CHAPTER 7

Monitoring

From the Home window of Cisco IP Solution Center (ISC), which 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 choose the following selections:

- **Task Manager, page 7-1** Create and schedule tasks and monitor task run details.
- **Ping, page 7-9** Perform Ping connectivity tests.
- **SLA, page 7-12** Manage probes and view reports.
- **TE Performance Report, page 7-42** TE performance report.
- **Reports, page 7-42** Create and schedule reports.

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, page 7-2
- Task Logs, page 7-8

Tasks

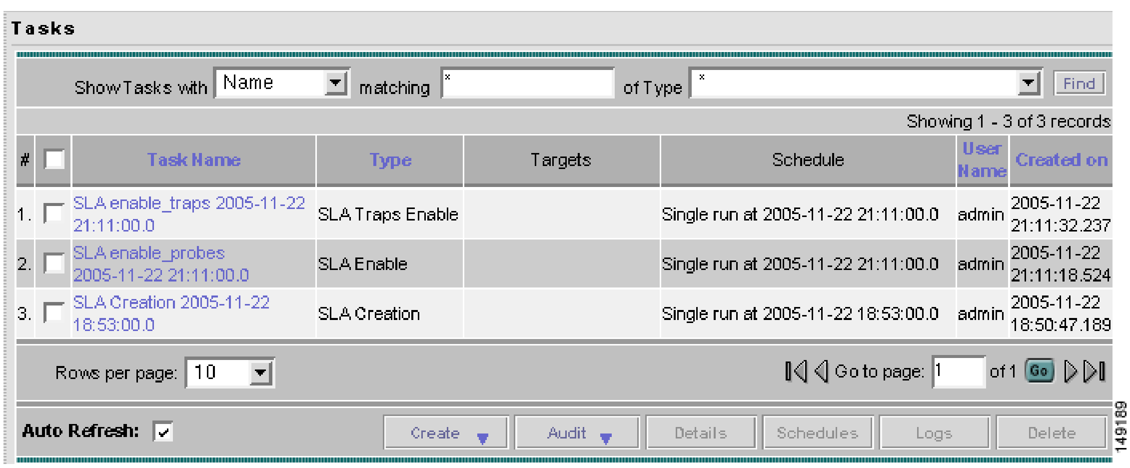
This section contains the following topics:

- Starting Task Manager, page 7-2
- Create, page 7-3
- Audit, page 7-6
- Details, page 7-6
- Schedules, page 7-7
- Logs, page 7-7
- Delete, page 7-7

Starting Task Manager

To start Task Manager, click the **Task Manager** icon. The Tasks list page appears, as shown in Figure 7-2, "Tasks."

Figure 7-2 Tasks



The Tasks window displays information about each task by **Task Name**, **Type**, **Targets**, **Schedules** date and time, the **User Name** who created those tasks, and the date **Created on**. To view, schedule, or delete the listed tasks, check the corresponding check box.

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

Create

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.
- **Collect Config From Files**—Collects configurations from files for MDE only.
- **Password Management**—Manages user passwords and SNMP community strings.
- **SLA Collection**—Collects data from SLA enabled devices.
- **Service Deployment**—Deploys an existing SR.
- **Synchronize Shared UNI**—This task is created automatically when there is a need to synchronize shared UNI attributes across services or links. This task cannot be created or deleted from the GUI. You can only add or change the schedules for this task.
- **TE Discovery**—Populates the repository with tunnel and route data from the Traffic Engineering network.
- **TE Interface Performance**—Calculates tunnel and 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)**. If you choose **Simplified**, you can make many selections in one window. If you choose **Advanced (via wizard)**, you navigate through many windows to make your selections.

