Monitoring

From the Home window of Cisco IP Solution Center (ISC), you receive upon logging in, click the **Monitoring** tab and you receive a window as shown in Figure 7-1, "Monitoring Selections."

Figure 7-1 Monitoring Selections

Next you can navigate to the following selections:

- **Task Manager, page 7-1** Create and schedule tasks and monitor task run details.
- **Ping, page 7-8** Perform Ping connectivity tests.
- **SLA, page 7-14** Manage probes and view reports.
- **TEM Performance Report, page 7-59** TEM performance report.

Task Manager

ISC provides a Task Manager that allows you to view pertinent information about both current and expired tasks of all types, and to create and schedule new tasks, delete specified tasks, and delete the active and expired tasks.

This section contains the following subsections:

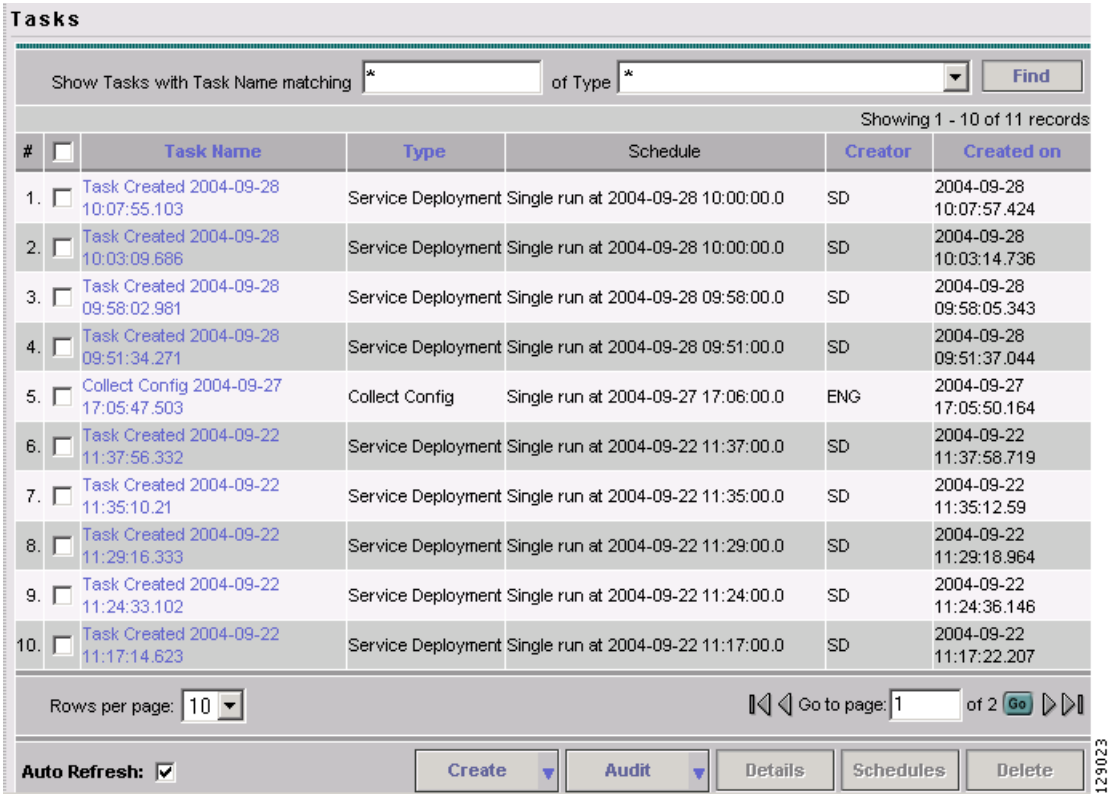
Tasks

Starting Task Manager

To start Task Manager, follow these steps:

Step 1 Click the **Task Manager** icon. The Tasks list page appears, as shown in Figure 7-2, "Tasks."

Figure 7-2 Tasks



#		Task Name	Type	Schedule	Creator	Created on
1.	☐	Task Created 2004-09-28 10:07:55.103	Service Deployment	Single run at 2004-09-28 10:00:00.0	SD	2004-09-28 10:07:57.424
2.	☐	Task Created 2004-09-28 10:03:09.686	Service Deployment	Single run at 2004-09-28 10:00:00.0	SD	2004-09-28 10:03:14.736
3.	☐	Task Created 2004-09-28 09:58:02.981	Service Deployment	Single run at 2004-09-28 09:58:00.0	SD	2004-09-28 09:58:05.343
4.	☐	Task Created 2004-09-28 09:51:34.271	Service Deployment	Single run at 2004-09-28 09:51:00.0	SD	2004-09-28 09:51:37.044
5.	☐	Collect Config 2004-09-27 17:05:47.503	Collect Config	Single run at 2004-09-27 17:06:00.0	ENG	2004-09-27 17:05:50.164
6.	☐	Task Created 2004-09-22 11:37:56.332	Service Deployment	Single run at 2004-09-22 11:37:00.0	SD	2004-09-22 11:37:58.719
7.	☐	Task Created 2004-09-22 11:35:10.21	Service Deployment	Single run at 2004-09-22 11:35:00.0	SD	2004-09-22 11:35:12.59
8.	☐	Task Created 2004-09-22 11:29:16.333	Service Deployment	Single run at 2004-09-22 11:29:00.0	SD	2004-09-22 11:29:18.964
9.	☐	Task Created 2004-09-22 11:24:33.102	Service Deployment	Single run at 2004-09-22 11:24:00.0	SD	2004-09-22 11:24:36.146
10.	☐	Task Created 2004-09-22 11:17:14.623	Service Deployment	Single run at 2004-09-22 11:17:00.0	SD	2004-09-22 11:17:22.207

The Tasks window displays information about each task by **Task Name**, **Type**, **Schedule** date and time, the user name of the **Creator** who created those tasks, and the date **Created on**. To view, schedule, or delete the listed tasks, select the corresponding check box.

New Tasks can also be created or audited using this window.

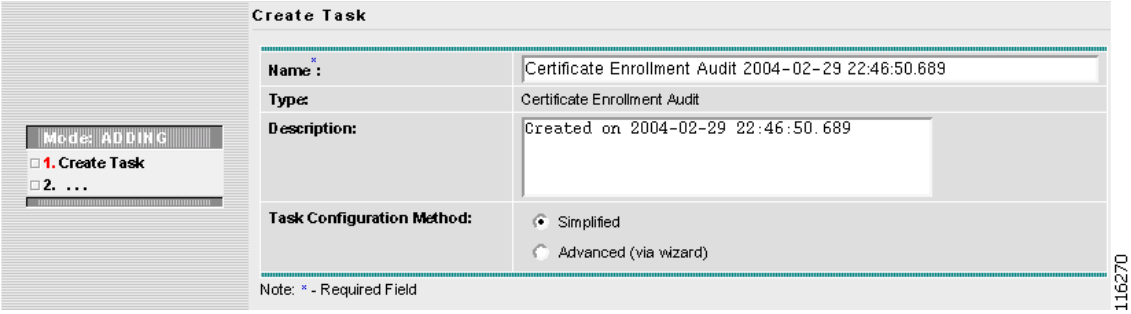
Creating a New Task

To create a new task, follow these steps:

Step 1 From the **Tasks** page, as shown in Figure 7-2, "Tasks," click **Create**. From the resulting drop-down list, you can choose from the following and that choice becomes the **Type** in Figure 7-3, "Create Tasks,":

- **Collect Config** - collects configuration from devices.
- **Password Management** - manages user passwords and SNMP community strings.
- **SLA Collection** - collects data from SLA enabled devices.
- **Service Deployment** - deploys an existing SR.
- **TE Discovery** - populates the repository with tunnel and route data from the Traffic Engineering network.
- **TE Interface Performance** - calculates tunnel/interface bandwidth utilization using SNMP.

Figure 7-3 Create Tasks



Step 2 **Name**: Enter the name of the task. You can accept the default value.

Step 3 **Type**: Defined in Step 1.

Step 4 **Description**: (optional) Enter a description.

Step 5 **Task Configuration Method** (default: **Simplified**) Choose **Simplified** or **Advanced (via wizard)**.

Step 6 Click **Next** to continue. Depending on what type of task you select, the Task Devices or Task Service Requests page appears, as shown in Figure 7-4, "Task Devices" and Figure 7-5, "Task Service Requests," respectively, with variations.

Figure 7-4 Task Devices

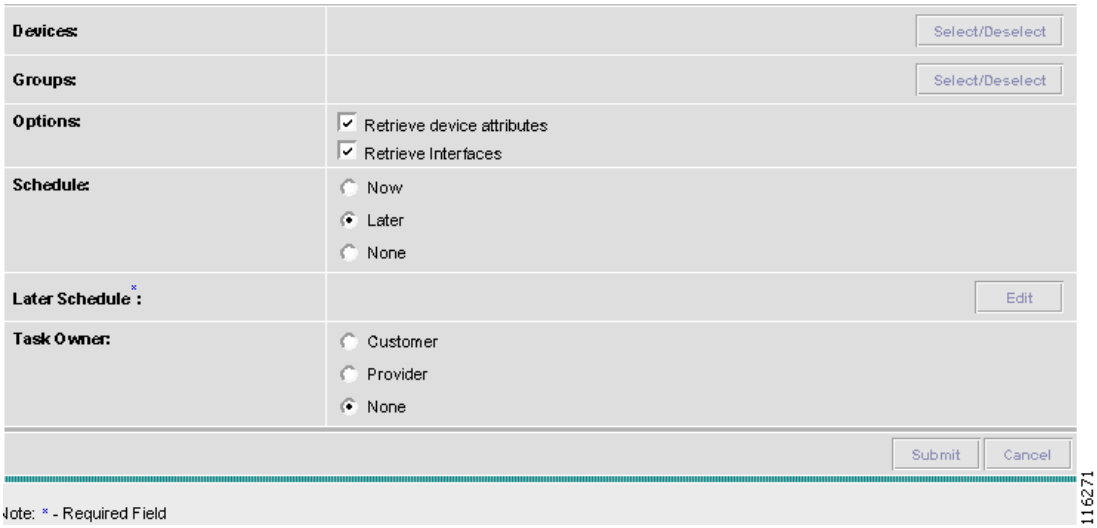
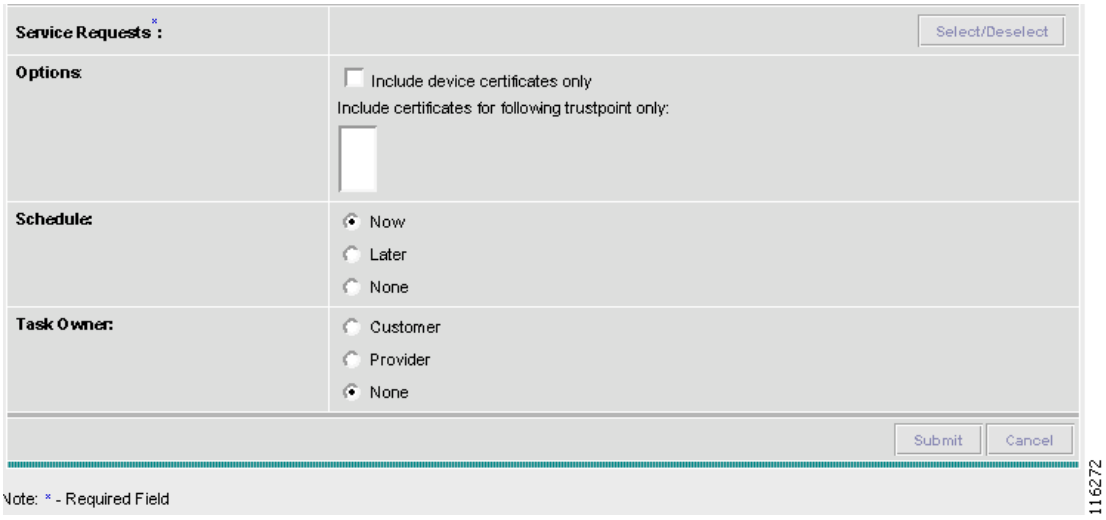


Figure 7-5 Task Service Requests



Step 7 Click **Select/Deselect** to add devices or service requests.

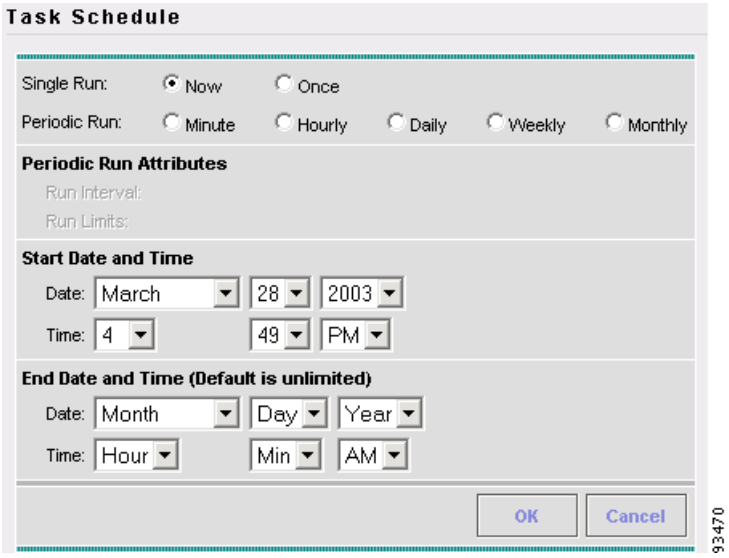
Step 8 In the resulting selection window, select the devices or service requests and click **Select**. The selected devices or service requests appear in Figure 7-4, "Task Devices" or Figure 7-5, "Task Service Requests," respectively.

Step 9 **Groups** might or might not appear depending on the task you specify in the previous step. If it does appear, you can add groups of devices, similarly to Step 7 and Step 8. If it doesn't appear or after you complete this device group selection, proceed to Step 11.

Step 10 Choose the **Options**.

Step 11 For **Schedule**, click **Now**, **Later**, or **None**. If you choose **Later**, a Later Schedule category appears. You are then required to click the **Edit** button and the Task Scheduler page appears, as shown in Figure 7-6, "Task Schedule Details."

Figure 7-6 Task Schedule Details



Step 12 Select information to schedule the task and click **OK** (default is to schedule **Now**).

Step 13 Click **Submit** to continue. The new task is added to the list of tasks.

Audit

To get audit information, follow these steps:

Step 1 From the **Tasks** page, as shown in Figure 7-2, "Tasks," click **Audit**. From the resulting drop-down list, you can choose from the following and that choice becomes the **Type** in Figure 7-3, "Create Tasks,":

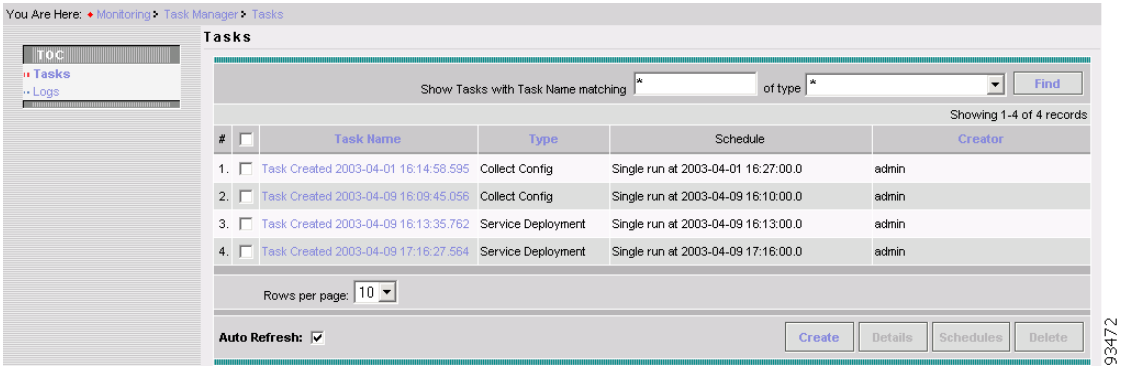
- **Certificate Enrollment Audit** - verifies certificate enrollment.
- **Config Audit** - compares ISC generated configlet against the one in the device.
- **IPsec Functional Audit** - audits IPsec functionality.- **This feature is NOT SUPPORTED in this release.** -
- **L2VPN (L2TPv3) Functional Audit** - audits L2TPv3 functionality.
- **MPLS Functional Audit** - audits MPLS functionality.
- **TE Functional Audit** - checks the Label-Switch Path (LSP) on a router against the LSP stored in the repository.

Task Logs

Task Logs can be used to understand the status of a task, whether or not it completed successfully. You can also use the Task Logs to troubleshoot why a task has failed. To view the Task Logs, follow these steps:

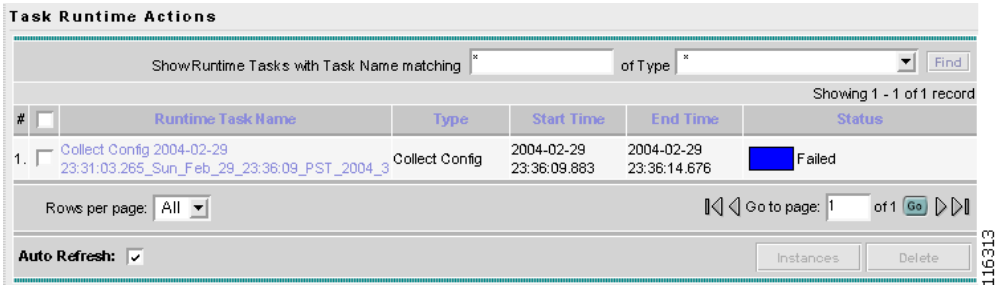
Step 1 Click **Task Manager**. The Tasks page appears, as shown in Figure 7-7, "Tasks."

Figure 7-7 Tasks



Step 2 Click **Logs** under the TOC heading located on the left-hand side. The Task Runtime Actions page appears, as shown in the Figure 7-8, "Task Runtime Actions."

Figure 7-8 Task Runtime Actions



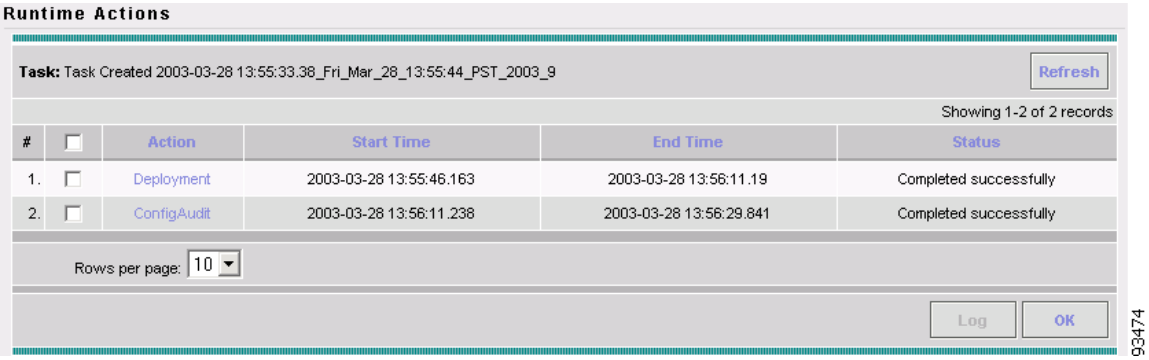
This window displays the task by Runtime Task Name, and the Type, Start Time, End Time and the Status of the task. You can use this window to view or delete the logs.

Step 3 To view the log, select the check box for the row that represents the task.

Step 4 Click **Instances**. The Runtime Actions page appears, as shown in Figure 7-9, "Runtime Actions."

Note If you want to delete a runtime task, click **Delete**.

