potential substantial savings is a scenario in which a network has 200 routers, but the configuration files for only 20 of the routers have changed. In this example, SmartCollector collects only the configuration files for the 20 that have changed rather than for all 200 routers. If only 10 percent of the routers have their configuration files changed between scheduled collections, each SmartCollection takes only 10 percent of the resources of a full collection.

Note that periodically (as determined by the *cycle_t* variable in the *csm.properties* file), the scheduler ignores the reduced target list and collects from all routers in the original target list. Thus even those routers whose traps failed to reach the MPLS VPN Solution are collected periodically.

- Prior to configuring traps, be sure to set up the appropriate routers for collection as described in the “Setting Up Routers for Collecting Configuration Files” section on page 4-45.
- 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 the SNMP community strings are set 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.

Populating Router Interface Information to the Repository

Prior to registering the configuration file change traps, you must populate the router interface information in the Repository, as follows:

Step 1 From the VPN Console, choose **Monitoring**>**Configure Traps** > **Populate interface information for Cisco Router Targets**.

Step 2 Step through the Populate Interface Information wizard.

This wizard sets up a scheduled task that polls for information about router interfaces. It extracts the interface name, index number, and IP address and subnet mask for each interface. The collected interface information is stored with each router definition.

This information is used to create the various accounting reports and to map the "config-change" traps to the appropriate routers.

Registering for Changed Configuration File Traps

This section explains how to register traps for changed configuration files, which indicates the routers for which data will be collected only if the routers have changed.

Step 1 From the VPN Console, choose **Monitoring**>**Configure Traps > Register for Config-Change Traps**.

This wizard configures selected Cisco routers to send "config-change" traps to the current VPN Solutions Center workstation. This enables SmartCollection, through which configuration files are collected only from those routers whose configuration files have changed.

Note If configuration file collection tasks are running and you initiate SmartCollection by registering for traps, the PEs *must* be IOS version 12.x to return traps.

Step 2 Step through the wizard.

Deregistering for Changed Configuration File Traps

This section explains how to deregister the traps for changed configuration files.

Step 1 From the VPN Console, choose **Monitoring**>**Configure Traps > Deregister for Config-Change Traps**.

This wizard configures selected Cisco routers to stop sending "config-change" traps to the current VPN Solutions Center workstation. The selected routers will no longer be part of SmartCollection, through which configuration files are collected only from those routers whose configuration files have changed.

Step 2 Step through the wizard.