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

Figure 7-4 Task Devices

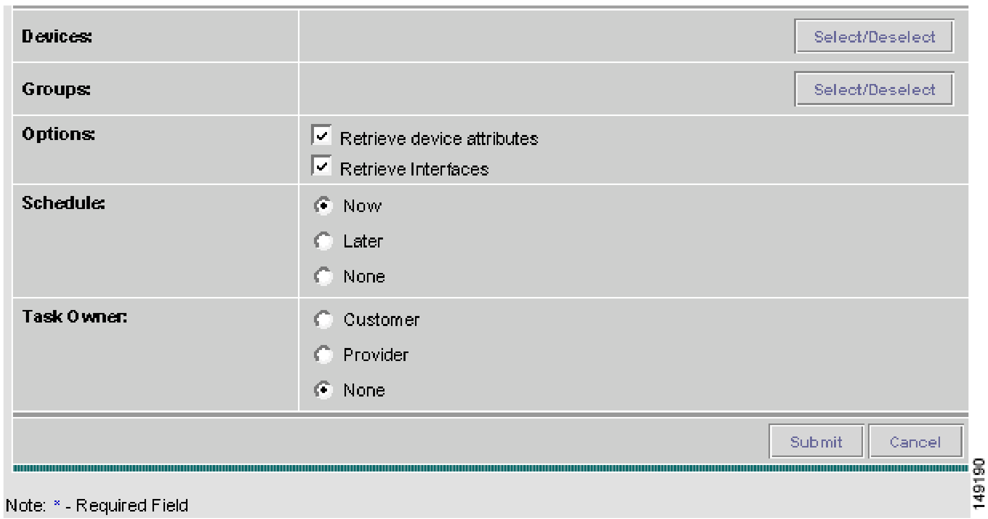


Figure 7-5 Service Deployment Task

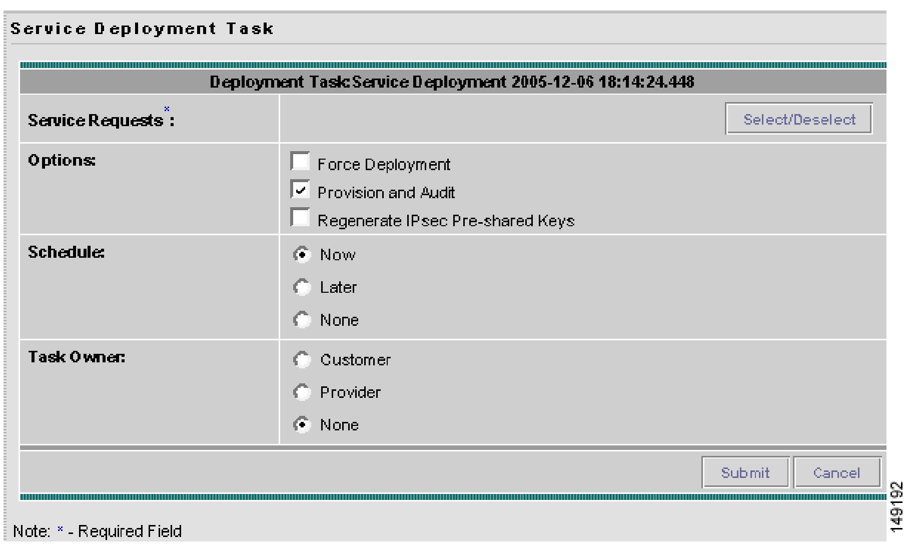
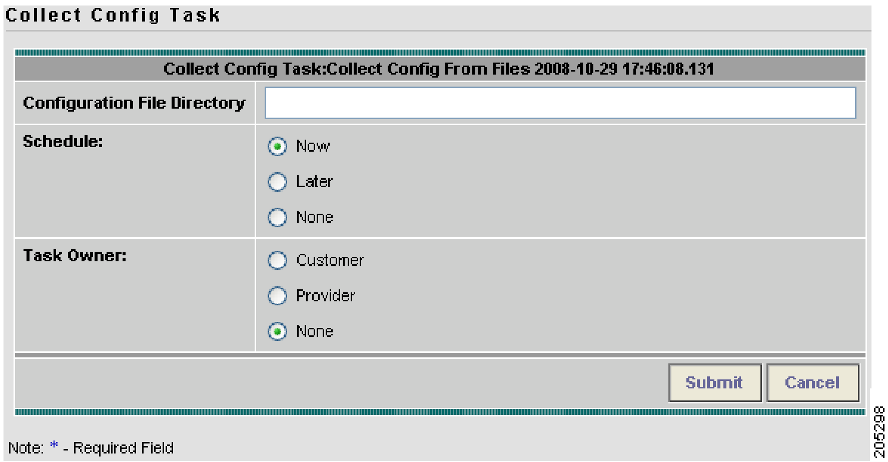


Figure 7-6 Collect Config From Files



Step 7 Where appropriate, click **Select/Deselect** to add devices or service requests.

> **Note** Step 7 to Step 10 do not apply for Collect Config From Files and TE Interface Performance.

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", Figure 7-5, "Service Deployment Task," or Figure 7-6, respectively.

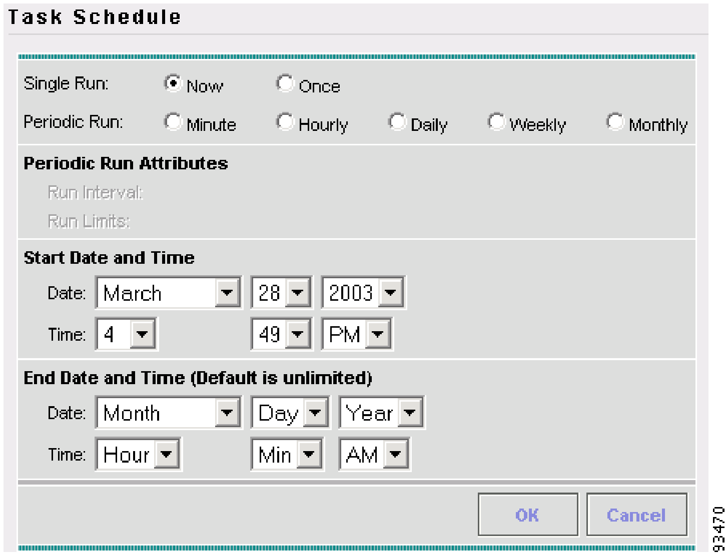
Step 9 **Groups** might or might not appear depending on the task you specify in the previous step. If it does appear, you can add groups of devices, similarly to Step 7 and Step 8. If it does not appear or after you complete this device group selection, proceed to Step 10.