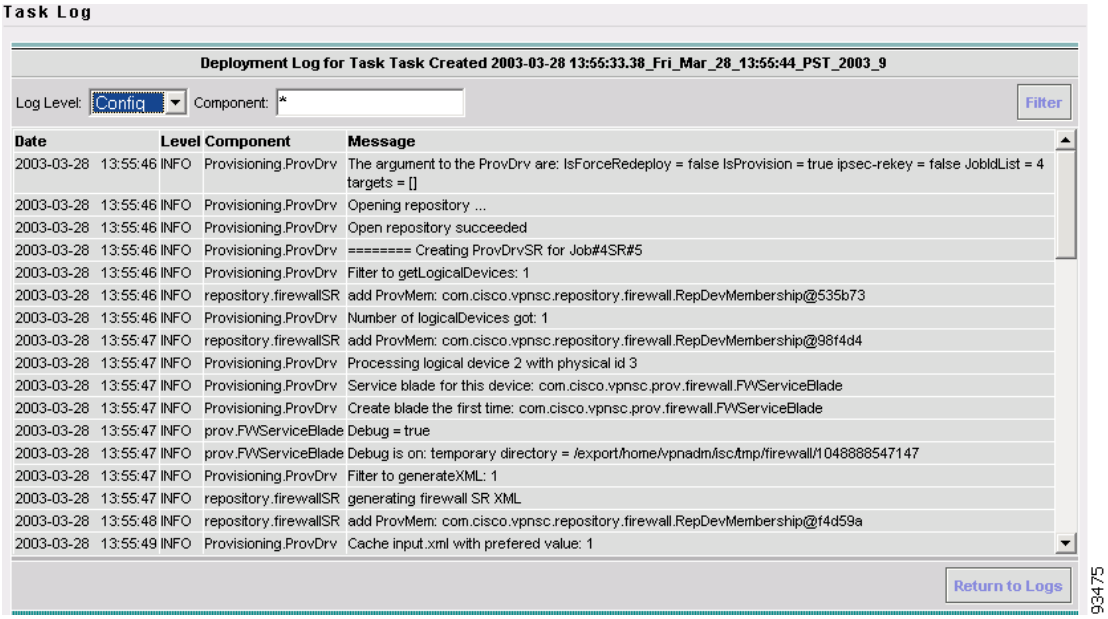
Figure 7-9 Runtime Actions



Step 5 Select the log you want to view in detail and select the check box for that row of information.

Step 6 Click **Log**. The Task Log page appears, as shown in Figure 7-10, "Task Log."

Figure 7-10 Task Log



It is possible to set the types of log level you want to view. Specify the Log Level and click on the Filter button to view that information you want to view.

Step 7 Click **Return to Logs** to specify another log to view.

Ping

Ping is the way ISC monitors the VPN connectivity, that is verify the connectivity among various edge devices comprising the VPN. To achieve this, you can perform a series of pings among these devices. Ping has the following benefits:

- Ping is service independent and therefore can be used for functional auditing of MPLS applications.
- Ping can establish whether a service is working without doing a functional audit for that service.
- Ping can be used to verify IPv4 connectivity among CPEs prior to VPN or Firewall- **This feature is NOT SUPPORTED in this release.** - service deployment.
- Ping fits well with Firewall service in conjunction with a VPN service for ensuring the firewall service did not break the VPN service.- **This feature is NOT SUPPORTED in this release.** -

However, Ping does not do the following:

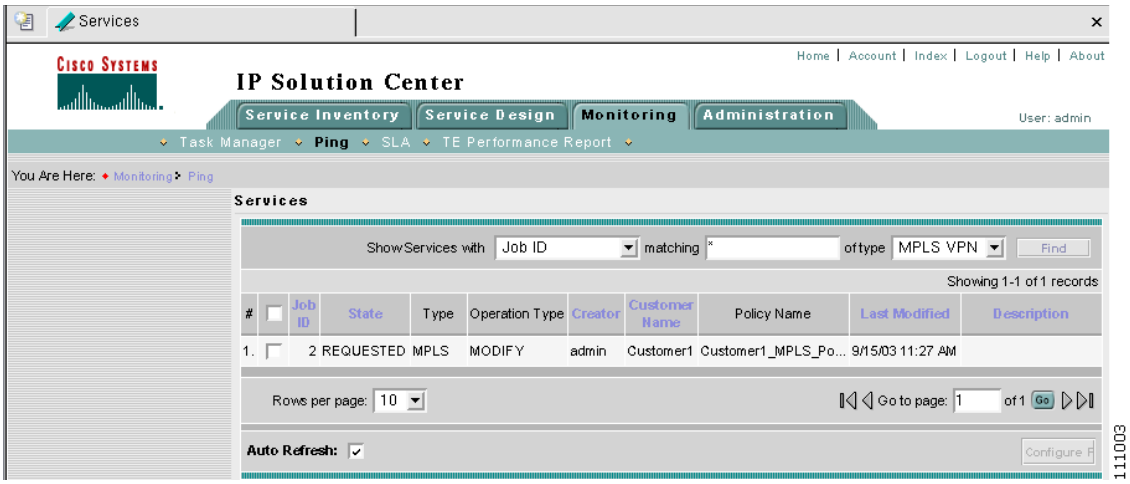
- Ping does not work in environments where ICMP traffic is blocked, for example, in an Cisco IOS router with an access-list denying all ICMP traffic or a PIX firewall which by default does not permit ICMP.
- Ping can only inform you that there is a connectivity problem. It does not offer any service-specific information. The connectivity problem can be due to many reasons, such as device failure, misconfiguration, and so on, which ping cannot distinguish.
- Only the immediate subnet behind the router's customer-facing (also, inside or nonsecured) interface is supported. Campus subnets cannot be supported.

The Ping GUI supports all possible pings for MPLS service requests.

This section explains how to ping MPLS service requests.

After you navigate **Monitoring > Ping**, you receive a window as shown in.Figure 7-11, "Services."

Figure 7-11 Services



From here you can use the **Show Services with** drop-down menu to select:

- **Job ID**
- **Customer Name**
- **VPN Name**

- **State**
- **Description**

Then for **matching**, enter the beginning characters of the names you want to match followed by *.

Then before clicking **Find**, from **of type** select **MPLS** or **IPsec** (**This feature is NOT SUPPORTED in this release**). -and proceed as follows:

- MPLS, page 7-9 explains the flow after choosing the type **MPLS**.
- IPsec, page 7-11 explains the flow after choosing the type **IPsec**.- **This feature is NOT SUPPORTED in this release.** -

Note At the bottom of many windows, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Note At the bottom of many windows you can click the **Auto Refresh** button to automatically refresh after **n** seconds, where **n** is the refresh rate set in DCPL, or you can unclick this button and not automatically refresh.

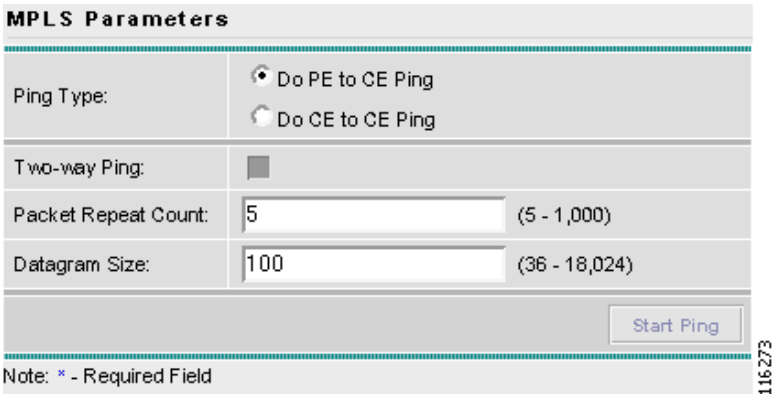
MPLS

After you navigate **Monitoring > Ping** and select **MPLS** as the **type**, follow these steps:

Step 1 Select the check box next to each row for which you want to configure ping parameters or select the check box in the heading row to select all the rows.

Step 2 Click the **Configure Ping Parameters** button which becomes enabled. A window as shown in Figure 7-12, "MPLS Parameters," appears.

Figure 7-12 MPLS Parameters

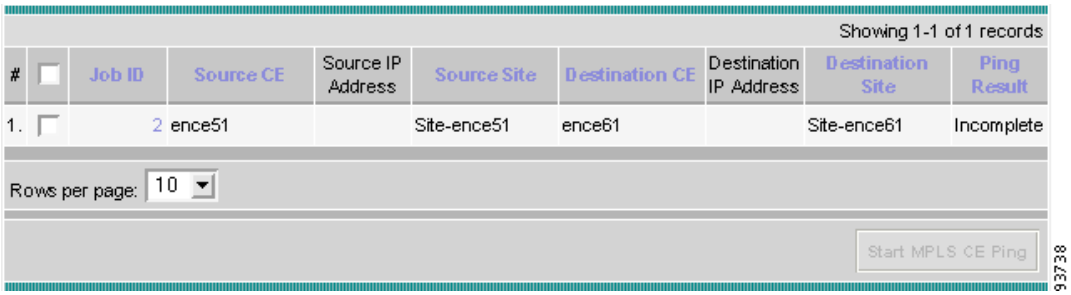


Fill in the following and then click **Start Ping**:

- **Ping Type—Do PE to CE** When this radio button is chosen, a VRF ping occurs for all PE CE pairs that form an MPLS VPN link. The IP addresses taken for this ping are the link end-point addresses. For example, assume that an MPLS service request has two linked PE1<>CE1 and PE2<>CE2. Then this selection initiates four VRF pings: (PE1, CE1), (PE2, CE2), (PE1, CE2), and (PE2, CE1). When this selection is chosen, then after you click **Start MPLS Ping**, you go directly to Step 6 and receive a result page.
- **Ping Type—Do CE to CE ping** When this radio button is chosen, a ping occurs between all CEs that make the end-point in the service request. When this selection is chosen, then after you click **Start MPLS Ping**, proceed to Step 3.
- **Two-way Ping** (default: unavailable and deselected) This check box is only available when you select **Do CE to CE ping**. When a ping occurs from device1 to device2 and this check box is selected, then a ping from device2 to device1 also occurs.
- **Packet Repeat count** (valid values: 5 - 1000) (default: 5) This value indicates how many ICMP packets to use for a ping.
- **Datagram size** (valid values: 36-18024) (default: 100) This value is the packet size of ICMP used for pinging.

Step 3 For **Do CE to CE ping**, you proceed to a window as shown in Figure 7-13, "MPLS CE Selection."

Figure 7-13 MPLS CE Selection



Step 4 Select the check box next to each row for which you want to select a CE or select the check box in the heading row to select all the rows.

Step 5 Click the **Start MPLS CE Ping** button which becomes enabled.

Step 6 You receive a results window as shown in Figure 7-14, "MPLS Ping Test Results.

Figure 7-14 MPLS Ping Test Results

Showing 1-4 of 4 records

#	Property Name	Property Value
1.	Packet repeat count	5
2.	Datagram size	100
3.	Two-way Ping	no
4.	Do PE to CE ping	no

Showing 1-2 of 2 records

#	Job ID	PE	Source IP Address	Source Region	CE	Destination IP Address	Destination Site	Ping Result
1.	12	mlpe2	40.40.40.13	West	mlce3	40.40.40.14	SJ	0/5 success
2.	27	mlpe2	40.40.40.29	West	mlce1	40.40.40.30	SF	0/5 success

Rows per page: 10

Auto Refresh: Redo Ping View Job Logs Refresh Close

93837

Step 7 The buttons at the bottom of the window are as follows:

- **Redo Ping** When you click this button, you restart all the pings. The parameters used are the same as those specified in the last request.
- **View Job Logs** When you click this button, you receive logs of all the ISC jobs created for doing ping. The ping application creates one job per selected service request.
- **Auto Refresh** If this check box is selected, a result refreshes every **n** seconds, where **n** is defined in DCPL as the refresh rate.
- **Refresh** To selectively refresh, turn off the **Auto Refresh** button and click this button whenever you want to update the results.
- **Close** Click this button to close the current ping request. You return to the **Monitoring** page.

Note Any column heading in blue indicates that by clicking that column header, you can sort on that column.

Step 8 Click **Close** and you are finished with this Ping session.

IPsec

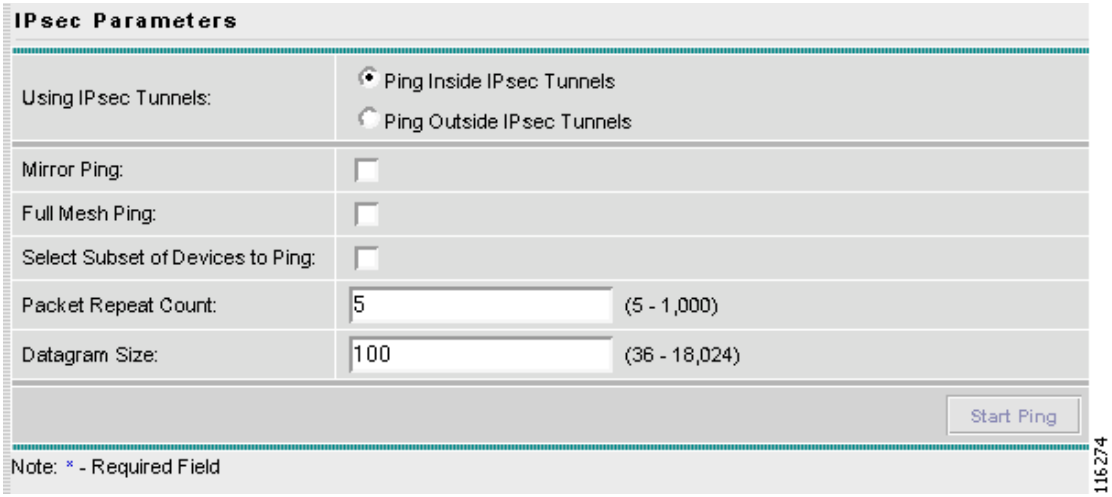
- This feature is NOT SUPPORTED in this release. -

After you navigate **Monitoring > Ping** and select **IPsec** as the **type**, follow these steps:

Step 1 Select the check box next to each row for which you want to configure ping parameters or select the check box in the heading row to select all the rows.

Step 2 Click the **Configure Ping Parameters** button which becomes enabled. A window as shown in Figure 7-15, "IPsec Parameters," appears.

Figure 7-15 IPsec Parameters



Fill in the following and then click **Start Ping**. If you select **Select subset of devices to ping**, you proceed to Step 3. If not, you proceed to Step 6.

- **Using IPsec tunnels** (required) (default: **Ping inside IPsec tunnels**) If you select the **Ping inside IPsec tunnels** radio button, you use nonsecure interfaces for ping. If you select the **Ping outside IPsec tunnels** radio button, you use secure interfaces for the ping.
- **Mirror Ping** (default: deselected) When a ping occurs from device1 to device2 and this check box is selected, then a ping from device2 to device1 also occurs.
- **Full mesh ping** (default: deselected) In a scenario like DMVPN, where spokes of a hub and spoke service request can talk to each other without going through the hub, you might be required to do a full-mesh ping, that is ping as though the service request is full-mesh. In this case, select this check box.
- **Select subset of devices to ping** (default: deselected) When this check box is selected, you receive the ability to select the pings you require rather than pinging all the choices.

Note **Full mesh ping** and **Select subset of devices to ping** can be used in conjunction to verify that the DMVPN is working. For example, for a hub and spoke service request with three spokes, if spoke1 and spoke2 are connected, you are interested in following pings: (hub, spoke1), (hub, spoke2), (hub, spoke3), and (spoke1,spoke2). You can select both check boxes **Full mesh ping** and **Select subset of devices to ping**. Then on the CE selection page you receive all possible ping combinations between a hub and four spokes. You can select the four required pings and view the result.

- **Packet repeat count** (valid values: 5 - 1000) (default: 5) This value indicates how many ICMP packets to use for a ping.
- **Datagram size** (valid values: 36-18024) (default: 100) This value is the packet size of ICMP used for pinging.

Step 3 If you selected **Select subset of devices to ping**, you receive a window as shown in Figure 7-16, "IPsec CE Selection."

Figure 7-16 IPsec CE Selection

Showing 1-2 of 2 records

#		Job ID	Source CE	Source IP Address	Source Site	Destination CE	Destination IP Address	Destination Site	Ping Result
1.		4	carson	10.128.0.254	SJ	barnes.cisco.com	10.128.16.1	Boulder	Incomplete
2.		4	barnes	10.128.16.1	Boulder	carson.cisco.com	10.128.0.254	SJ	Incomplete

Rows per page: 10

Start IPSec CE Ping

93740

Step 4 Select the check box next to each row for which you want to select a CE or select the check box in the heading row to select all the rows.

Step 5 Click the **Start IPsec CE Ping** button which becomes enabled.

Step 6 You receive a results window as shown in Figure 7-17, "IPsec Ping Test Results.

Figure 7-17 IPsec Ping Test Results

Showing 1-5 of 5 records

#	Property Name	Property Value
1.	Two-way Ping	yes
2.	Ping inside IPsec tunnels	yes
3.	Packet repeat count	5
4.	Datagram size	100
5.	Full mesh ping	yes

Showing 1-2 of 2 records

#	Job ID	Source Device	Source IP Address	Source Location	Destination Device	Destination IP Address	Destination Location	Ping Result
1.	2	ipsec-cpe-geneva	10.10.130.2	Customer1::Site1	ipsec-cpe-milan	10.10.110.2	Customer1::Site2	0/5 success
2.	2	ipsec-cpe-milan	10.10.110.2	Customer1::Site2	ipsec-cpe-geneva	10.10.130.2	Customer1::Site1	0/5 success

Rows per page: 10

Auto Refresh: Redo Ping View Job Logs Refresh Close

93741

Step 7 The buttons at the bottom of the window are as follows:

- **Redo Ping** When you click this button, you restart all the pings. The parameters used are the same as those specified in the last request.
- **View Job Logs** When you click this button, you receive logs of all the ISC jobs created for doing ping. The ping application creates one job per selected service request.
- **Auto Refresh** If this check box is selected, a result refreshes every **n** seconds, where **n** is defined in DCPL as the refresh rate.
- **Refresh** To selectively refresh, turn off the **Auto Refresh** button and click this button whenever you want to update the results.
- **Close** Click this button to close the current ping request. You return to the **Monitoring** page.

Note Any column heading in blue indicates that by clicking that column header, you can sort on that column.

Step 8 Click **Close** and you are finished with this Ping session.

SLA

A service-level agreement (SLA) defines a level of service provided by a service provider to any customer. Performance is monitored through the SLA server. ISC monitors the service-related performance criteria by provisioning, collecting, and monitoring SLAs on Cisco IOS routers that support the Service Assurance Agent (SA Agent) devices. To provision the SLAs and to collect statistics for each SLA, the data collection task requires minimal user input.

The SLA collection task collects the relevant performance data, stores it persistently, aggregates it, and presents useful reports. The SLA collection task collects from the SA Agent MIB on devices. ISC leverages the SA Agent MIB to monitor SLA performance on a 24 x 7 basis. Using the MIB, you can monitor network traffic for the popular protocols: Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), File Transfer Protocol (FTP), Hyper text Transfer Protocol (HTTP), Internet Control Message Protocol Echo (ICMP Echo), Jitter (voice jitter), Transmission Control Protocol Connect (TCP Connect), and User Datagram Protocol Echo (UDP Echo).

Note SLA uses the embedded Sybase database, independent of whether you choose Oracle as your database.

Note The SLA operations **Create**, **Delete**, **Enable Probes**, **Disable Probes**, **Enable Traps**, and **Disable Traps** automatically result in the creation of a task, which executes the actual operation. You can view the status of the task by navigating **Monitoring > Task Manager > Logs**.

This section explains how to configure SLA probes, collect SLA data, and view SLA reports about these SLA probes.

Before you navigate **Monitoring > SLA**, implement the setup procedures in the "Setup Prior to Using SLA" section on page 7-14."

Then navigate **Monitoring > SLA** and you can select one of the following:

- Probes, page 7-15 is the default selection.
- Reports, page 7-54

Setup Prior to Using SLA

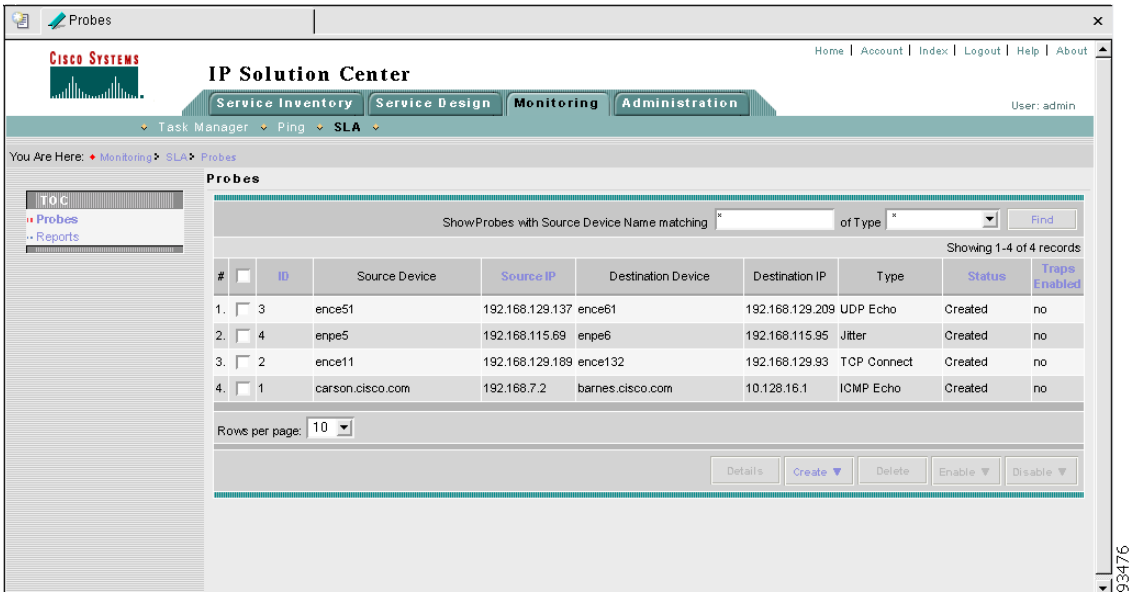
SLA is an SNMP activity. Be sure SNMP is enabled and the SNMP settings on the router match the settings in the repository.

When creating an SLA **From MPLS CPE**, **From MPLS PE**, or **From IPsec CPE (This feature is NOT SUPPORTED in this release.)**, the service requests associated with the devices *must* be in the Deployed state.

Probes

When you navigate **Monitoring > SLA > Probes**, you receive a window as shown in Figure 7-18, "SLA Probes."

Figure 7-18 SLA Probes



The default button that is enabled is **Create** and from the **Create** drop-down menu, you can choose to create SLA probes **From Any SA Agent Device(s)**; **From MPLS CPE**; **From MPLS PE**; or **From IPsec CPE (This feature is NOT SUPPORTED in this release.)**. However, if you select one or more existing probes by clicking the row(s) of existing probe(s), to select the specific probe(s), or you click the box in the header row, to select all the probes, then you have access to the other buttons, **Details**, **Delete**, **Enable**, and **Disable**. For **Enable** and **Disable**, the drop-down menu contains options to enable or disable SLA **Probes** and SLA **Traps**.

At the top of this window, for **Show Probes with Source Device Name matching** you can enter the beginning characters of the names you want to match followed by *; then for **of Type**, you can keep the default of *, which searches for all the protocol types, or you can select the drop-down menu to select a specific protocol type; and then click **Find**.

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

The explanations of the buttons and subsequent drop-down menus is given as follows:

- Create From Any SA Agent Device(s), page 7-16 This section explains how to create probes from any SA Agent device(s).
- Create from MPLS CPE, page 7-22 This section explains how to create probes from an MPLS CPE.
- Create From MPLS PE or MVRF-CE, page 7-29 This section explains how to create probes from an MPLS PE.
- Create from IPsec CPE, page 7-36 - **This feature is NOT SUPPORTED in this release.** -
- Protocols, page 7-41 This section is common Probes information for each of the **Create** paths.
- Details, page 7-46 This section gives details about a specified probe or all the probes.

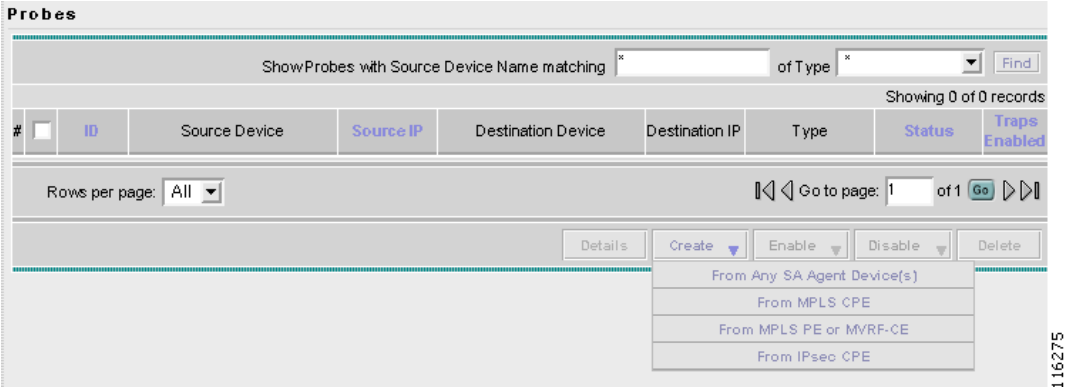
- Delete, page 7-47 This section explains how to delete a probe.
- Enable Probes, page 7-49 This section explains how to enable the Status and move it from Created to Active.
- Enable Traps, page 7-50 This section explains how to enable traps.
- Disable Probes, page 7-51 This section explains how to disable the Status and move it from Active to Created.
- Disable Traps, page 7-53 This sections explains how to disable traps.

Create From Any SA Agent Device(s)

When you navigate **Monitoring > SLA > Probes**, the default is the **Probes** page with only the **Create** button enabled. From the **Create** drop-down menu, you can select **From Any SA Agent Device(s)**, as shown in Figure 7-19, "SLA Probes > Create > From Any SA Agent Device(s)."

Note IP connectivity must be available between the SA Agent devices.

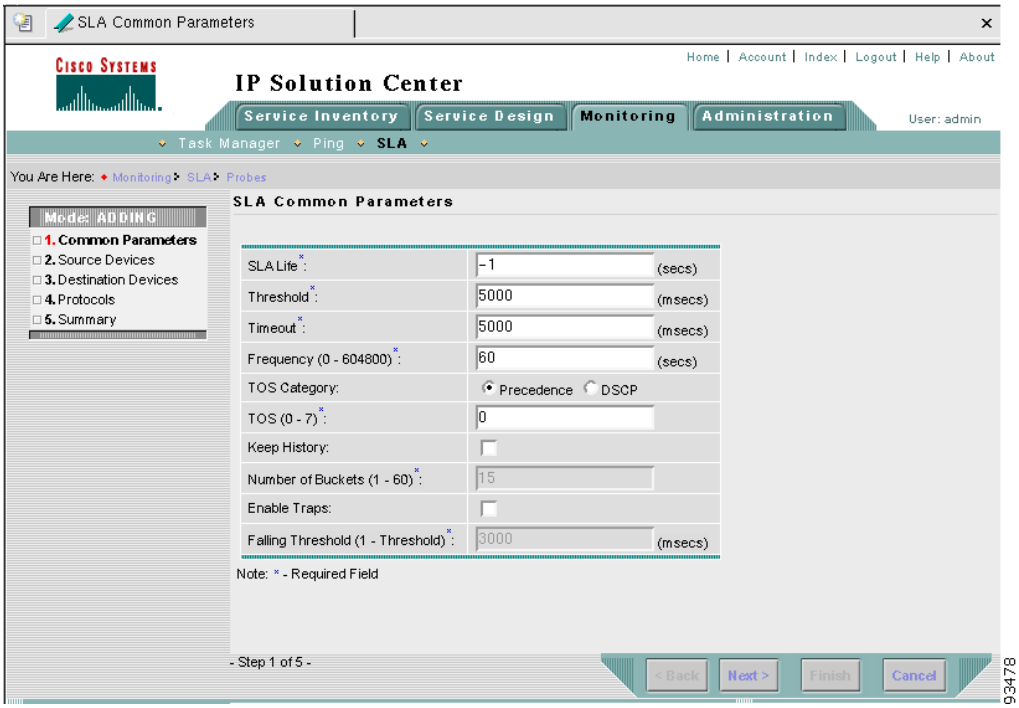
Figure 7-19 SLA Probes > Create > From Any SA Agent Device(s)



You then proceed through the following steps:

Step 1 The first window to appear is as shown in Figure 7-20, "SLA Common Parameters."

Figure 7-20 SLA Common Parameters



Accept the defaults or change the information in the fields of the common SLA parameters, as follows, and then click **Next**:

- **SLA Life** (required) is the number of seconds that the probe is active (with the maximum value of a 32-bit integer in seconds). If the value is set to **-1**, the typical and default value, the probe is active forever.
- **Threshold** (required) is an integer that defines the threshold limit in milliseconds. When this threshold is exceeded and traps are enabled, a trap is sent. 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 value for **Threshold** must not exceed the value for **Timeout**. The default value is **5000**.
- **Timeout** (required) is the duration in milliseconds to wait for an SA Agent operation completion. The value for **Timeout** must be less than or equal to the value for **Frequency** and greater than or equal to the value for **Threshold**. The default value is **5000**
- **Frequency (0 - 604800)** (required) is the duration in seconds between initiating each SA Agent operation. The value for **Frequency** must be greater than or equal to the value for **Timeout**. The default value is **60**.
- **TOS Category** (default: **Precedence**) If you select the **Precedence** radio button for **TOS Category**, you have one set of type of service (TOS) values. If you select the **DSCP** radio button for **TOS Category**, you have a different set of TOS values.
- **TOS** (required) is an integer. The range and meanings of the values depend on whether the radio button in the **TOS Category** is set to **Precedence** (values: 0 to 7) or **DSCP** (values: 0 to 63).
  - When the **TOS Category** is set to **Precedence**, the valid values are **0** to **7**. These values represent the three most significant bits of the ToS field in an IP header. The default value is **0**. The meanings of the **Precedence** values are specified in Table 7-1, "Meanings of Precedence Values."

Note Type of Service does not apply to the **DNS** and **DHCP** types of SLA probes. ISC ignores any ToS value set for these two types of SLA probes. For example, if you first select a ToS value of 5, then select the **DNS**, **DHCP,** and **ICMP Echo** protocols for an SLA probe, ISC applies the selected ToS value to the **ICMP Echo** probe only.

Table 7-1 Meanings of Precedence Values

ToS Value	Binary Value	Meaning
7	111	Network Control
6	110	Internetwork Control
5	101	CRITIC/ECP
4	100	Flash Override
3	011	Flash
2	010	Immediate
1	001	Priority
0	000	Routine

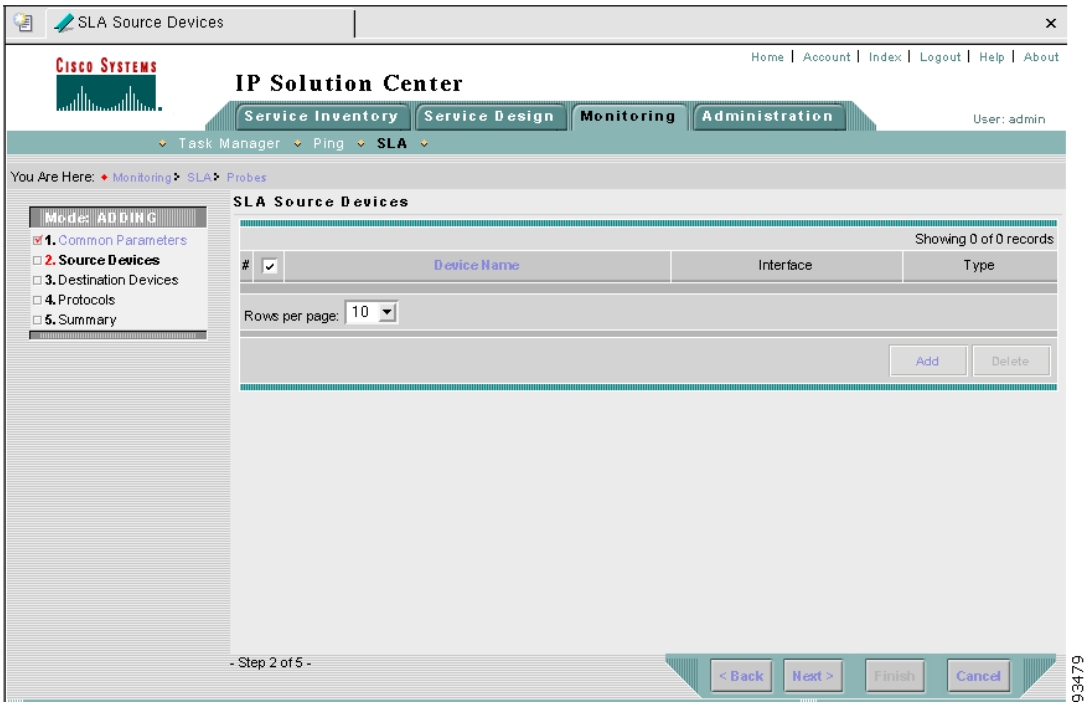
– When the **TOS Category** is set to **DSCP**, the valid values are **0** to **63**. These values represent the six most significant bits of this ToS field in an IP header. The default value is **0**. The interpretation of these **TOS** values is user specified.

Note ISC maps the 0 - 7 PRECEDENCE values to the three most significant ToS bits by left-shifting the value by five positions. Similarly, the 0 - 63 DSCP values are left-shifted by two positions.

- **Keep History** (default: deselected) If you select the **Keep History** check box, you indicate to keep the recent History Table on the router. Specifically, it is kept in the SA Agent MIB that keeps the raw round-trip time (RTT) SLA measurement. This selection also enables you to indicate the **Number of Buckets** of raw history data to keep. If you leave the default of a deselected check box for **Keep History**, no raw history data is kept. **Keep History** is not supported for **HTTP** and **Jitter**.
- **Number of Buckets (1 - 60)** (required) The default is **15** when the **Keep History** box is selected. The range is 1 to 60 and indicates the number of most recent raw data entries to be kept in the raw history data. When the specified **Number of Buckets** is surpassed, removal of buckets starts with the oldest bucket to keep only the number of raw data entries specified.
- **Enable Traps** (default: deselected, which means No) If you select the **Enable Traps** box, the created SLA is configured to send three types of traps. This selection also enables you to indicate the **Falling Threshold**. If you leave the **Enable Traps** box deselected, the traps are disabled on the SLAs created in this task.
- **Falling Threshold (1 - Threshold)** (required) The default is **3000** in milliseconds when the **Enable Traps** box is selected. The range is **1** to the **Threshold** value in milliseconds. When traps are enabled and the delay meets the specified number of milliseconds, a trap is sent.

Step 2 The next window to appear is as shown in Figure 7-21, "SLA Source Devices."

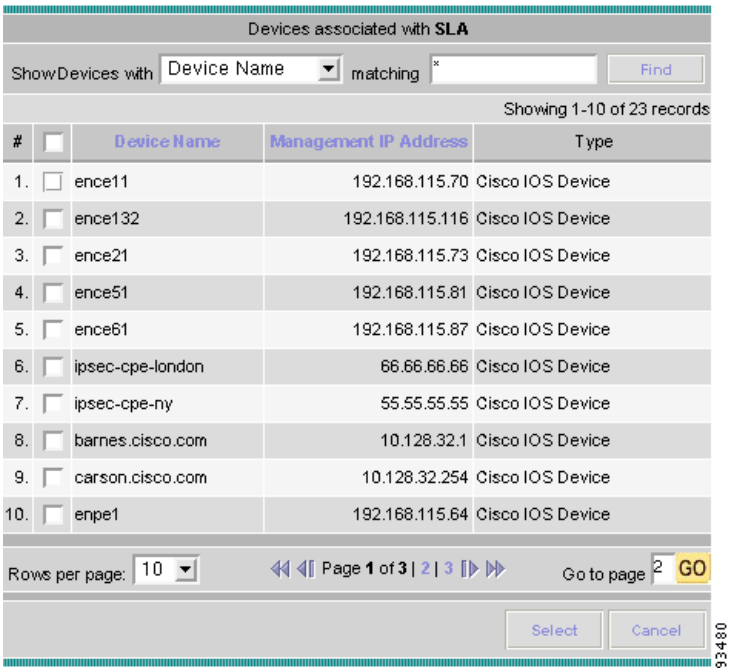
Figure 7-21 SLA Source Devices



Step 3 Click the **Add** button and a window appears as shown in Figure 7-22, "SLA Devices > Add," which lists all the devices in the database that have a minimum of one interface. At the top of this window you can select the drop-down menu for **Show Devices with** and select **Device Name**, **Device Group**, or **Collection Zone**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to each row for the device you want to select or click the box in the heading row to select all the devices. Then click **Select**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**. At the bottom of the page, you can also click on other pages to view and make all your choices.

Figure 7-22 SLA Devices > Add



Step 4 You return to Figure 7-21 and the newly added source device(s) appear. The information about this source device is specified in the following columns:

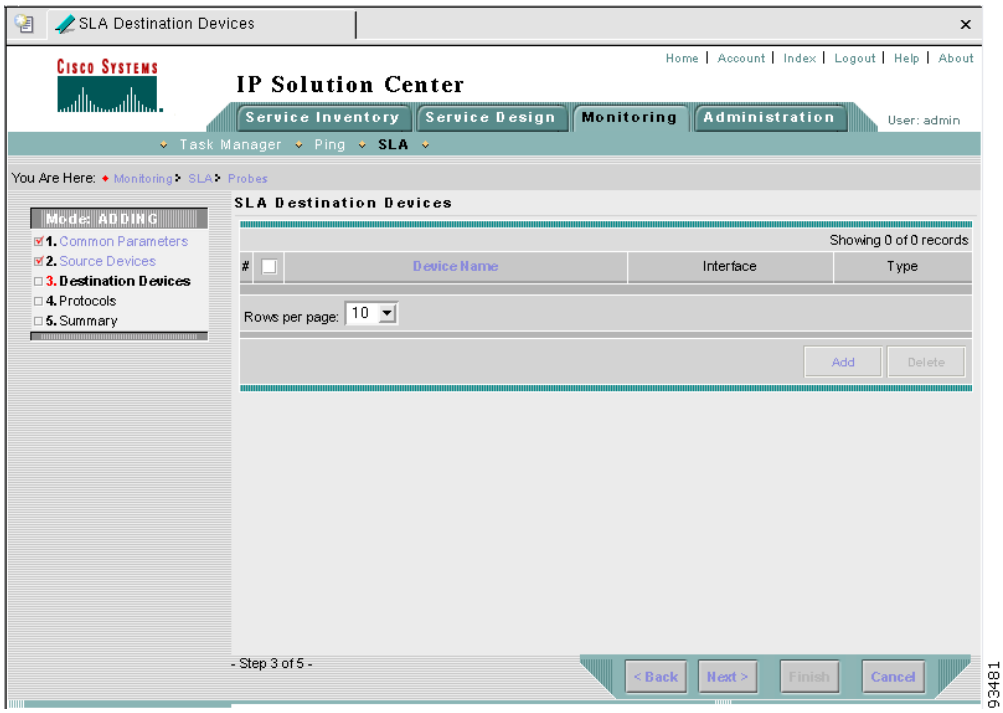
- **Device Name** You can click this heading and the device names are organized alphabetically.
- **Interface** You can click **Select** and from the resulting window, you can update the IP address. At the top of the window, you can click the drop-down menu for **Show Device Interfaces with** and select either **Interface Name** or **IP Address** and for **matching** you can enter the beginning characters of the names you want to match followed by *; and then click **Find**. At the bottom of the window, you can click the drop-down menu for **Rows per page** and select **5**, **10**, **20**, **30**, **40**, or **All**. You can select one radio button for an interface and click **Select** and the IP address changes in Figure 7-21.
- **Type** Gives you the type of the source device.

Step 5 You can repeat Step 3 to **Add** more devices, or you can **Delete** any of the currently selected source devices. To **Delete**, click the box next to each row for the device you want to delete or click the box in the heading row to select all the devices; then click **Delete**.

Note There is no second chance for deleting source devices. There is no confirm window.

Step 6 Click **Next**. The next window to appear is as shown in Figure 7-23, "SLA Destination Devices."

Figure 7-23 SLA Destination Devices



Step 7 Click the **Add** button and a window appears as shown in Figure 7-22, "SLA Devices > Add." At the top of this window you can select the drop-down menu for **Show Devices with** and select **Device Name**, **Device Group**, or **Collection Zone**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to each row for the device you want to select or click the box in the heading row to select all the devices. Then click **Select**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**. At the bottom of the page, you can also click on other pages to view and make all your choices.

Step 8 You return to Figure 7-23 and the newly added destination device(s) appear. The information about this destination device is specified in the following columns:

- **Device Name** You can click this heading and the device names are organized alphabetically.
- **Interface** You can click **Select** and from the resulting window, you can update the IP address. At the top of the window you can click the drop-down menu for **Show Device Interfaces with** and select either **Interface Name** or **IP Address** and for **matching** you can enter the beginning characters of the names you want to match followed by *; and then click **Find**. At the bottom of the window, you can click the drop-down menu for **Rows per page** and select **5**, **10**, **20**, **30**, **40**, or **All**. You can **Select** one radio button for an interface and click **Select** and the IP address changes in Figure 7-23.
- **Type** Gives you the type of the source device.

Step 9 You can repeat Step 7 to **Add** more devices, or you can **Delete** any of the currently selected source devices. To **Delete**, click the box next to each row for the device you want to delete or click the box in the heading row to select all the devices; then click **Delete**.