Step 10 Choose the **Options**. If the **Retrieve Interfaces** check box is checked, ISC uses Simple Network Management Protocol (SNMP) to retrieve device interface information, such as ifIndex, and so on. If the **Retrieve Interfaces** check box is unchecked, configuration collection information is still retrieved, but SNMP is not used. All scenarios other than doing IP Service Level Agreement (SLA) probes do not require SNMP or this option.

Step 11 If **Configuration File Directory** appears, enter the path to the directory on your ISC server into the **Configuration File Directory** text box, to indicate the directory on the ISC server where the offline configuration files are stored.

Step 12 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 7-7, "Task Schedule Details."

Figure 7-7 Task Schedule Details



Step 13 Select information to schedule the task and click **OK** (default is to schedule **Now**).

Step 14 Click **Submit** to continue. The new task is added to the list of tasks.

Audit

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

- **Config Audit**—Compares ISC generated configlet against the one in the device.
- **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.

Details

To get details about a particular task, follow these steps:

Step 1 From the **Tasks** page, as shown in Figure 7-2, "Tasks," check a check box for one task for which you want to see a detailed list of information.

Step 2 Click **Details.**

Step 3 Click **OK** to return to Figure 7-2, "Tasks."

Schedules

To change the scheduling of an existing task, follow these steps:

Step 1 From the **Tasks** page, as shown in Figure 7-2, "Tasks," check a check box for the one task for which you want to reset the scheduling directions.

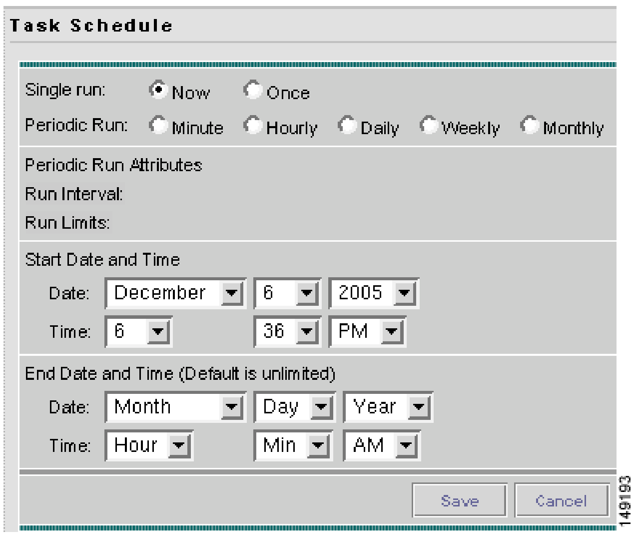
Step 2 Click **Schedules.**

Step 3 If you want to delete this task, proceed to Step 4. If you want to reset the scheduling directions, proceed to Step 5.

Step 4 In the new window, check the check box for the task you want to delete and click the **Delete** button. Then proceed to Step 7.

Step 5 In the new window, click **Create**, and you receive a window as shown in Figure 7-8, "Task Scheduling."

Figure 7-8 Task Scheduling



Step 6 Make the new scheduling selections you want and click **Save** to reset the scheduling directions.

Step 7 Uncheck any check boxes and click **OK** to return to Figure 7-2, "Tasks.'

Logs

This selection from the **Tasks** page, as shown in Figure 7-2, "Tasks," is another way of doing what is explained in the "Task Logs" section on page 7-8.

Delete

To delete one or more tasks, follow these steps:

Step 1 From the **Tasks** page, as shown in Figure 7-2, "Tasks," check one or more check boxes for the task(s) you want to delete. You receive a confirmation window.

Step 2 If you want to delete, click **OK**. If not, click **Cancel**.