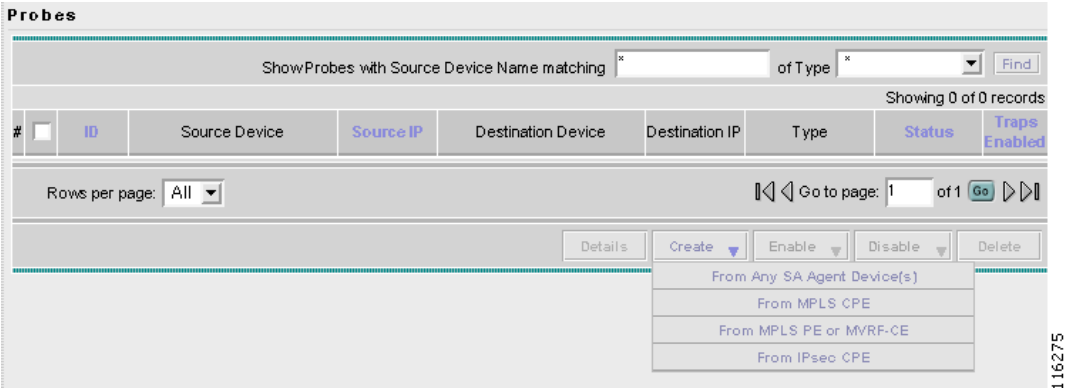
Note There is no second chance for deleting destination devices. There is no confirm window.

Step 10 Click **Next**. Proceed to the "Protocols" section on page 7-41."

Create from MPLS CPE

When you navigate **Monitoring > SLA > Probes** and select no probe, you have access to the **Create** button. From the **Create** drop-down menu, you can select **From MPLS CPE**, as shown in Figure 7-24, "SLA Probes > Create > From MPLS CPE."

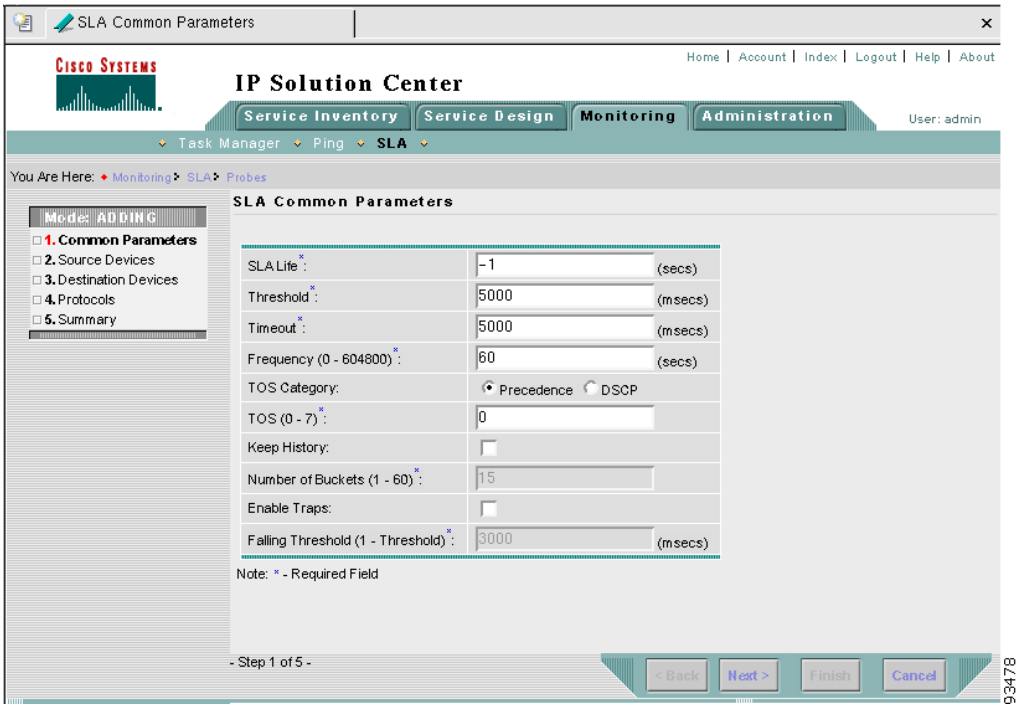
Figure 7-24 SLA Probes > Create > From MPLS CPE



You then proceed through the following steps:

Step 1 The first window to appear is as shown in Figure 7-25, "SLA Common Parameters."

Figure 7-25 SLA Common Parameters



Accept the defaults or change the information in the fields of the common SLA parameters, as follows, and then click **Next**:

- **SLA Life** (required) is the number of seconds that the probe is active (with the maximum value of a 32-bit integer in seconds). If the value is set to **-1**, the typical and default value, the probe is active forever.
- **Threshold** (required) is an integer that defines the threshold limit in milliseconds. When this threshold is exceeded and traps are enabled, a trap is sent. 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 value for **Threshold** must not exceed the value for **Timeout**. The default value is **5000**.
- **Timeout** (required) is the duration in milliseconds to wait for an SA Agent operation completion. The value for **Timeout** must be less than or equal to the value for **Frequency** and greater than or equal to the value for **Threshold**. The default value is **5000**
- **Frequency (0 - 604800)** (required) is the duration in seconds between initiating each SA Agent operation. The value for **Frequency** must be greater than or equal to the value for **Timeout**. The default value is **60**.
- **TOS Category** (default: **Precedence**) If you select the **Precedence** radio button for **TOS Category**, you have one set of type of service (TOS) values. If you select the **DSCP** radio button for **TOS Category**, you have a different set of TOS values.
- **TOS** (required) is an integer. The range and meanings of the values depend on whether the radio button in the **TOS Category** is set to **Precedence** (values: 0 to 7) or **DSCP** (values: 0 to 63).
  - When the **TOS Category** is set to **Precedence**, the valid values are **0** to **7**. These values represent the three most significant bits of the ToS field in an IP header. The default value is **0**. The meanings of the **Precedence** values are specified in Table 7-2, "Meanings of Precedence Values."

Note Type of Service does not apply to the **DNS** and **DHCP** types of SLA probes. ISC ignores any ToS value set for these two types of SLA probes. For example, if you first select a ToS value of 5, then select the **DNS**, **DHCP,** and **ICMP Echo** protocols for an SLA probe, ISC applies the selected ToS value to the **ICMP Echo** probe only.

Table 7-2 Meanings of Precedence Values

ToS Value	Binary Value	Meaning
7	111	Network Control
6	110	Internetwork Control
5	101	CRITIC/ECP
4	100	Flash Override
3	011	Flash
2	010	Immediate
1	001	Priority
0	000	Routine

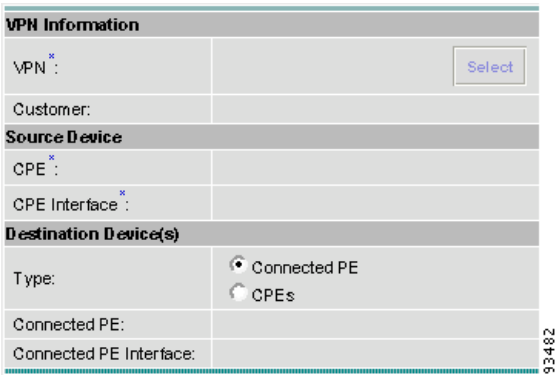
– When the **TOS Category** is set to **DSCP**, the valid values are **0** to **63**. These values represent the six most significant bits of this ToS field in an IP header. The default value is **0**. The interpretation of these **TOS** values is user specified.

Note ISC maps the 0 - 7 PRECEDENCE values to the three most significant ToS bits by left-shifting the value by five positions. Similarly, the 0 - 63 DSCP values are left-shifted by two positions.

- **Keep History** (default: deselected) If you select the **Keep History** box, you indicate to keep the recent History Table on the router. Specifically, it is kept in the SA Agent MIB that keeps the raw round-trip time (RTT) SLA measurement. This selection also enables you to indicate the **Number of Buckets** of raw history data to keep. If you leave the default of a deselected check box for **Keep History**, no raw history data is kept. **Keep History** is not supported for **HTTP** and **Jitter**.
- **Number of Buckets (1 - 60)** (required) The default is **15** when the **Keep History** check box is selected. The range is 1 to 60 and indicates the number of most recent raw data entries to be kept in the raw history data. When the specified **Number of Buckets** is surpassed, removal of buckets starts with the oldest bucket to keep only the number of raw data entries specified.
- **Enable Traps** (default: deselected, which means No) If you select the **Enable Traps** check box, the created SLA is configured to send three types of traps. This selection also enables you to indicate the **Falling Threshold**. If you leave the **Enable Traps** check box deselected, the traps are disabled on the SLAs created in this task.
- **Falling Threshold (1 - Threshold)** (required) The default is **3000** in milliseconds when the **Enable Traps** box is selected. The range is **1** to the **Threshold** value in milliseconds. When traps are enabled and the delay meets the specified number of milliseconds, a trap is sent.

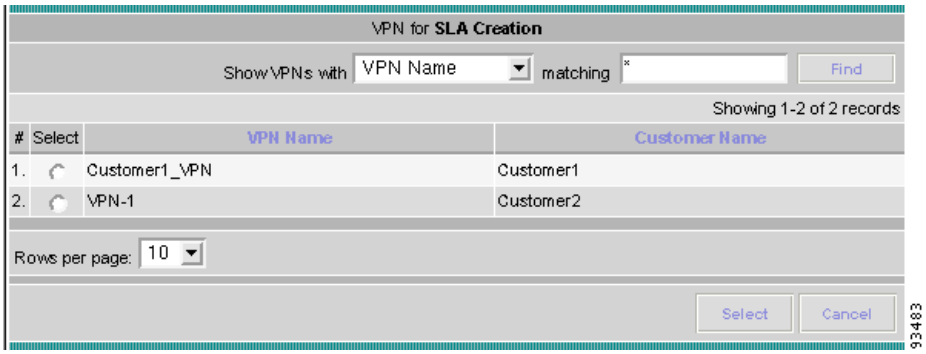
Step 2 The next window to appear is as shown in Figure 7-26, "SLA CPE Parameters."

Figure 7-26 SLA CPE Parameters



Step 3 Click the **Select** button for **VPN** and a window appears as shown in Figure 7-27, "Select VPN," which lists all the VPNs in the database.

Figure 7-27 Select VPN



At the top of this window you can select the drop-down menu for **Show VPNs with** and select **VPN Name** or **Customer Name**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to each row for the VPN you want to select. Then click **Select**.

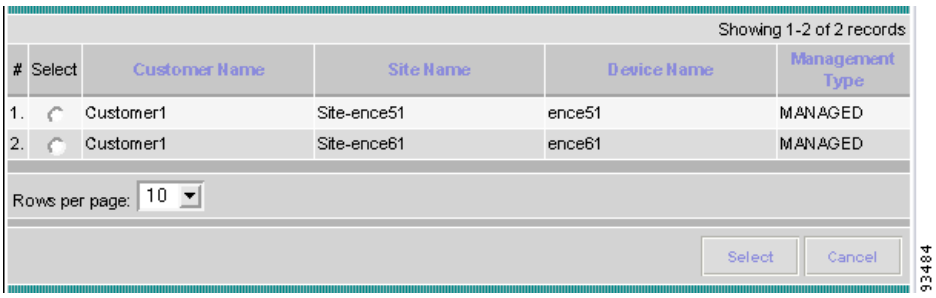
Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Step 4 You return to Figure 7-26 and the newly added VPN and Customer information appear and a **Select** button appears for **CPE**. You can change the VPN by repeating Step 3.

Step 5 Click the **Select** button for **CPE** and a window appears as shown in Figure 7-28, "Select CPE," which lists the CPEs associated with the selected VPN. Click the box next to the row for the CPE you want to select. Then click **Select**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

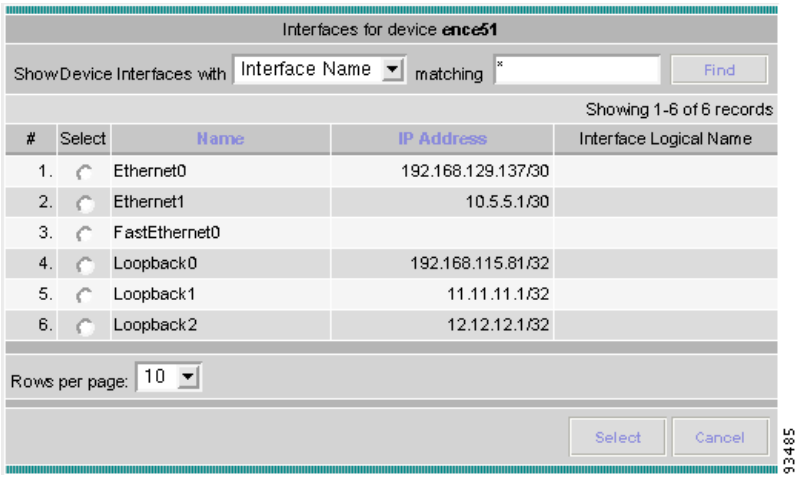
Figure 7-28 Select CPE



Step 6 You return to Figure 7-26 and the newly added **CPE** and its first interface appears. You can change the CPE by repeating Step 5.

Step 7 If you want to change the default **CPE Interface** information that appears, click **Select** and you receive a window as shown in Figure 7-29, "Interfaces."

Figure 7-29 Interfaces



At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *****; and then click **Find**. Click the box next to the row for the VPN you want to select. Then click **Select**.

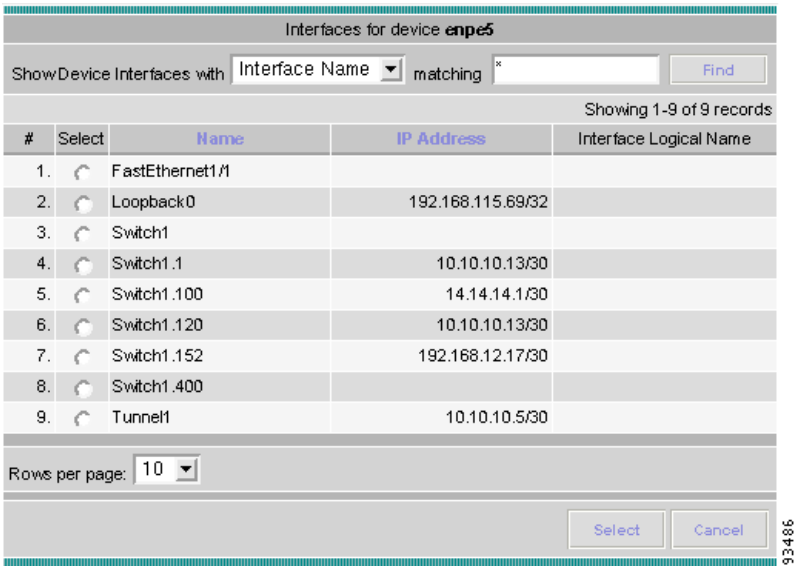
Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Step 8 You return to Figure 7-26 and the newly added **CPE Interface** appears. You can change the CPE Interface by repeating Step 7.

Step 9 You can keep the default **Type**, by leaving the radio button for **Connected PE** chosen, which creates an SLA between the CPE and its directly connected PE, or you can select the radio button for **CPEs** in the same VPN. If you keep the default of **Connected PE**, proceed to Step 10. If you click the **CPEs** radio button, proceed to Step 13.

Step 10 Click **Select** for **Connected PE Interface** and a window appears as shown in Figure 7-30, "Connected PE Interface."

Figure 7-30 Connected PE Interface



At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *****; and then click **Find**. Click the box next to the row for the Name you want to select. Then click **Select**.

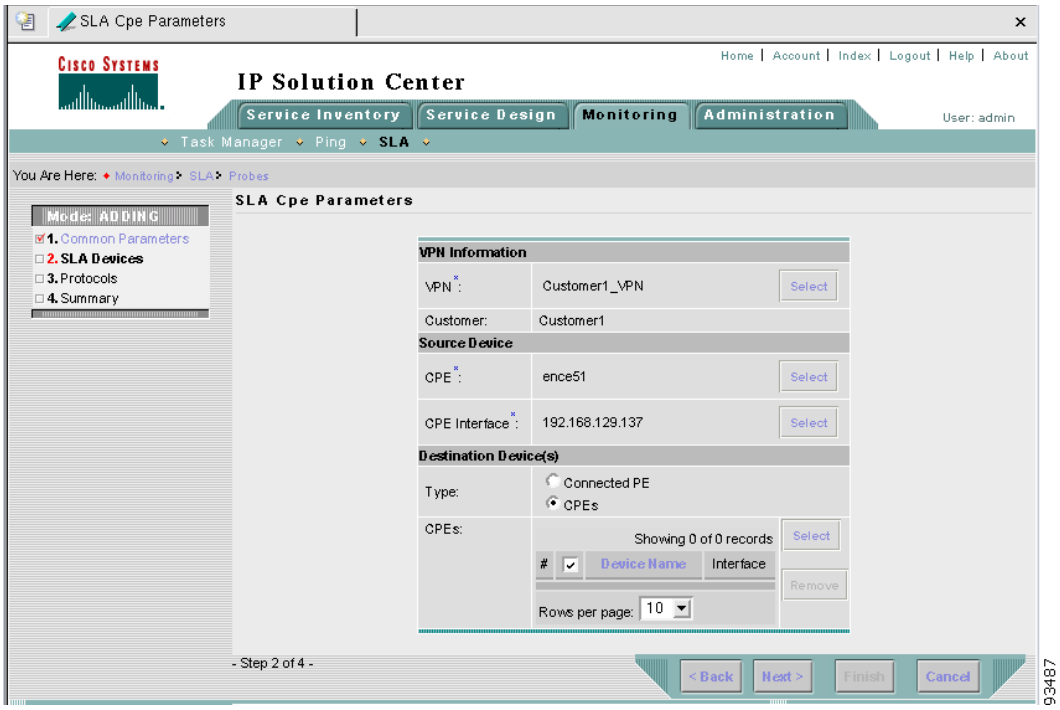
Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Step 11 You return to Figure 7-26 and the newly added **Connected PE Interface** appears. You can change the Connected PE Interface by repeating Step 10.

Step 12 Click **Next** and proceed to the "Protocols" section on page 7-41.

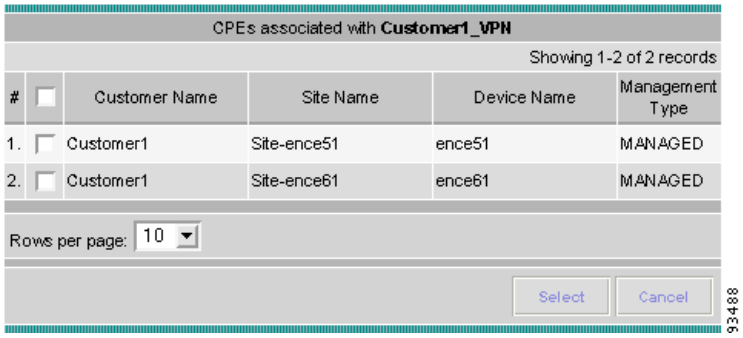
Step 13 When you click **CPEs**, the window is as shown in Figure 7-31, "CPEs."

Figure 7-31 CPEs



Step 14 Click the **Select** button for **CPEs** and a window appears as shown in Figure 7-32, "Select CPE Associated with the Specified VPN," which lists all the CPEs associated with the specified VPN in the database.

Figure 7-32 Select CPE Associated with the Specified VPN



Select the check box next to the row(s) for the CPE(s) you want to select or the check box in the header row to select all the listed CPEs. Then click **Select**.

Note Do *not* add a device chosen as a **Source Device** to **Destination Device(s)**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Step 15 You return to Figure 7-31 and the newly added **Device Name** appears.

Step 16 Click **Select** in the **Interface** column and a window appears as in Figure 7-29.

At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the CPE you want to select. Then click **Select**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Step 17 You return to Figure 7-31 and the newly added **CPE Interface** appears. You can change the CPE Interface by repeating Step 16.

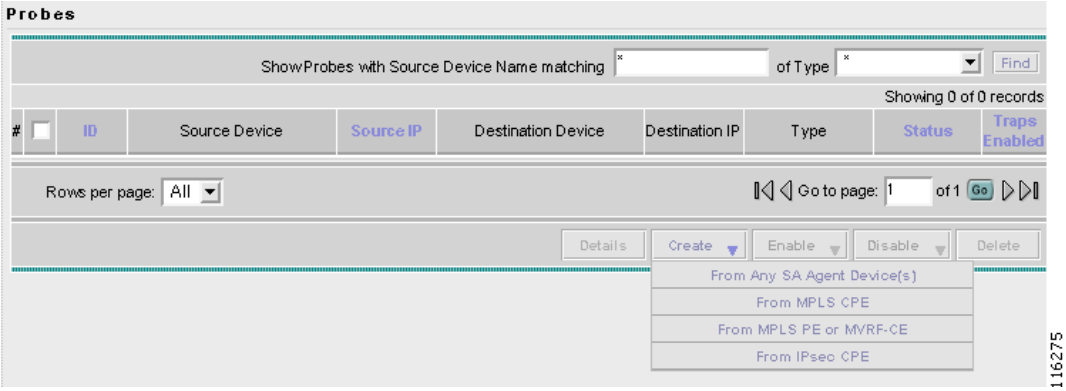
Step 18 Select the check box next to each row for the Devices you want to remove or select the check box in the heading row to remove all the Devices. Then click the **Remove** button and a window as shown in Figure 7-31 appears without the removed Device(s).