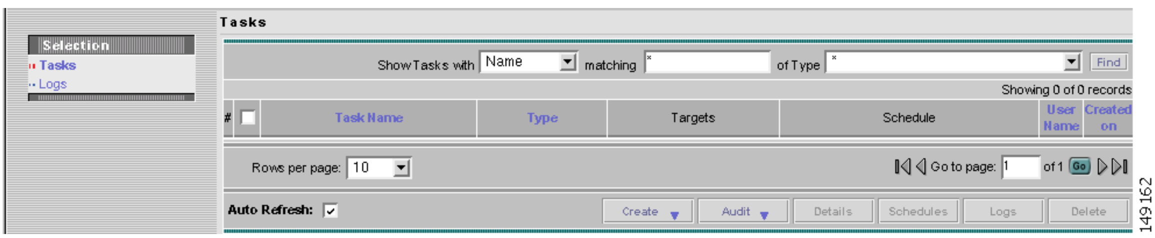
Step 3 You return to an updated **Tasks** page, as shown in Figure 7-2, "Tasks."

Task Logs

Task Logs can be used to understand the status of a task, whether 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:

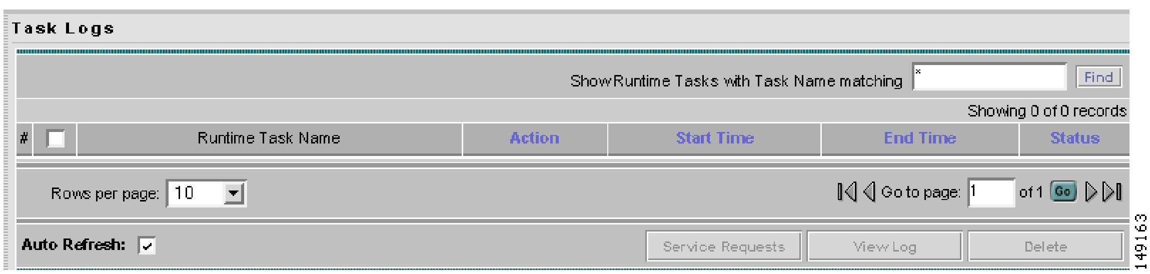
Step 1 Click **Task Manager**. The Tasks page appears, as shown in Figure 7-9, "Tasks."

Figure 7-9 Tasks



Step 2 Click **Logs** under the TOC heading located on the left-hand side. The Task Logs page appears, as shown in the Figure 7-10, "Task Logs."

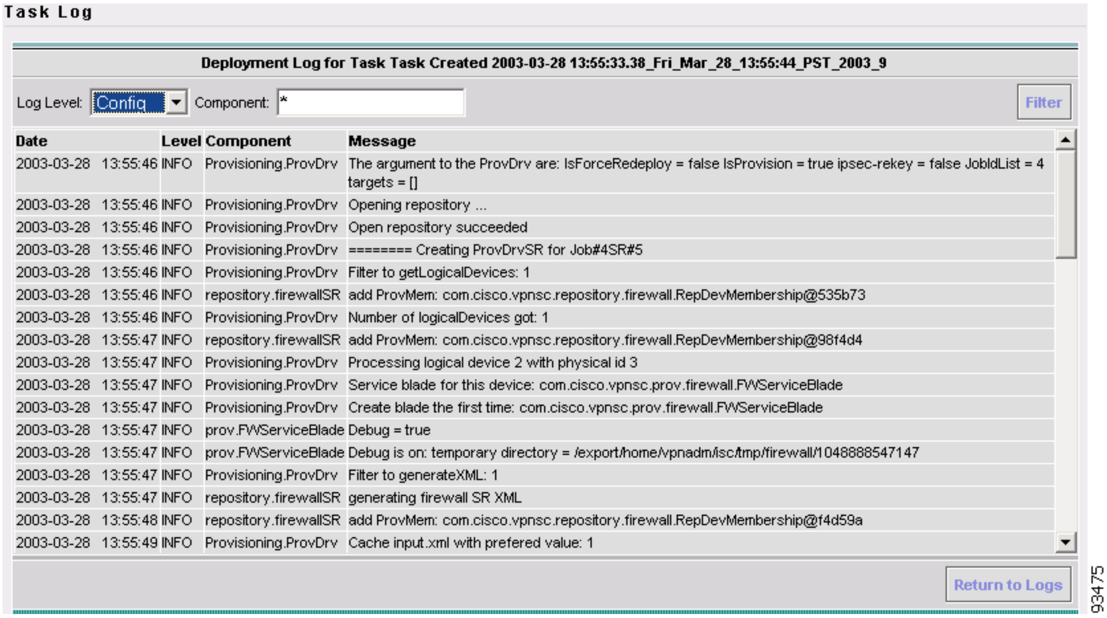
Figure 7-10 Task Logs



This window displays the task by **Runtime Task Name**, and the **Action**, **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, check the check box for the row that represents the task and click the **View Log** button. The Task Log page appears, as shown in Figure 7-11, "Task Log."

Figure 7-11 Task Log



Date	Level	Component	Message
2003-03-28 13:55:46	INFO	Provisioning.ProvDrv	The argument to the ProvDrv are: IsForceRedeploy = false IsProvision = true ipsec-rekey = false JobIdList = 4 targets = []
2003-03-28 13:55:46	INFO	Provisioning.ProvDrv	Opening repository ...
2003-03-28 13:55:46	INFO	Provisioning.ProvDrv	Open repository succeeded
2003-03-28 13:55:46	INFO	Provisioning.ProvDrv	======== Creating ProvDrvSR for Job#4SR#5
2003-03-28 13:55:46	INFO	Provisioning.ProvDrv	Filter to getLogicalDevices: 1
2003-03-28 13:55:46	INFO	repository.firewallSR	add ProvMem: com.cisco.vpnsc.repository.firewall.RepDevMembership@535b73
2003-03-28 13:55:46	INFO	Provisioning.ProvDrv	Number of logicalDevices got: 1
2003-03-28 13:55:47	INFO	repository.firewallSR	add ProvMem: com.cisco.vpnsc.repository.firewall.RepDevMembership@98f4d4
2003-03-28 13:55:47	INFO	Provisioning.ProvDrv	Processing logical device 2 with physical id 3
2003-03-28 13:55:47	INFO	Provisioning.ProvDrv	Service blade for this device: com.cisco.vpnsc.prov.firewall.FWServiceBlade
2003-03-28 13:55:47	INFO	Provisioning.ProvDrv	Create blade the first time: com.cisco.vpnsc.prov.firewall.FWServiceBlade
2003-03-28 13:55:47	INFO	prov.FWServiceBlade	Debug = true
2003-03-28 13:55:47	INFO	prov.FWServiceBlade	Debug is on: temporary directory = /export/home/vpnadm/isc/tmp/firewall/1048888547147
2003-03-28 13:55:47	INFO	Provisioning.ProvDrv	Filter to generateXML: 1
2003-03-28 13:55:47	INFO	repository.firewallSR	generating firewall SR XML
2003-03-28 13:55:48	INFO	repository.firewallSR	add ProvMem: com.cisco.vpnsc.repository.firewall.RepDevMembership@f4d59a
2003-03-28 13:55:49	INFO	Provisioning.ProvDrv	Cache input.xml with prefered value: 1

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 4 Click **Return to Logs** to specify another log to view.

Ping

Ping is the way ISC monitors the VPN connectivity, that is, verifies the connectivity among various edge devices comprising the VPN.

Note Ping features are not supported on devices running IOS XR.

To achieve this, you can perform a series of pings among these devices. Ping has the following benefits:

- Service independent and therefore can be used for functional auditing of MPLS applications.
- Can establish whether a service is working without doing a functional audit for that service.
- Can be used to verify IPv4 connectivity among CPEs prior to VPN service deployment.

However, Ping does not do the following:

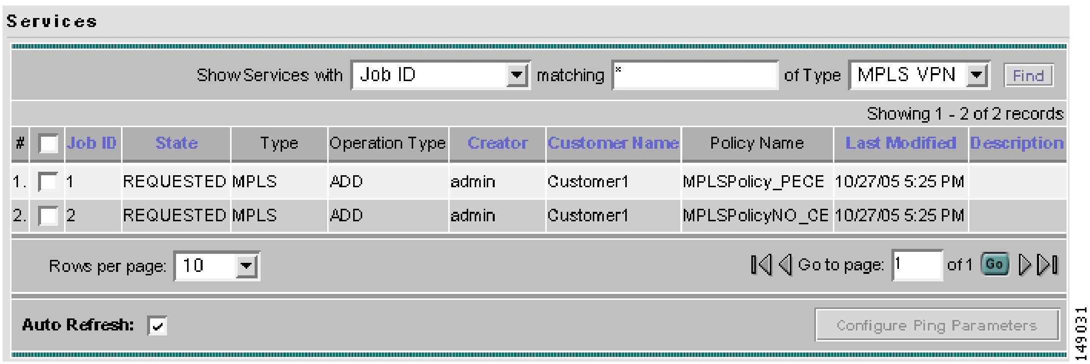
- Ping does not work in environments where ICMP traffic is blocked, for example, in a Cisco IOS router with an access-list denying all ICMP traffic.
- Ping can only inform you that there is a connectivity problem. It does not offer any service-specific information. The connectivity problem can be due 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.

Note ISC has a component Cisco MPLS Diagnostics Expert that might help you. See the *Cisco MPLS Diagnostics Expert 2.1.3 Failure Scenarios Guide on ISC 5.1*.

After you choose **Monitoring > Ping**, you receive a window as shown in Figure 7-12, "Services."