Step 19 When Figure 7-31 reflects what you want, click **Next** and proceed to the "Protocols" section on page 7-41.

Create From MPLS PE or MVRF-CE

When you navigate **Monitoring > SLA > Probes** and select no probe, you have access to the **Create** button. From the **Create** drop-down menu, you can select **From MPLS PE or MVRF-CE**, as shown in Figure 7-33, "SLA Probes > Create > From MPLS PE or MVRF-CE."

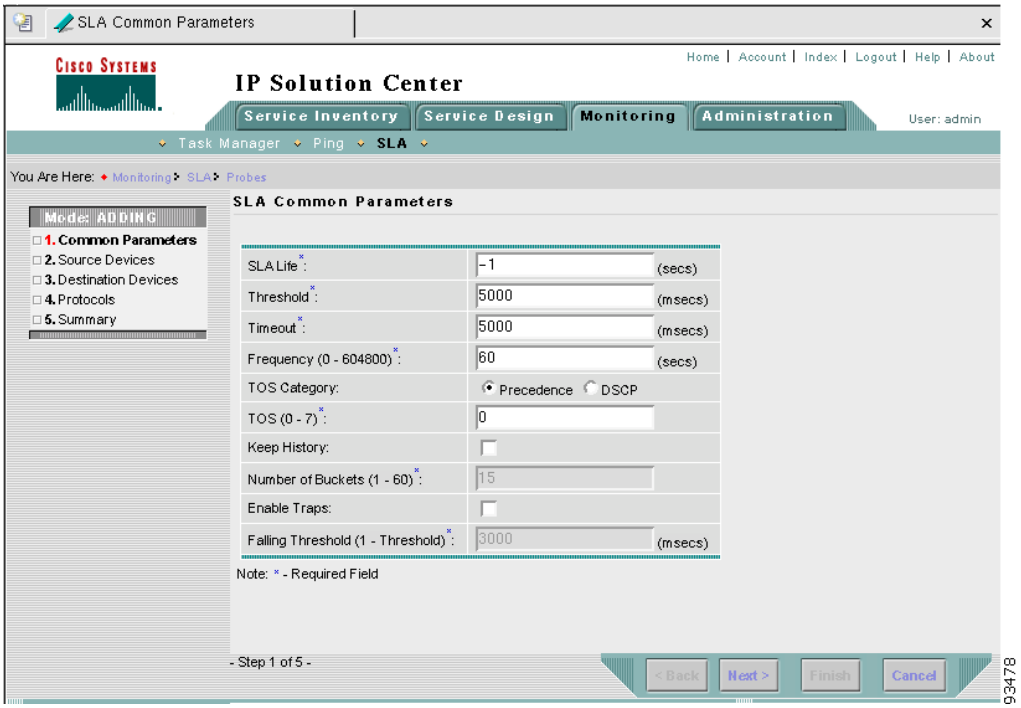
Figure 7-33 SLA Probes > Create > From MPLS PE or MVRF-CE



You then proceed through the following steps:

Step 1 The first window to appear is as shown in Figure 7-34, "SLA Common Parameters."

Figure 7-34 SLA Common Parameters



Accept the defaults or change the information in the fields of the common SLA parameters, as follows, and then click **Next**:

- **SLA Life** (required) is the number of seconds that the probe is active (with the maximum value of a 32-bit integer in seconds). If the value is set to **-1**, the typical and default value, the probe is active forever.
- **Threshold** (required) is an integer that defines the threshold limit in milliseconds. When this threshold is exceeded and traps are enabled, a trap is sent. 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 value for **Threshold** must not exceed the value for **Timeout**. The default value is **5000**.
- **Timeout** (required) is the duration in milliseconds to wait for an SA Agent operation completion. The value for **Timeout** must be less than or equal to the value for **Frequency** and greater than or equal to the value for **Threshold**. The default value is **5000**
- **Frequency (0 - 604800)** (required) is the duration in seconds between initiating each SA Agent operation. The value for **Frequency** must be greater than or equal to the value for **Timeout**. The default value is **60**.
- **TOS Category** (default: **Precedence**) If you select the **Precedence** radio button for **TOS Category**, you have one set of type of service (TOS) values. If you select the **DSCP** radio button for **TOS Category**, you have a different set of TOS values.
- **TOS** (required) is an integer. The range and meanings of the values depend on whether the radio button in the **TOS Category** is set to **Precedence** (values: 0 to 7) or **DSCP** (values: 0 to 63).
  - When the **TOS Category** is set to **Precedence**, the valid values are **0** to **7**. These values represent the three most significant bits of the ToS field in an IP header. The default value is **0**. The meanings of the **Precedence** values are specified in Table 7-3, "Meanings of Precedence Values."

Note Type of Service does not apply to the **DNS** and **DHCP** types of SLA probes. ISC ignores any ToS value set for these two types of SLA probes. For example, if you first select a ToS value of 5, then select the **DNS**, **DHCP,** and **ICMP Echo** protocols for an SLA probe, ISC applies the selected ToS value to the **ICMP Echo** probe only.

Table 7-3 Meanings of Precedence Values

ToS Value	Binary Value	Meaning
7	111	Network Control
6	110	Internetwork Control
5	101	CRITIC/ECP
4	100	Flash Override
3	011	Flash
2	010	Immediate
1	001	Priority
0	000	Routine

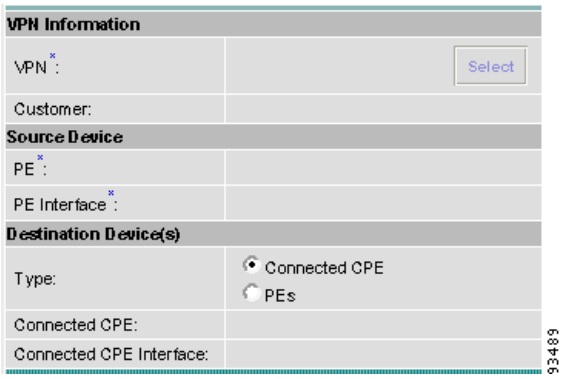
– When the **TOS Category** is set to **DSCP**, the valid values are **0** to **63**. These values represent the six most significant bits of this ToS field in an IP header. The default value is **0**. The interpretation of these **TOS** values is user specified.

Note ISC maps the 0 - 7 PRECEDENCE values to the three most significant ToS bits by left-shifting the value by five positions. Similarly, the 0 - 63 DSCP values are left-shifted by two positions.

- **Keep History** (default: deselected) If you select the **Keep History** check box, you indicate to keep the recent History Table on the router. Specifically, it is kept in the SA Agent MIB that keeps the raw round-trip time (RTT) SLA measurement. This selection also enables you to indicate the **Number of Buckets** of raw history data to keep. If you leave the default of a deselected check box for **Keep History**, no raw history data is kept. **Keep History** is not supported for **HTTP** and **Jitter**.
- **Number of Buckets (1 - 60)** (required) The default is **15** when the **Keep History** check box is selected. The range is 1 to 60 and indicates the number of most recent raw data entries to be kept in the raw history data. When the specified **Number of Buckets** is surpassed, removal of buckets starts with the oldest bucket to keep only the number of raw data entries specified.
- **Enable Traps** (default: deselected, which means No) If you select the **Enable Traps** check box, the created SLA is configured to send three types of traps. This selection also enables you to indicate the **Falling Threshold**. If you leave the **Enable Traps** box deselected, the traps are disabled on the SLAs created in this task.
- **Falling Threshold (1 - Threshold)** (required) The default is **3000** in milliseconds when the **Enable Traps** box is selected. The range is **1** to the **Threshold** value in milliseconds. When traps are enabled and the delay meets the specified number of milliseconds, a trap is sent.

Step 2 The next window to appear is as shown in Figure 7-35, "SLA CPE Parameters."

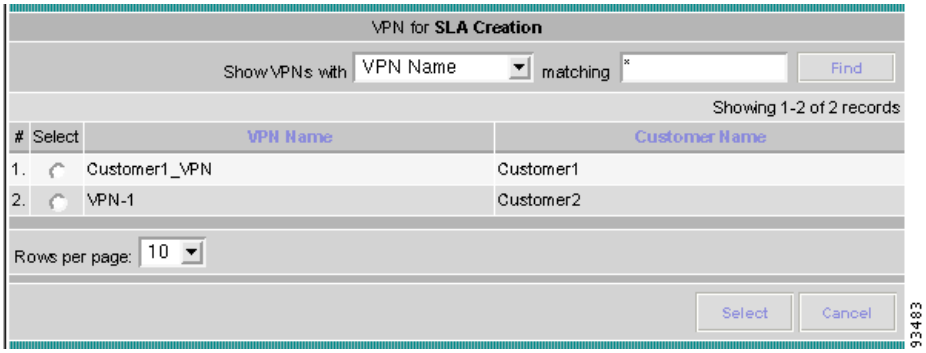
Figure 7-35 SLA CPE Parameters



Step 3 Click the **Select** button for **VPN** and a window appears as shown in Figure 7-36, "Select VPN," which lists all the VPNs in the database. At the top of this window you can select the drop-down menu for **Show VPNs with** and select **VPN Name** or **Customer Name**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the VPN you want to select. Then click **Select**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Figure 7-36 Select VPN

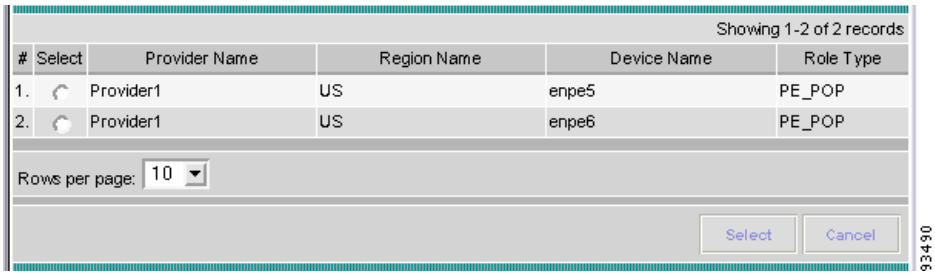


Step 4 You return to Figure 7-35 and the newly added VPN and Customer information appears. You can change the VPN and Customer by repeating Step 3.

Step 5 Click the new **Select** button for **PE** and a window appears as shown in Figure 7-37, "Select PE," which lists all the PEs associated with the selected VPN.Click the box next to the row for the PE you want to select. Then click **Select**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Figure 7-37 Select PE

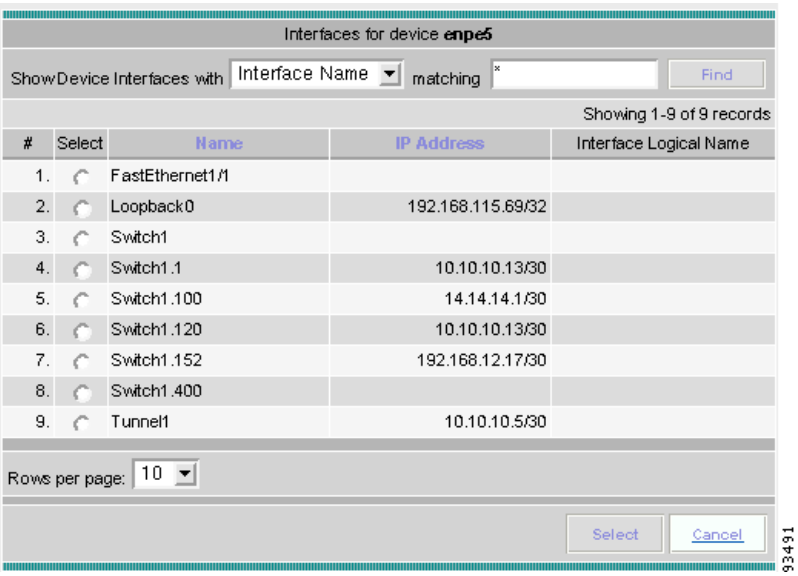


Step 6 You return to Figure 7-35 and the newly added PE information appears. You can change the PE by repeating Step 5.

Step 7 Click the new **Select** button for **PE Interface** and a window appears as shown in Figure 7-38, "Select Device Interface," which lists all the PE Interfaces in the database. At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *****; and then click **Find**. Click the box next to the row for the Device Interface you want to select. Then click **Select**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Figure 7-38 Select Device Interface

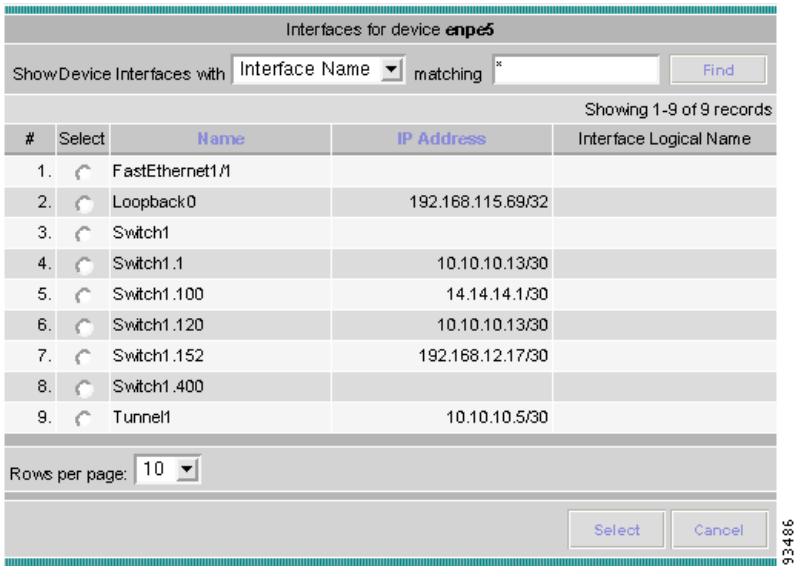


Step 8 You return to Figure 7-35 and the newly added **PE Interface** information appears. You can change the PE Interface by repeating Step 7.

Step 9 You can keep the default **Type**, by leaving the radio button for **Connected CPE** chosen or you can select the radio button for **PEs**. If you keep the default of **Connected PE**, proceed to Step 10. If you click the **PEs** radio button, proceed to Step 13.

Step 10 Click **Select** for **Connected PE Interface** and a window appears as shown in Figure 7-39, "Connected PE Interface."

Figure 7-39 Connected PE Interface



#	Select	Name	IP Address	Interface Logical Name
1.		FastEthernet1/1		
2.		Loopback0	192.168.115.69/32	
3.		Switch1		
4.		Switch1.1	10.10.10.13/30	
5.		Switch1.100	14.14.14.1/30	
6.		Switch1.120	10.10.10.13/30	
7.		Switch1.152	192.168.12.17/30	
8.		Switch1.400		
9.		Tunnel1	10.10.10.5/30	

At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *****; and then click **Find**. Click the box next to the row for the VPN you want to select. Then click **Select**.

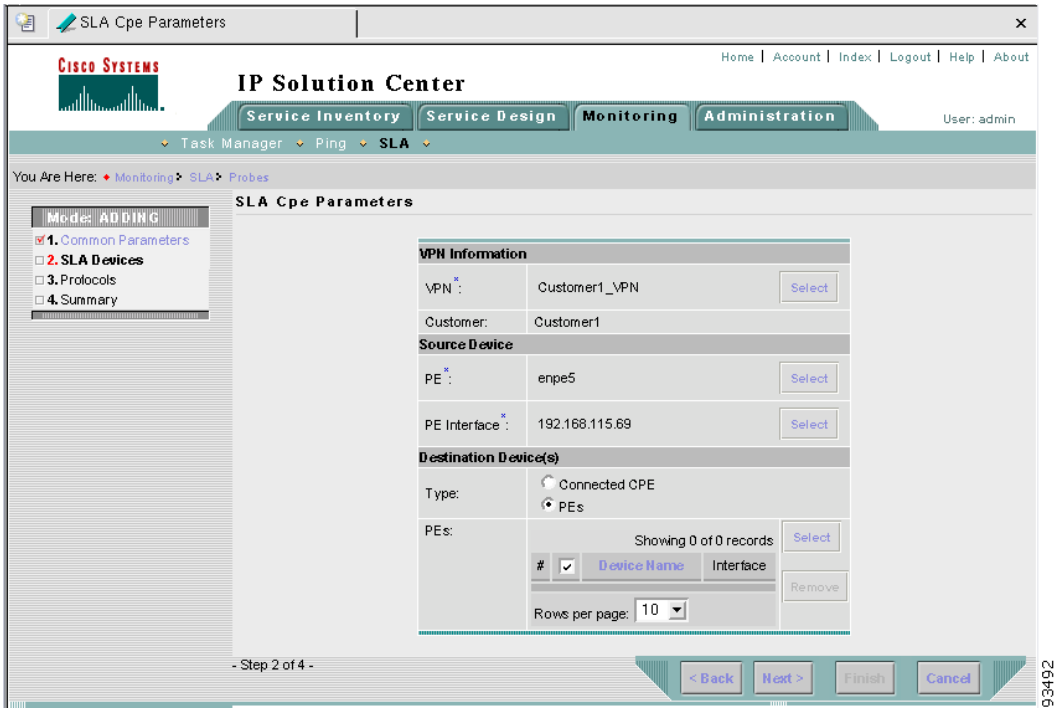
Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Step 11 You return to Figure 7-35 and the newly added **Connected PE Interface** appears. You can change the Connected PE Interface by repeating Step 10.

Step 12 Click **Next** and proceed to the "Protocols" section on page 7-41.

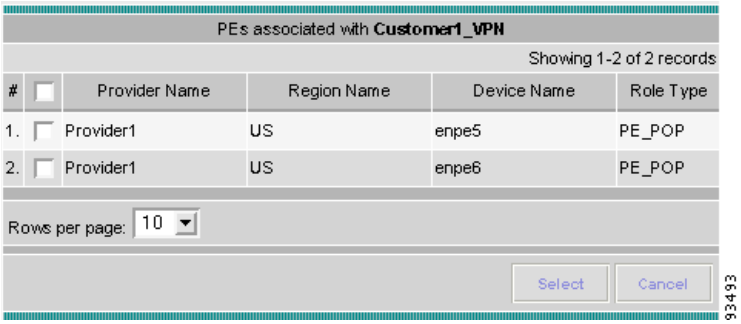
Step 13 When you click **PEs**, the window is as shown in Figure 7-40, "PEs."

Figure 7-40 PEs



Step 14 Click the **Select** button for **PE** and a window appears as shown in Figure 7-41, "Select PE Associated with the Specified VPN," which lists all the PEs associated with the specified VPN of the source PE.

Figure 7-41 Select PE Associated with the Specified VPN



Select the check box(es) next to the row(s) for the PE you want to select or the check box in the header row to select all the listed PEs. Then click **Select**.

Note Do *not* add a device chosen as a **Source Device** to **Destination Device(s)**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Step 15 You return to Figure 7-40 and the newly added **Device Name** appears.

Step 16 Click **Select** in the **Interface** column and a window appears as in Figure 7-39.

At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the VPN you want to select. Then click **Select**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Step 17 You return to Figure 7-40 and the newly added **PE Interface** appears. You can change the PE Interface by repeating Step 16.

Step 18 Select the check box next to each row for the Devices you want to remove or select the check box in the heading row to select all the Devices you want to remove. Then click the **Remove** button and a window as shown in Figure 7-40 appears without the removed Device(s).

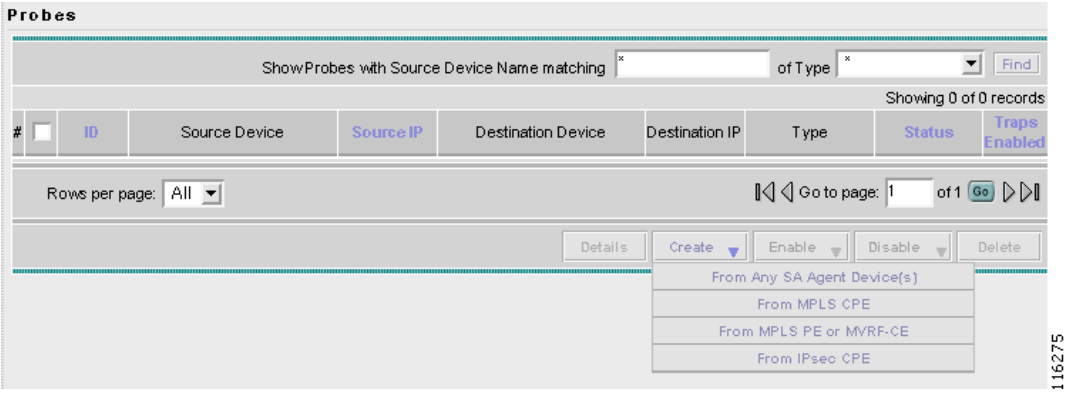
Step 19 When Figure 7-40 reflects what you want, click **Next** and proceed to the "Protocols" section on page 7-41.