Figure 7-12 Services

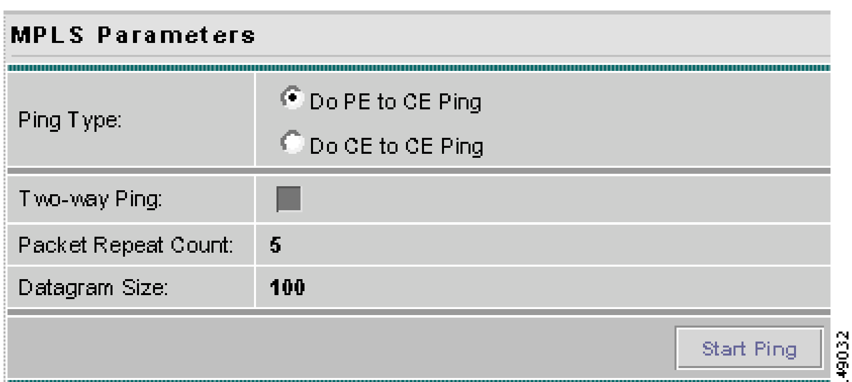


The **Type** field indicates **MPLS**. Follow these steps:

Step 1 Check the check box next to each row for which you want to configure ping parameters.

Step 2 Click the **Configure Ping Parameters** button, which becomes enabled. A window as shown in Figure 7-13, "MPLS Parameters," appears.

Figure 7-13 MPLS Parameters



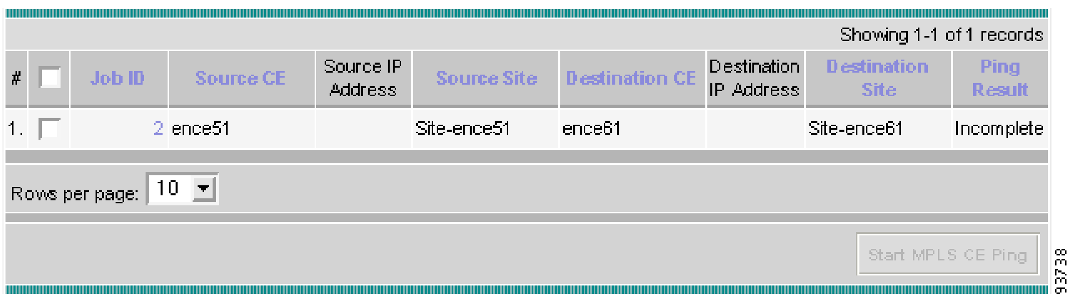
Fill in the following and then click **Start Ping**:

- **Ping Type: Do PE to CE Ping**—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 endpoint 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 Ping**, you go directly to Step 5 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 endpoint in the service request. When this selection is chosen, then after you click **Start Ping**, you go 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 checked, then a ping from device2 to device1 also occurs.
- **Packet Repeat Count** (default: 5)—This value indicates how many ICMP packets to use for a ping.
- **Datagram size** (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 7-14, "MPLS CE Selection."

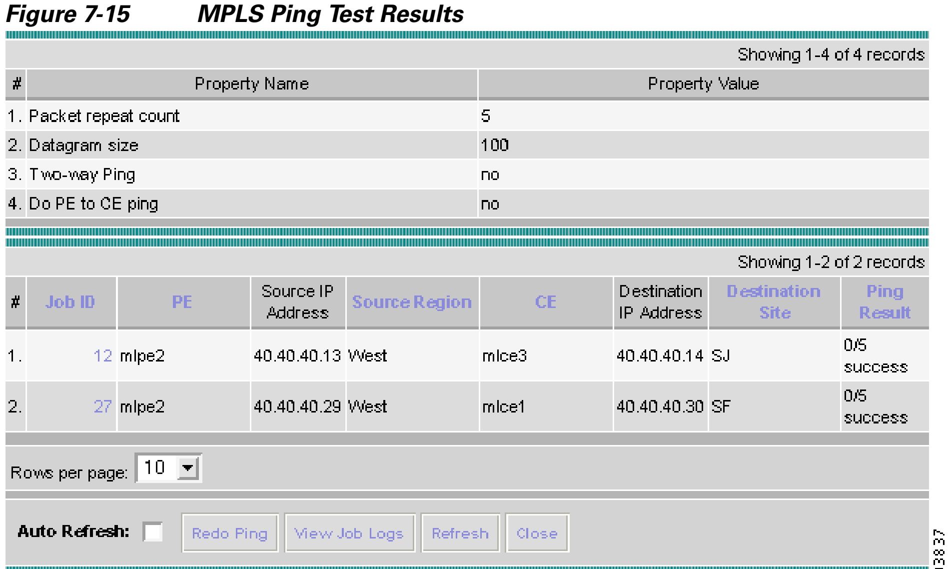
Figure 7-14 MPLS CE Selection



Step 4 Check the check box next to each row for which you want to select a CE.

Step 5 Click the **Start MPLS CE Ping** button, which becomes enabled. You receive a results window as shown in Figure 7-15, "MPLS Ping Test Results.

Figure 7-15 MPLS Ping Test Results



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.
- **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 6 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.

Note SLA features are not supported on devices running IOS XR.

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)
- 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 choose **Monitoring > SLA**, implement the setup procedures in the "Setup Prior to Using SLA" section on page 7-13."

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

- Probes, page 7-13 is the default selection.
- Reports, page 7-36

Setup Prior to Using SLA

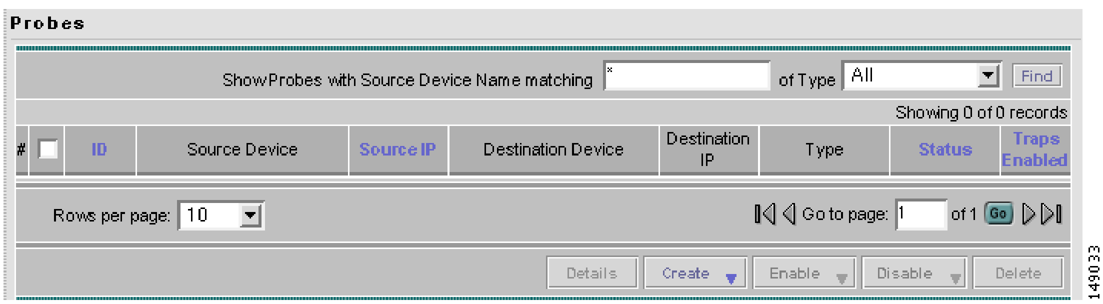
SLA is an SNMP activity. Be sure SNMP is enabled and the SNMP settings on the router match the settings in the repository.

When creating an SLA **From MPLS CPE** or **From MPLS PE or MVRF-CE**, the service requests associated with the devices *must* be in the Deployed state.

Probes

When you choose **Monitoring > SLA > Probes**, you receive a window as shown in Figure 7-16, "SLA Probes."

Figure 7-16 SLA Probes



The default button that is enabled is **Create** and from the **Create** drop-down list, you can choose to create SLA probes **From Any SA Agent Device(s)**; **From MPLS CPE**; or **From MPLS PE or MVRF-CE**. However, if you select one or more existing probes by clicking the row(s) of existing probe(s), then you have access to the other buttons, **Details**, **Delete**, **Enable**, and **Disable**. For **Enable** and **Disable**, the drop-down list contains options to enable or disable SLA **Probes** and SLA **Traps**.

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

- Create Common Parameters, page 7-14—This section explains the SLA common parameters for all of the probe creation types: **From Any SA Agent Device(s)**; **From MPLS CPE**; or **From MPLS PE or MVRF-CE**.
- Create From Any SA Agent Device(s), page 7-16—This section explains how to create probes from any SA Agent device(s) and begins after creating common parameters.
- Create from MPLS CPE, page 7-18—This section explains how to create probes from an MPLS CPE and begins after creating common parameters.
- Create From MPLS PE or MVRF-CE, page 7-23—This section explains how to create probes from an MPLS PE or MVRF-CE and begins after creating common parameters.
- Protocols, page 7-25—This section is common Probes information for each of the **Create** paths.

- Details, page 7-31—This section gives details about a specified probe.
- Delete, page 7-32—This section explains how to delete a probe.
- Enable Probes, page 7-33—This section explains how to enable the Probe and change its status from Created to Active state.
- Enable Traps, page 7-34—This section explains how to enable traps.
- Disable Probes, page 7-35—This section explains how to disable the Probe and change its status from Active to Disabled.
- Disable Traps, page 7-36—This sections explains how to disable traps.

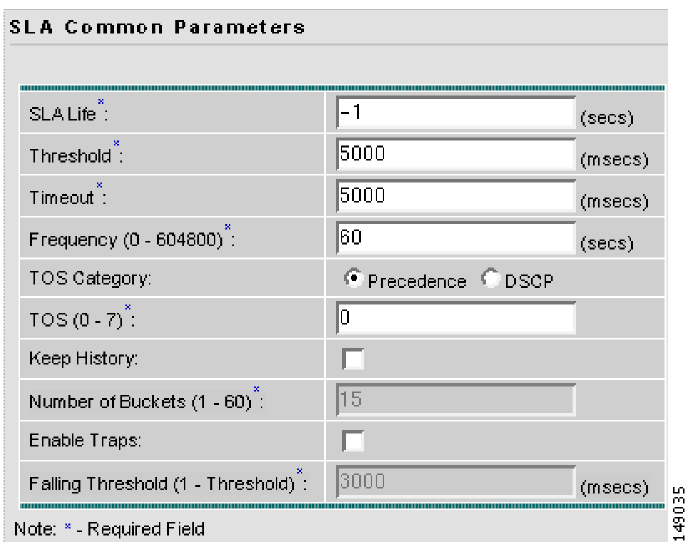
Create Common Parameters

When you choose **Monitoring > SLA > Probes**, the default is the **Probes** page with only the **Create** button enabled, as shown in Figure 7-16. From the **Create** drop-down list, you can choose **From Any SA Agent Device(s)**, **From MPLS CPE**, or **From MPLS PE or MVRF-CE**. The first window to appear in all ways of creation is specified here. Then you proceed to the specific creation type you have chosen.