Create from IPsec CPE

- **This feature is NOT SUPPORTED in this release.** -

When you navigate **Monitoring > SLA > Probes** and select no probe, you have access to the **Create** button. From the **Create** drop-down menu, you can select **From IPsec CPE**, as shown in Figure 7-42, "SLA Probes > Create > From IPsec CPE."

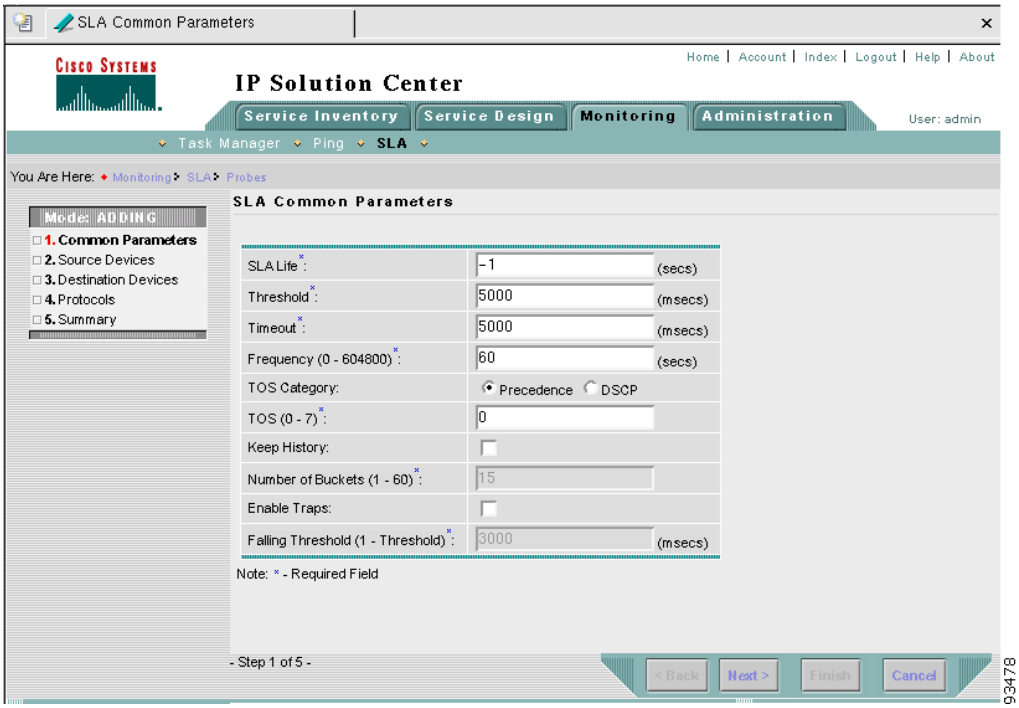
Figure 7-42 SLA Probes > Create > From IPsec CPE



You then proceed through the following steps:

Step 1 The first window to appear is as shown in Figure 7-34, "SLA Common Parameters."

Figure 7-43 SLA Common Parameters



Accept the defaults or change the information in the fields of the common SLA parameters, as follows, and then click **Next**:

- **SLA Life** (required) is the number of seconds that the probe is active (with the maximum value of a 32-bit integer in seconds). If the value is set to **-1**, the typical and default value, the probe is active forever.
- **Threshold** (required) is an integer that defines the threshold limit in milliseconds. When this threshold is exceeded and traps are enabled, a trap is sent. 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 value for **Threshold** must not exceed the value for **Timeout**. The default value is **5000**.
- **Timeout** (required) is the duration in milliseconds to wait for an SA Agent operation completion. The value for **Timeout** must be less than or equal to the value for **Frequency** and greater than or equal to the value for **Threshold**. The default value is **5000**
- **Frequency (0 - 604800)** (required) is the duration in seconds between initiating each SA Agent operation. The value for **Frequency** must be greater than or equal to the value for **Timeout**. The default value is **60**.
- **TOS Category** (default: **Precedence**) If you select the **Precedence** radio button for **TOS Category**, you have one set of type of service (TOS) values. If you select the **DSCP** radio button for **TOS Category**, you have a different set of TOS values.
- **TOS** (required) is an integer. The range and meanings of the values depend on whether the radio button in the **TOS Category** is set to **Precedence** (values: 0 to 7) or **DSCP** (values: 0 to 63).
  - When the **TOS Category** is set to **Precedence**, the valid values are **0** to **7**. These values represent the three most significant bits of the ToS field in an IP header. The default value is **0**. The meanings of the **Precedence** values are specified in Table 7-4, "Meanings of Precedence Values."

Note Type of Service does not apply to the **DNS** and **DHCP** types of SLA probes. ISC ignores any ToS value set for these two types of SLA probes. For example, if you first select a ToS value of 5, then select the **DNS**, **DHCP,** and **ICMP Echo** protocols for an SLA probe, ISC applies the selected ToS value to the **ICMP Echo** probe only.

Table 7-4 Meanings of Precedence Values

ToS Value	Binary Value	Meaning
7	111	Network Control
6	110	Internetwork Control
5	101	CRITIC/ECP
4	100	Flash Override
3	011	Flash
2	010	Immediate
1	001	Priority
0	000	Routine

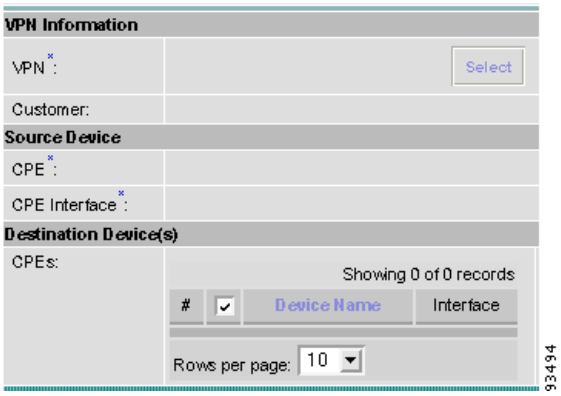
– When the **TOS Category** is set to **DSCP**, the valid values are **0** to **63**. These values represent the six most significant bits of this ToS field in an IP header. The default value is **0**. The interpretation of these **TOS** values is user specified.

Note ISC maps the 0 - 7 PRECEDENCE values to the three most significant ToS bits by left-shifting the value by five positions. Similarly, the 0 - 63 DSCP values are left-shifted by two positions.

- **Keep History** (default: deselected) If you select the **Keep History** check box, you indicate to keep the recent History Table on the router. Specifically, it is kept in the SA Agent MIB that keeps the raw round-trip time (RTT) SLA measurement. This selection also enables you to indicate the **Number of Buckets** of raw history data to keep. If you leave the default of a deselected check box for **Keep History**, no raw history data is kept. **Keep History** is not supported for **HTTP** and **Jitter**.
- **Number of Buckets (1 - 60)** (required) The default is **15** when the **Keep History** check box is selected. The range is 1 to 60 and indicates the number of most recent raw data entries to be kept in the raw history data. When the specified **Number of Buckets** is surpassed, removal of buckets starts with the oldest bucket to keep only the number of raw data entries specified.
- **Enable Traps** (default: deselected, which means No) If you select the **Enable Traps** check box, the created SLA is configured to send three types of traps. This selection also enables you to indicate the **Falling Threshold**. If you leave the **Enable Traps** box deselected, the traps are disabled on the SLAs created in this task.
- **Falling Threshold (1 - Threshold)** (required) The default is **3000** in milliseconds when the **Enable Traps** check box is selected. The range is **1** to the **Threshold** value in milliseconds. When traps are enabled and the delay meets the specified number of milliseconds, a trap is sent.

Step 2 The next window to appear is as shown in Figure 7-44, "SLA CPE Parameters."

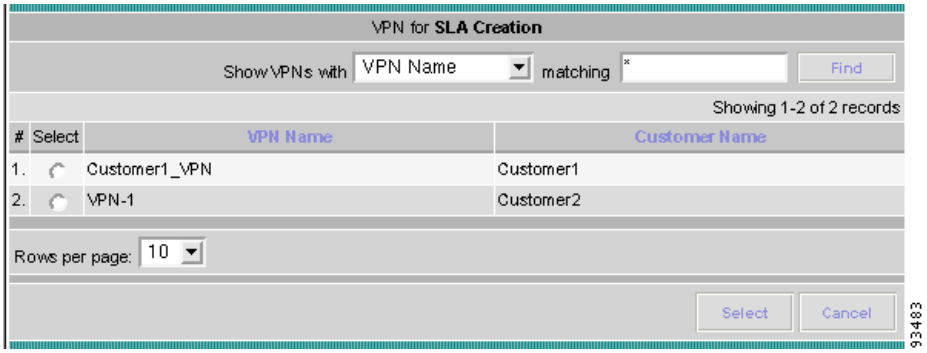
Figure 7-44 SLA CPE Parameters



Step 3 Click the **Select** button for **VPN** and a window appears as shown in Figure 7-45, "Select VPN," which lists all the VPNs in the database. At the top of this window you can select the drop-down menu for **Show VPNs with** and select **VPN Name** or **Customer Name**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the VPN you want to select. Then click **Select**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Figure 7-45 Select VPN

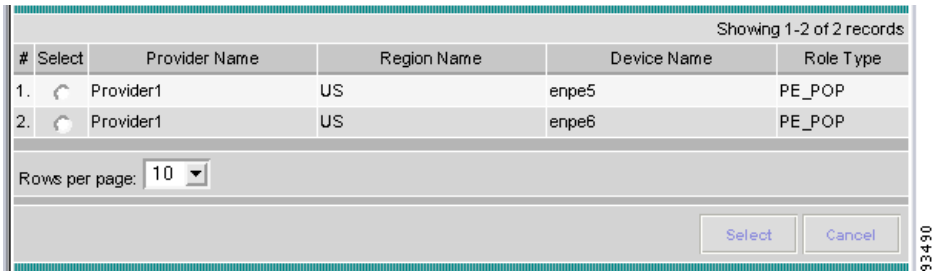


Step 4 You return to Figure 7-44 and the newly added VPN and Customer information appears. You can change the VPN and Customer by repeatingStep 3.

Step 5 Click the new **Select** button for **CPE** and a window appears as shown in Figure 7-46, "Select CPE," which lists all the CPEs associated with the selected VPN. Click the box next to the row for the CPE you want to select. Then click **Select**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Figure 7-46 Select CPE

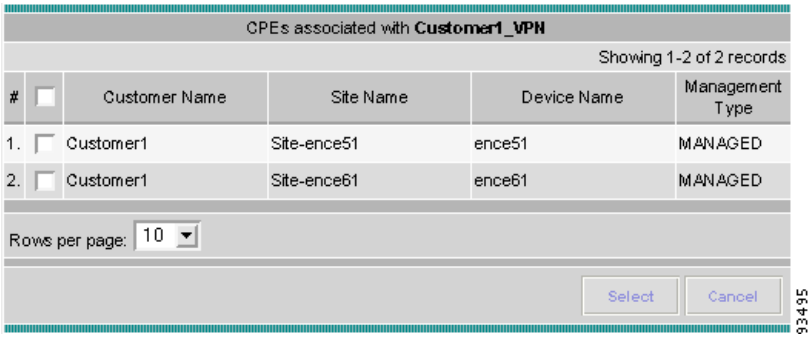


Step 6 You return to Figure 7-44 and the newly added CPE and CPE Interface information appears. You can change the CPE by repeating Step 5.

Step 7 You can change the CPE Interface by clicking the **Select** button for the CPE Interface and reselecting.

Step 8 Click the **Select** button for **CPEs** and a window appears as shown in Figure 7-47, "Select CPE Associated with the Specified VPN," which lists all the CPEs associated with the specified VPN of the source CPE.

Figure 7-47 Select CPE Associated with the Specified VPN



Select the check box(es) next to the row(s) for the CPE you want to select or select the check box in the header row to select all the listed CPEs. Then click **Select**.

Note Do *not* add a device chosen as a **Source Device** to **Destination Device(s)**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Step 9 You return to Figure 7-44 and the newly added devices appear. You can change the device by repeating Step 8.

Step 10 Click **Select** in the **Interface** column and a window appears as in Figure 7-39.

At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the VPN you want to select. Then click **Select**.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Step 11 You return to Figure 7-44 and the newly added **CPE Interface** appears. You can change the CPE Interface by repeating Step 10.

Step 12 Select the check box next to each row for the Devices you want to remove or select the check box in the heading row to select all the Devices you want to remove. Then click the **Remove** button and a window as shown in Figure 7-44 appears without the removed Device(s).

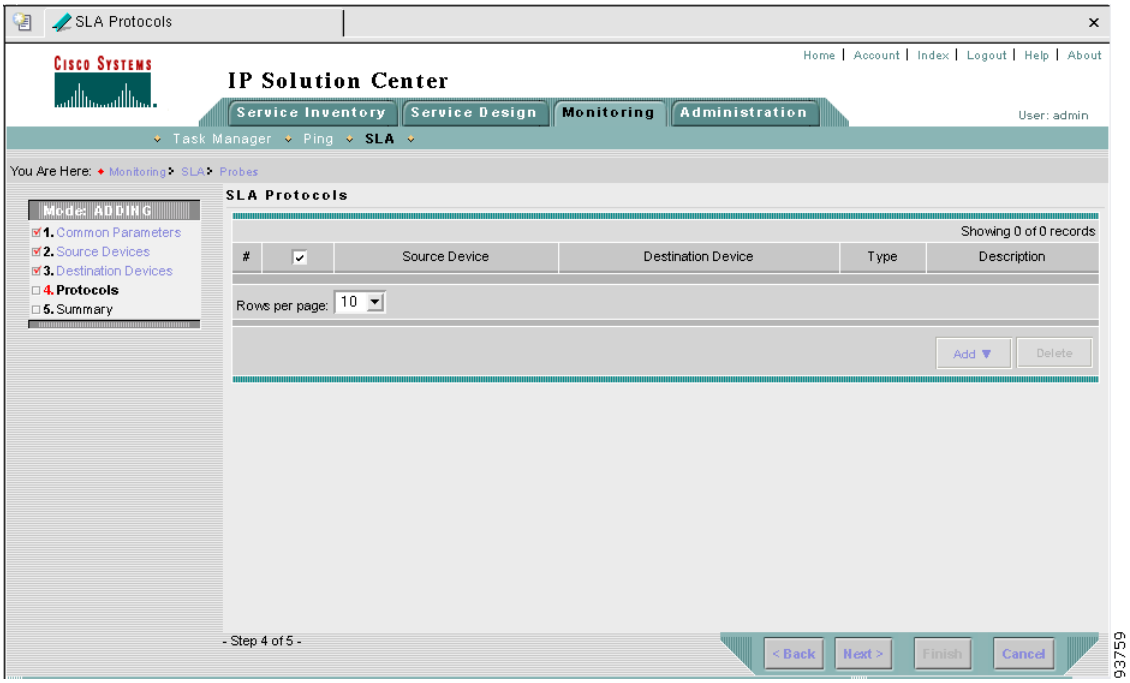
Step 13 When Figure 7-44 reflects what you want, click **Next** and proceed to the "Protocols" section on page 7-41.

Protocols

You navigate to this location after you have completed all the steps in one of the **Create** functions: Create From Any SA Agent Device(s), page 7-16; Create from MPLS CPE, page 7-22; Create From MPLS PE or MVRF-CE, page 7-29; or Create from IPsec CPE, page 7-36. Follow these steps:

Step 1 The next window to appear is as shown in Figure 7-48, "Protocols." At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**

Figure 7-48 Protocols

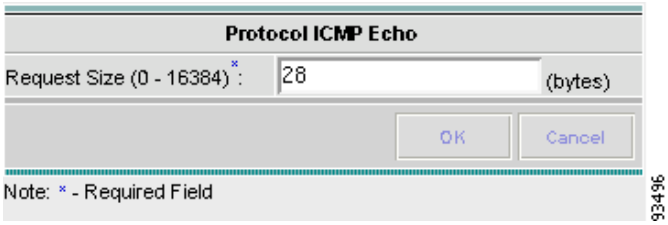


Step 2 Click the **Add** drop-down menu and select:

- **ICMP Echo** (only available if destination devices are available) Proceed to Step 3.
- **TCP Connect** (not available for Create from MPLS PE; for all the other Creates, TCP Connect is only available if destination devices are available) Proceed to Step 4.
- **UDP Echo** (only available if destination devices are available) Proceed to Step 5.
- **Jitter** (only available if destination devices are available) Proceed to Step 6.
- **FTP** (not available for Create from MPLS PE) Proceed to Step 7.
- **DNS** (not available for Create from MPLS PE) Proceed to Step 8.
- **HTTP** (not available for Create from MPLS PE) Proceed to Step 9.
- **DHCP** (not available for Create from MPLS PE) Proceed to Step 10.

Step 3 From Step 2, if you chose **ICMP Echo**, you receive a window as shown in Figure 7-49, "Protocol ICMP Echo."

Figure 7-49 Protocol ICMP Echo

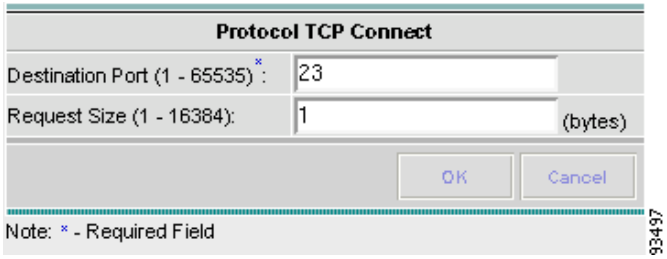


Enter the required information as follows, click **OK**, and then proceed to Step 11.

- **Request Size (0 - 16384)** (required) is a number that represents the number of octets (in bytes) to be placed into the data portion of the packet. The default is **28**.

Step 4 From Step 2, if you chose **TCP Connect**, you receive a window as shown in Figure 7-50, "Protocol TCP Connect."

Figure 7-50 Protocol TCP Connect

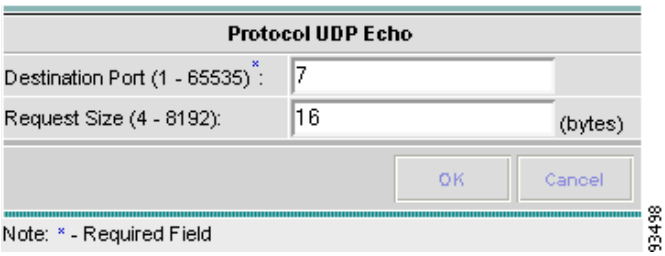


Enter the required and optional information as follows, click **OK**, and then proceed to Step 11.

- **Destination Port (1 - 65535)** (required) is the port number on the target to where the monitoring packets is sent. If you do not specify a specific port, port **23** is used.
- **Request Size (1 - 16384)** (optional) is a number that represents the number of octets (in bytes) to be placed into the data portion of the packet. The default is **1**.

Step 5 From Step 2, if you chose **UDP Echo**, you receive a window as shown in Figure 7-51, "Protocol UDP Echo."

Figure 7-51 Protocol UDP Echo

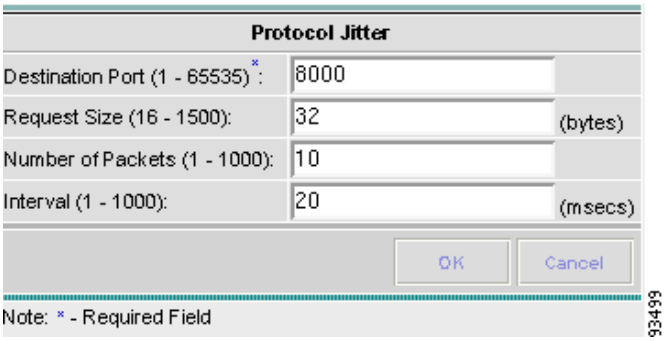


Enter the required and optional information as follows, click **OK**, and then proceed to Step 11.

- **Destination Port (1 - 65535)** (required) is the port number on the target to where the monitoring packets are sent. If you do not specify a specific port, port **7** is used.
- **Request Size (4 - 8192)** (optional) is a number that represents the number of octets (in bytes) to be placed into the data portion of the packet. The default is **16**.

Step 6 From Step 2, if you chose **Jitter**, you receive a window as shown in Figure 7-52, "Protocol Jitter."

Figure 7-52 Protocol Jitter

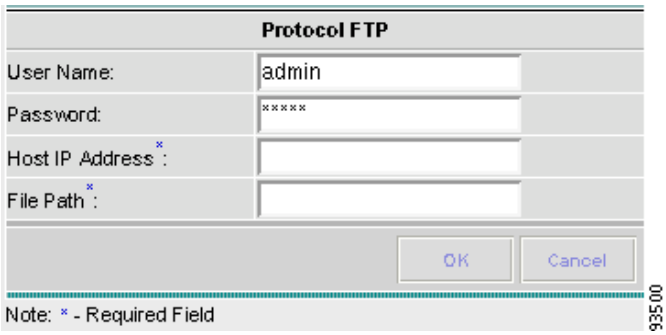


Enter the required and optional information as follows, click **OK**, and then proceed to Step 11.

- **Destination Port (1 - 65535)** (required) is the port number on the target to where the monitoring packets are sent. If you do not specify a specific port, port **8000** is used.
- **Request Size (16 - 1500)** (optional) is a number that represents the number of octets (in bytes) to be placed into the data portion of the packet. The default is **32**.
- **Number of Packets (1 - 1000)** (optional) is an integer that represents the number of packets that must be transmitted. The default value is **10**.
- **Interval (1 - 1000)** (optional) is an integer, **1** to **1,000**, that represents the inter-packet delay between packets in milliseconds.The default value is **20**.

Step 7 From Step 2, if you chose **FTP**, you receive a window as shown in Figure 7-53, "Protocol FTP."

Figure 7-53 Protocol FTP

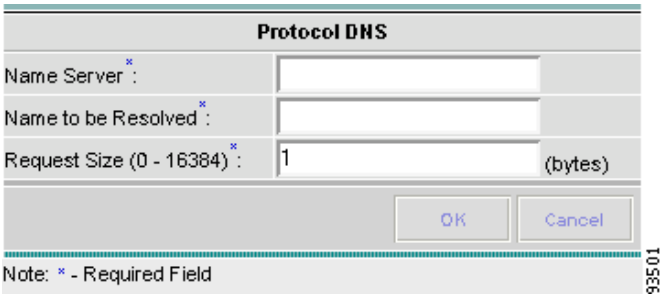


Enter the required and optional information as follows, click **OK**, and then proceed to Step 11.

- **User Name** (optional) If blank, **anonymous** is used.
- **Password** (optional) If blank, **test** is used.
- **Host IP Address** (required) Enter the IP address for File Transfer Protocol (FTP).
- **File Path** (required) Enter the path of the file you want to FTP on the FTP server.

Step 8 From Step 2, if you chose **DNS**, you receive a window as shown in Figure 7-54, "Protocol DNS."

Figure 7-54 Protocol DNS

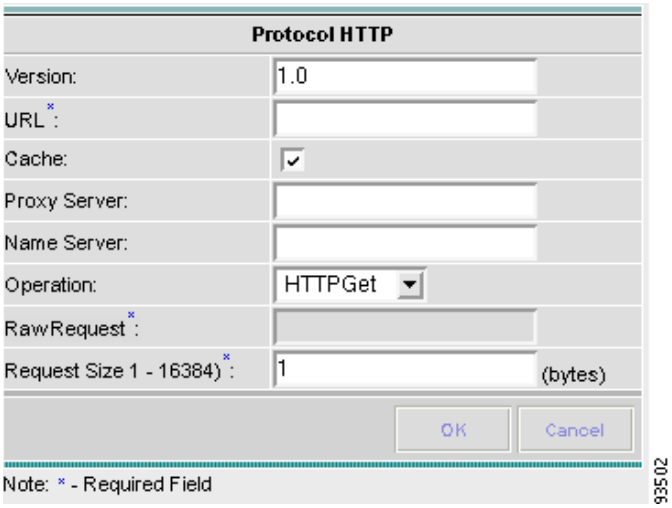


Enter the required information as follows, click **OK**, and then proceed to Step 11.

- **Name Server** (required) is the string that specifies the IP address of the name server. The address is in dotted IP address format.
- **Name to be Resolved** (required) is a string that is either the name or the IP address that is to be resolved by the DNS server. If the string is a name, the length is 255 characters. If the string is an IP address, it is in dotted IP address format.
- **Request Size (0 - 16384)** (required) is a number that represents the number of octets (in bytes) to be placed into the data portion of the packet. The default is **1**.

Step 9 From Step 2, if you chose **HTTP**, you receive a window as shown in Figure 7-55, "Protocol HTTP."

Figure 7-55 Protocol HTTP



Enter the optional and required information as follows, click **OK**, and then proceed to Step 11.

- **Version** (default: 1.0) is a string that specifies the version of the HTTP server. Do not change this. ISC only supports version 1.0.
- **URL** (required) is a string that represents the URL to which an HTTP probe should communicate, *HTTPServerName*[*/directory*]*/filename* or *HTTPServerAddress*[*/directory*]*/filename* (for example: **http://www.cisco.com/index.html** or **http://209.165.201.22/index.html**). If you specify the *HTTPServerName*, the **Name Server** is required. If you specify the *HTTPServerAddress*, the **Name Server** is not required.
- **Cache** (default: selected, which means Yes) For a deselected check box, the HTTP request should not download cached pages. For a selected check box, the HTTP request downloads cached pages if available, otherwise the request is forwarded to the HTTP server.
- **Proxy Server** (optional) is a string that represents the proxy server information (with a maximum of 255 characters). The default is the null string.
- **Name Server** (optional, dependent on the **URL** setting) is the string that specifies the IP address of the name server. The address is in dotted IP address format.
- **Operation** (default: **HTTPGet)** If you want **HTTPRaw**, which represents the HTTP request with user defined payload, instead of the default **HTTPGet** which represents the HTTP get request, use the drop-down menu and make that choice.
- **Raw Request** (required if the **Operation** is **HTTPRaw**; not available if the **Operation** is **HTTPGet**) is a string that is only needed if the **Operation** is **HTTPRaw**. It allows you to invoke other types of HTTP operations other than the simple GET operation.
- **Request Size (1 - 16384)** (required) is a number that represents the number of octets (in bytes) to be placed into the data portion of the packet. The default is **28**.

Step 10 From Step 2, if you chose **DHCP**, you have no information to add. Proceed to Step 11.

Step 11 You return to Figure 7-48 and additional columns of information now appear based on the Protocol information you provided. Before you click **Next** to proceed, determine if you want to **Add** more protocols, in which case repeat Step 2 to Step 10, or **Delete** any of the currently selected protocols, in which case, click **Delete** and proceed much as in Step 2 to Step 10 to now delete protocols.

Note There is no second chance for deleting destination devices. There is no confirm window.

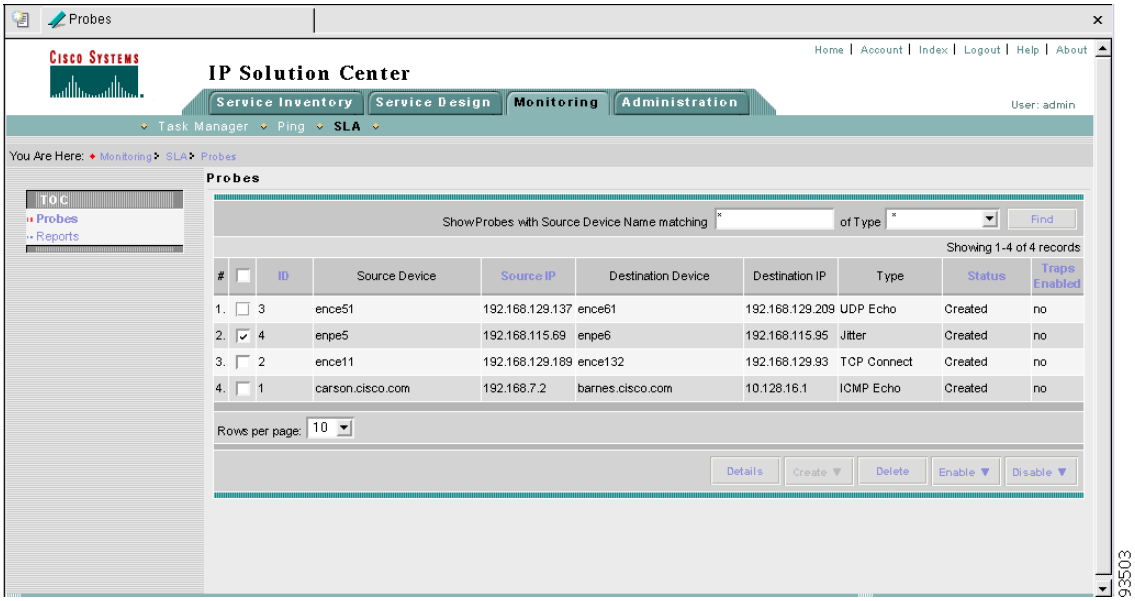
Step 12 The next window to appear is a Probe Creation Task Summary window that shows the **Description** (date and time created), **Common Parameters**, **Source Devices**, **Destination Devices**, and **Protocols** that you have defined. If all exists the way you want it, click **Finish**. Otherwise, click **Back** and make corrections.

Details

When you navigate **Monitoring > SLA > Probes**, you can get details by following these steps:

Step 1 Select an existing probe by selecting the corresponding check box for which you want details. Then you have access to the **Details** button, as shown in Figure 7-56, "SLA Probes > Details."

Figure 7-56 SLA Probes > Details



Step 2 After you click the **Details** button, you receive a window as shown in Figure 7-57, "SLA Probes Details." This includes the **Common Attributes** information defined when you first **Create** and the **Protocol Specific Attributes** information defined in the section Protocols.

Figure 7-57 SLA Probes Details

	Probe UDP Echo
Common Attributes	
Source IP Address:	192.168.129.137
Destination IP Address:	192.168.129.209
Status:	Created
SLA Life:	unlimited
Threshold:	5000 msecs
Timeout:	5000 msecs
Frequency:	60 secs
TOS Category:	PRECEDENCE
TOS:	0
Keep History:	false
Traps Enabled:	false
Protocol Specific Attributes	
Destination Port:	7
Request Size:	16 bytes

OK

93504

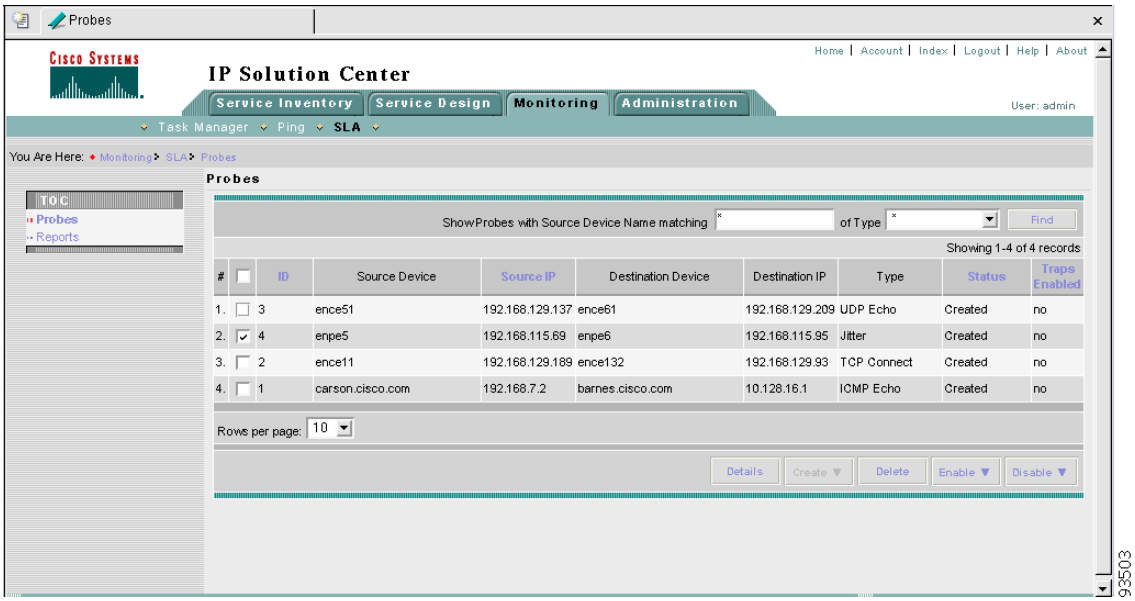
Step 3 Click **OK** to return to a window as shown in Figure 7-56. You can continue to select more **Details** or complete another function.

Delete

When you navigate **Monitoring > SLA > Probes**, you can delete probes from the list by following these steps:

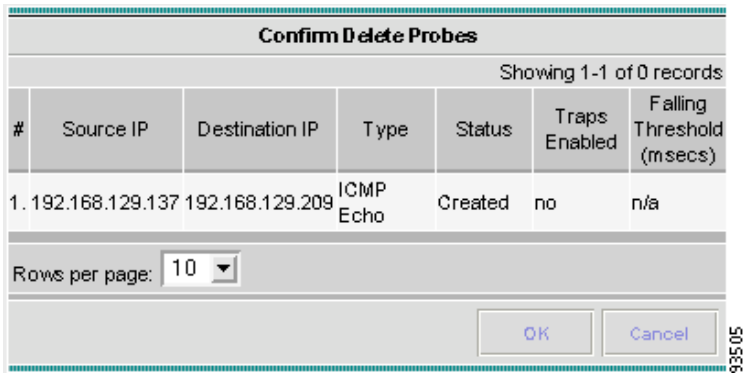
Step 1 Select one or more existing probes by clicking on the box(es) for the row(s) of existing probe(s) or you can click the box in the header row, to select all the probes. Then you have access to the **Delete** button, as shown in Figure 7-58, "SLA Probes > Delete."

Figure 7-58 SLA Probes > Delete



Step 2 After you click the **Delete** button, a window as shown in Figure 7-59, "Confirm Delete Probes," appears.

Figure 7-59 Confirm Delete Probes



Step 3 Click **OK** if Figure 7-59 reflects what you want to delete or click **Cancel** if it does not.

Note After the probe is deleted, it is deleted from the probe list page but still remains in the database.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

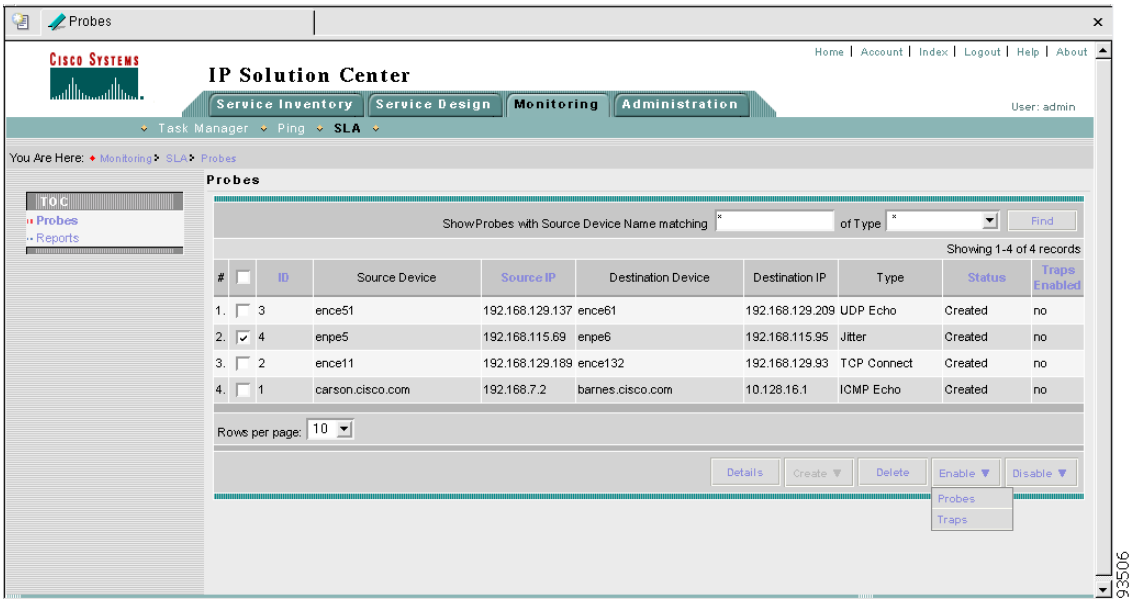
Step 4 You return to Figure 7-58 with updated information.

Enable Probes

When you navigate **Monitoring > SLA > Probes**, you can enable probes by following these steps:

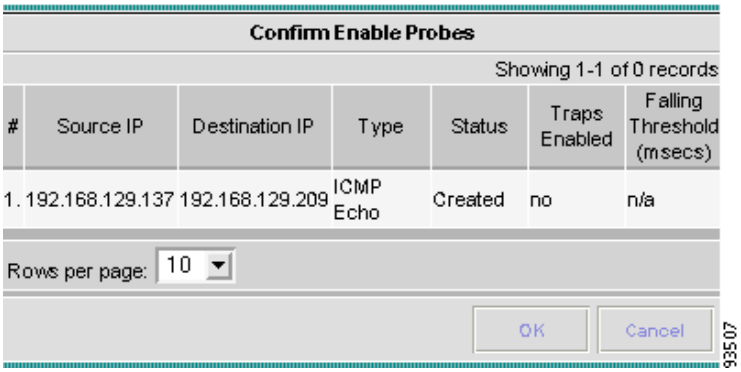
Step 1 Select one or more existing probes by clicking on the box(es) for the row(s) of existing probe(s) or you can click the box in the header row, to select all the probes. Then you have access to the **Enable** button. From the **Enable** drop-down menu, you have access to **Probes**, as shown in Figure 7-60, "SLA Probes > Enable > Probes."

Figure 7-60 SLA Probes > Enable > Probes



Step 2 After you select **Enable > Probes,** a window as shown in Figure 7-61, "Confirm Enable Probes," appears. All the traps have 3000 ms as the falling threshold set automatically.

Figure 7-61 Confirm Enable Probes



Step 3 Click **OK** if Figure 7-61 reflects the probes you want to enable or click **Cancel** if it does not. In both cases, you return to Figure 7-60.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

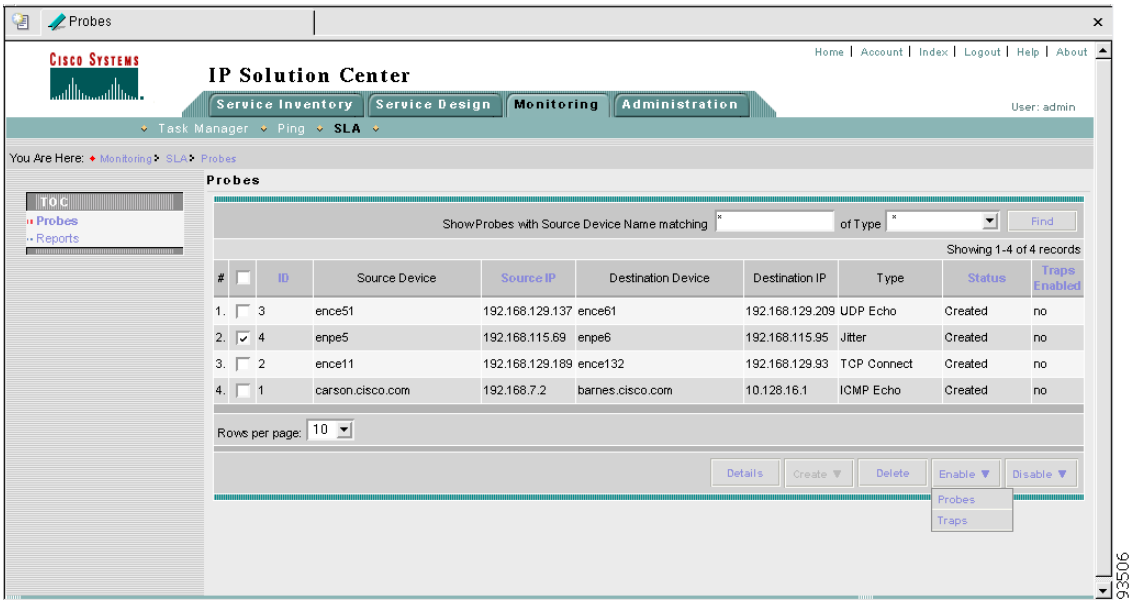
Step 4 If this was successful, you receive a Status window with a green check mark for **Succeeded**. The Status column is set to **Active** when the probe is created successfully on the router.

Enable Traps

When you navigate **Monitoring > SLA > Probes**, you can enable traps by following these steps:

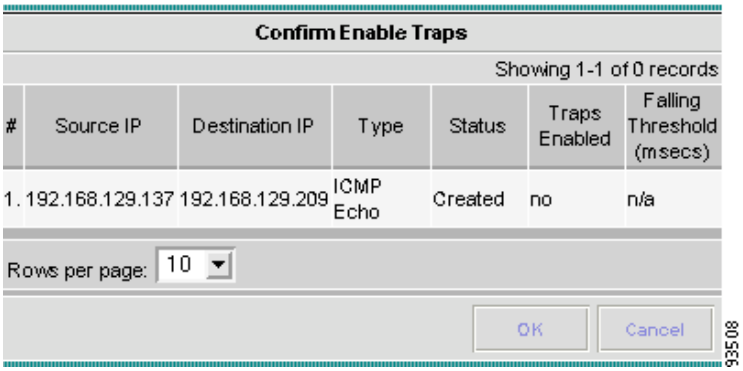
Step 1 Select one or more existing probes by clicking on the box(es) for the row(s) of existing probe(s) or you can click the box in the header row, to select all the probes. Then you have access to the **Enable** button. From the **Enable** drop-down menu, you have access to **Traps**, as shown in Figure 7-62, "SLA Probes > Enable > Traps."

Figure 7-62 SLA Probes > Enable > Traps



Step 2 After you select **Enable > Traps**, a window as shown in Figure 7-63, "Confirm Enable Traps," appears.

Figure 7-63 Confirm Enable Traps



Step 3 Click **OK** if Figure 7-63 reflects the traps you want to enable or click **Cancel** if it does not. In both cases you return to Figure 7-62.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

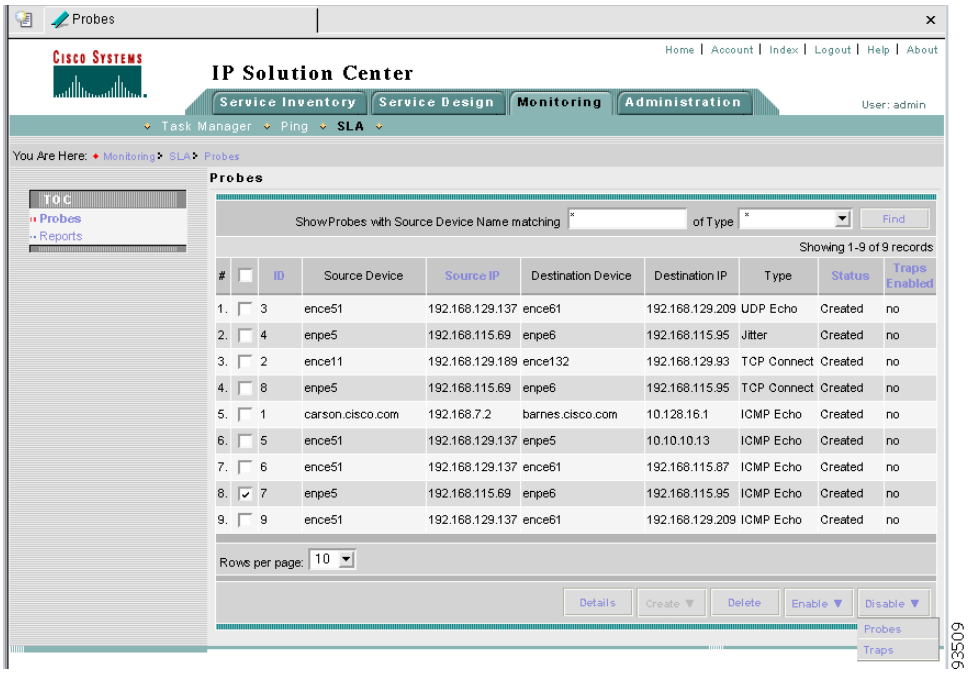
Step 4 If this was successful, you receive a Status window with a green check mark for **Succeeded**. The Traps Enabled column is set to **yes** when the probes on the router are successfully changed.

Disable Probes

When you navigate **Monitoring > SLA > Probes**, you can use **Disable Probes** to delete probes on the devices. Follow these steps:

Step 1 Select one or more enabled probes by clicking on the box(es) for the row(s) of existing probe(s) or you can click the box in the header row, to select all the probes. Then you have access to the **Disable** button. From the **Disable** drop-down menu, you have access to **Probes**, as shown in Figure 7-64, "SLA Probes > Disable > Probes."

Figure 7-64 SLA Probes > Disable > Probes



Step 2 After you select **Disable > Probes,** a window as shown in Figure 7-65, "Confirm Disable Probes," appears.

Figure 7-65 Confirm Disable Probes

Step 3 Click **OK** if Figure 7-65 reflects the probes you want to disable or click **Cancel** if it does not. In both cases you return to Figure 7-64.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

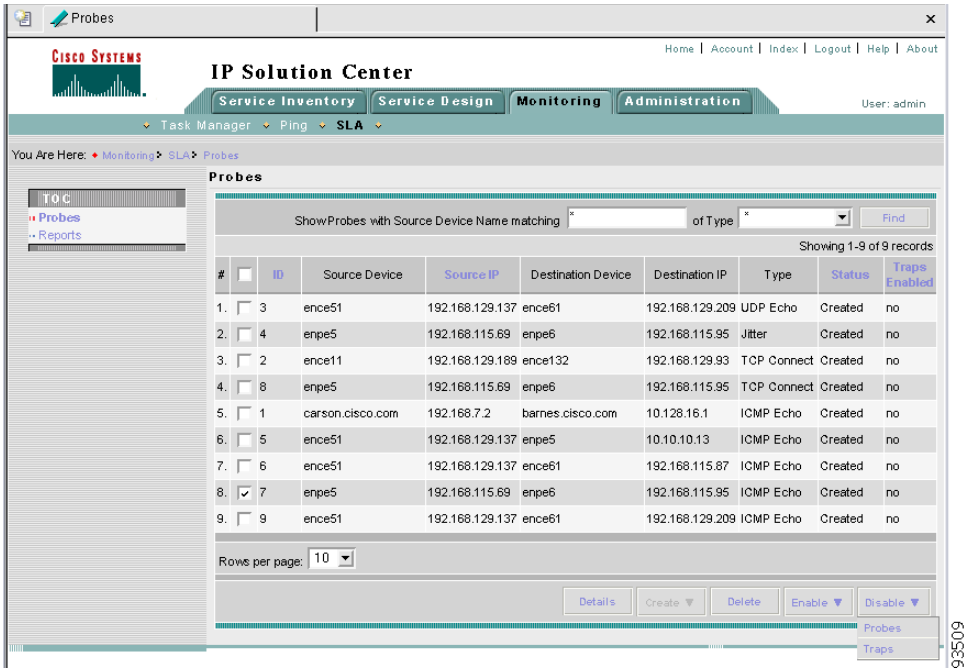
Step 4 If this was successful, you receive a Status window with a green check mark for **Succeeded**, and the probe's status becomes Disabled when the probe on the router is successfully removed.

Disable Traps

When you navigate **Monitoring > SLA > Probes**, you can disable traps by following these steps:

Step 1 Select one or more existing probes by clicking on the box(es) for the row(s) of existing probe(s) or you can click the box in the header row, to select all the probes. Then you have access to the **Disable** button. From the **Disable** drop-down menu, you have access to **Traps**, as shown in Figure 7-66, "SLA Probes > Disable > Traps."

Figure 7-66 SLA Probes > Disable > Traps



Step 2 After you select **Disable > Traps,** a window as shown in Figure 7-67, "Confirm Disable Traps," appears.

Figure 7-67 Confirm Disable Traps

Step 3 Click **OK** if Figure 7-67 reflects the traps you want to disable or click **Cancel** if it does not. In both cases you return to Figure 7-66.

Note At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Step 4 If this was successful, you receive a Status window with a green check mark for **Succeeded**. The traps are disabled when the probes on the router are successfully changed.

Reports

When you navigate **Monitoring > SLA > Reports**, you receive a window as shown in Figure 7-68, "SLA Reports."

Figure 7-68 SLA Reports

You can then click on any of the following choices and receive that report

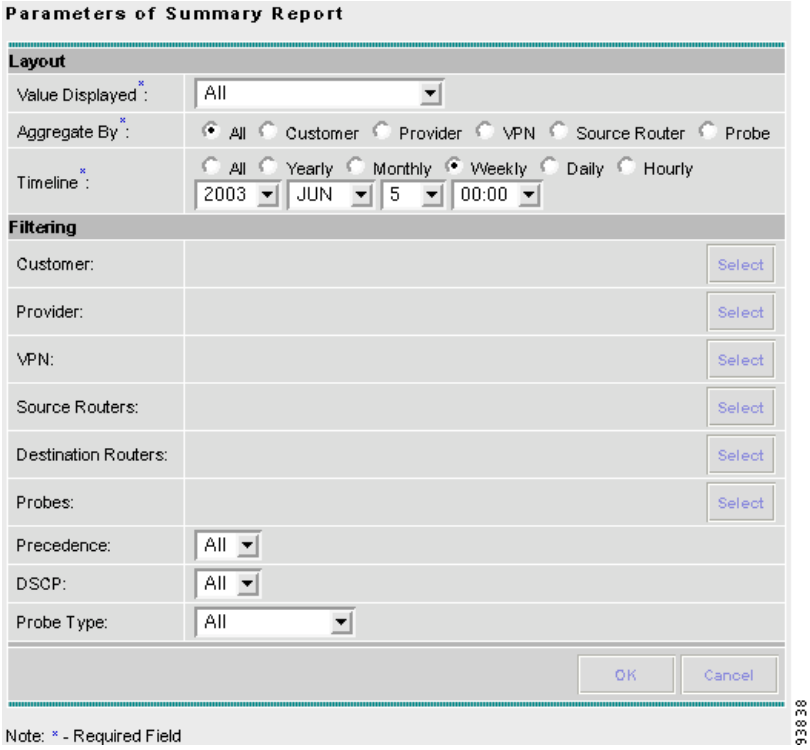
- Summary Report, page 7-55 This report summarizes all the information other than for HTTP and Jitter (ICMP Echo, TCP Connect, UDP Echo, FTP, DNS, and DHCP).
- HTTP Report, page 7-57 This is a summary report for HTTP information.
- Jitter Report, page 7-58 This is a summary report for Jitter information.
- Summary CoS Report, page 7-58 This report a summary report for Class of Service (CoS) other than for HTTP and Jitter (ICMP Echo, TCP Connect, UDP Echo, FTP, DNS, and DHCP).
- HTTP CoS Report, page 7-59 This report is for HTTP CoS information.
- Jitter CoS Report, page 7-59 This report is for Jitter CoS information.

Summary Report

From Figure 7-68, select **Summary Report** and proceed as follows:

Step 1 The resulting window is shown in Figure 7-69, "Parameters of Summary Report."

Figure 7-69 Parameters of Summary Report



Step 2 For Figure 7-69, fill in the **Layout** fields, as follows:

- **Value Displayed** (required) (default: **All**) Click the drop-down menu and select one of the following:
  - **All** to display all the values
  - **Connections (#)** to display the number of connections
  - **Timeouts (#)** to display the number of timeouts
  - **Connectivity (%)** to display connectivity as a percentage
  - **Threshold Violations (%)** to display threshold violations as a percentage
  - **Max Delay (ms)** to display the maximum delay in milliseconds
  - **Min Delay (ms)** to display the minimum delay in milliseconds
  - **Avg Delay (ms)** to display the average delay in milliseconds.

- **Aggregate By** (required) (default: All) Click the radio button for how you want to aggregate the data, by **All**, **Customer**, **Provider**, **VPN, Source Router**, or **Probe**.
- **Timeline** (required) (default: **Weekly**; starting with midnight of the first day of the selected week) Click the radio button for the report data that you want to display, **All** data; **Yearly** data; **Monthly** data; **Weekly** data; **Daily** data; or **Hourly** data. Also click the drop-down menus for the year, month, day of the month, and time of day for which to start the report.

Step 3 For Figure 7-69, fill in the **Filtering** fields, as follows:

Note The report contains only the data that fulfills all the conditions in the filtering fields (all the conditions are ANDed together).

- **Customer** (optional) Click the **Select** button and from the resulting list of Customers, filter the list if you choose. From the listed Customers, click the radio button for the Customer for which you want this SLA report. Then click Select. The result is that you return to Figure 7-69 and the selected customer is listed for **Customer**. You can repeat this process if you want to change your selection.
- **Provider** (optional) Click the **Select** button and from the resulting list of Providers, filter the list if you choose. From the listed Providers, click the radio button for the Provider for which you want this SLA report. Then click **Select**. The result is that you return to Figure 7-69 and the selected provider is listed for **Provider**. You can repeat this process if you want to change your selection.
- **VPN** (optional) Click the **Select** button and from the resulting list of VPNs, filter the list if you choose. From the listed VPNs, click the radio button for the VPN for which you want this SLA report. Then click **Select**. The result is that you return to Figure 7-69 and the selected VPN is listed for **VPN**. You can repeat this process if you want to change your selection.
- **Source Routers** (optional) Click the **Select** button and from the resulting list of devices, filter the list if you choose. From the listed devices, select the check box(es) for device(s) or the check box in the header row to select all the devices for which you want this SLA report. Then click **Select**. The result is that you return to Figure 7-69 and **Source Routers** contains the selected device(s). You can repeat this process if you want to change your selection.
- **Destination Routers** (optional) Click the **Select** button and from the resulting list of devices, filter the list if you choose. From the listed devices, select the check box(es) for device(s) or the check box in the header row to select all the devices for which you want this SLA report. Then click **Select**. The result is that you return to Figure 7-69 and **Destination Routers** contains the selected device(s). You can repeat this process if you want to change your selection.
- **Probes** (optional) Click the **Select** button and from the resulting list of source probes, filter the list if you choose. From the listed source probes, select the check box(es) for source probe(s) or the check box in the header row to select all the source probes for which you want this SLA report. Then click **Select**. The result is that you return to Figure 7-69 and **Probes** contains the selected source probe(s). You can repeat this process if you want to change your selection.
- **Precedence** (default: **All**) Click the drop-down menu to select the other **Precedence** TOS choices, **0** to **7**. These values represent the three most significant bits of the ToS field in an IP header. The meanings of the **Precedence** values are specified in Table 7-1, "Meanings of Precedence Values."

Note ISC maps the 0 - 7 PRECEDENCE values to the three most significant ToS bits by left-shifting the value by five positions.

Note Type of Service does not apply to the **DNS** and **DHCP** types of SLA probes. ISC ignores any ToS value set for these two types of SLA probes. For example, if you first select a ToS value of 5, then select the **DNS**, **DHCP,** and **ICMP Echo** protocols for an SLA probe, ISC applies the selected ToS value to the **ICMP Echo** probe only.

- **DSCP** (default: **All**) Click the drop-down menu to select the other **DSCP** TOS choices, **0** to **63**. These values represent the six most significant bits of this ToS field in an IP header. The interpretation of these **TOS** values is user specified.

Note ISC maps the 0 - 63 DSCP values to the six most significant ToS bits by left-shifting the values by two positions.

Note Type of Service does not apply to the **DNS** and **DHCP** types of SLA probes. ISC ignores any TOS value set for these two types of SLA probes. For example, if you first select a TOS value of 5, then select the **DNS**, **DHCP,** and **ICMP Echo** protocols for an SLA probe, ISC applies the selected ToS value to the **ICMP Echo** probe only.

- **Probe Type** (default: **All**) Click the drop-down menu to select from the following types of probes: ICMP Echo; UDP Echo; TCP Connect; HTTP; DNS; Jitter; DHCP; FTP.

Note These probe types are explained in detail in the "Protocols" section on page 7-41.

Step 4 Click **OK** in Figure 7-69 after you have the information you want.

Step 5 The result is a Summary Report with the selections you made listed. You can **Modify**, **Refresh**, **Print**, or **Close** this report with the appropriate button.

Note If you choose **Modify**, you receive a window such as Figure 7-69 in which you can modify your selections as explained in the previous steps.

HTTP Report

From Figure 7-68, select **HTTP Report** and proceed similarly to the "Summary Report" section on page 7-55, with the following exceptions:

- Value Displayed
- There is no **Destination Routers** selection
- There is no **Probe Type** drop-down menu in the equivalent of Figure 7-69, because the probe type is automatically **HTTP**. The result is an HTTP Report.

Jitter Report

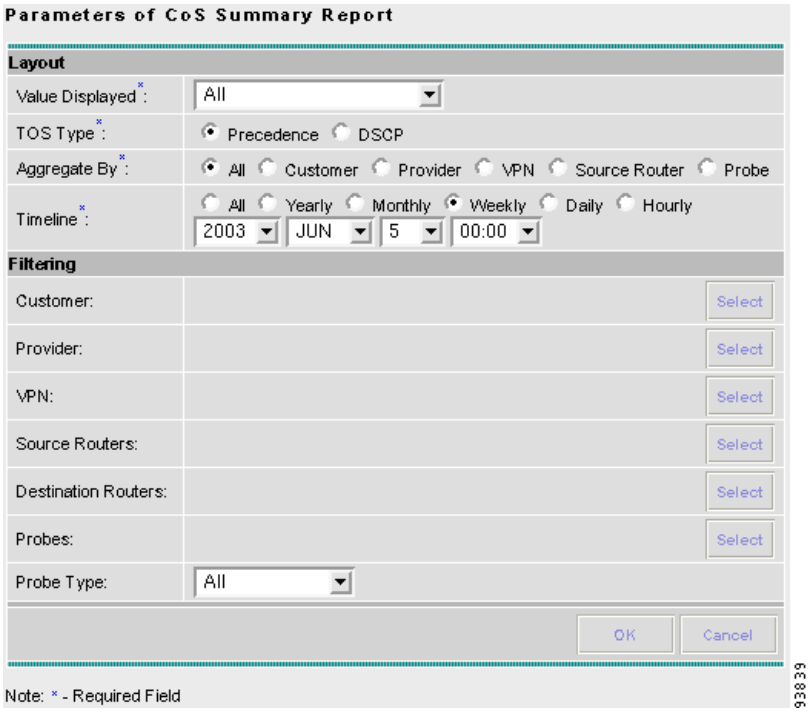
From Figure 7-68, select **Jitter Report** and proceed exactly as in the "Summary Report" section on page 7-55, with only two exceptions. There is no **Destination Routers** selection and there is no **Probe Type** drop-down menu in the equivalent of Figure 7-69, because the probe type is automatically **Jitter**. The result is a Jitter Report.

Summary CoS Report

From Figure 7-68, select **Summary CoS Report** for a summary of the Class of Service (CoS) reports, which are based on the TOS values of the SLA probes, and proceed as follows:

Step 1 The resulting window is shown in Figure 7-70, "Parameters of CoS Summary Report."

Figure 7-70 Parameters of CoS Summary Report



Step 2 For Figure 7-70, fill in the **Layout** fields, as shown in Step 2 of the "Summary Report" section on page 7-55, with the following exception. After **Value Displayed** and before **Aggregate By**, select the radio button **Precedence** (default) or **DSCP** for the new **TOS Type**. The explanations are given in the Filtering section, Step 3 of the "Summary Report" section on page 7-55.

Step 3 For Figure 7-70, fill in the **Filtering** fields, as shown in Step 3 of the "Summary Report" section on page 7-55, with the exception that there are no **Precedence** or **DSCP** drop-down menus, they are now in the **Layout** fields, as explained in Step 2 in this section.

Step 4 Click **OK** in Figure 7-70 after you have the information you want.

Step 5 The result is a CoS Summary Report with the selections you made listed. You can **Modify**, **Refresh**, **Print**, or **Close** this report with the appropriate button.

Note If you choose **Modify**, you receive a window such as Figure 7-70 in which you can modify your selections as explained in the previous steps.

HTTP CoS Report

From Figure 7-68, select **HTTP Report** and proceed exactly as in the "Summary CoS Report" section on page 7-58, with only two exceptions. There is no **Destination Routers** selection and there is no **Probe Type** drop-down menu in the equivalent of Figure 7-70, because the probe type is automatically **HTTP**. The result is an HTTP CoS Report. This CoS report is based on the TOS values of the SLA probes.

Jitter CoS Report

From Figure 7-68, select **Jitter Report** and proceed exactly as in the "Summary CoS Report" section on page 7-58, with only two exceptions. There is no **Destination Routers** selection and there is no **Probe Type** drop-down menu in the equivalent of Figure 7-70, because the probe type is automatically **Jitter**. The result is a Jitter CoS Report. This CoS report is based on the TOS values of the SLA probes.

TEM Performance Report

TEM Performance Report for Traffic Engineering Management is explained in detail in *Cisco IP Solution Center Traffic Engineering Management User Guide, 4.0.*