Follow these steps:

Step 1 Choose **Create**, and the window to appear is as shown in Figure 7-17, "SLA Common Parameters."

Figure 7-17 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)—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)—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 service affecting agent (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)—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)—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 choose the **Precedence** radio button for **TOS Category**, you have one set of type of service (TOS) values. If you choose the **DSCP** radio button for **TOS Category**, you have a different set of TOS values.
- **TOS** (required)—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 choose a ToS value of 5, then choose 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: unchecked)**—If you check 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 an unchecked 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 checked. 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: unchecked, which means No)—If you check 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 unchecked, 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 checked**. 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 Next you proceed to Create From Any SA Agent Device(s), page 7-16, Create from MPLS CPE, page 7-18, or Create From MPLS PE or MVRF-CE, page 7-23.

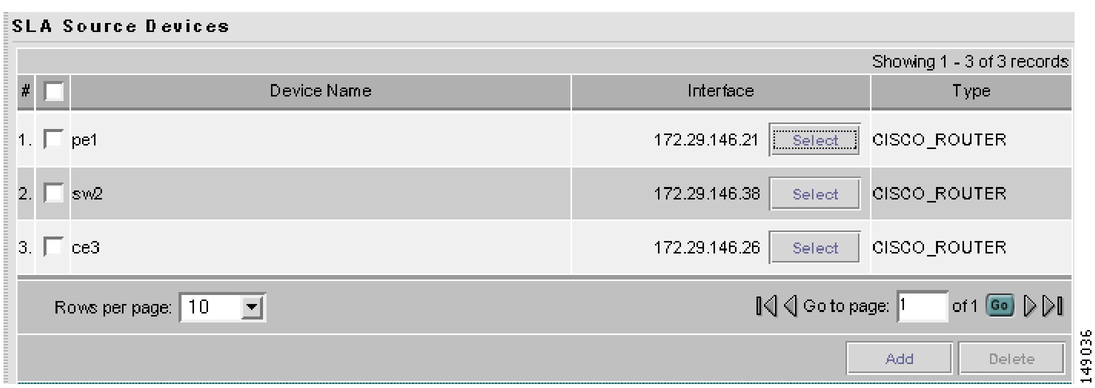
Create From Any SA Agent Device(s)

After you have completed the steps in Create Common Parameters, page 7-14, follow these steps:

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

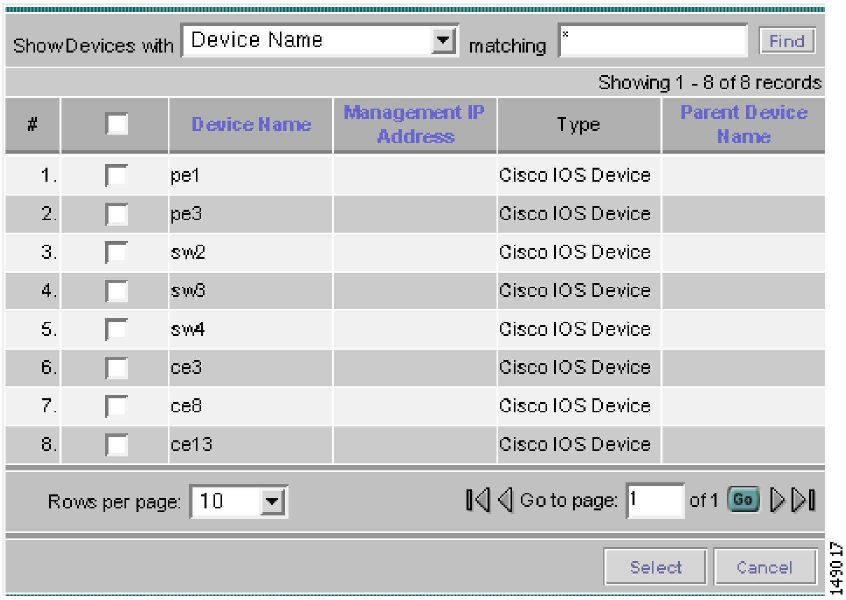
Step 1 The next window to appear is as shown in Figure 7-18, "SLA Source Devices."

Figure 7-18 SLA Source Devices



Step 2 Click the **Add** button and a window appears as shown in Figure 7-19, "SLA Devices > Add," which lists all the devices in the database that have a minimum of one interface. Check the check box next to each row for the device you want to select, then click **Select**.

Figure 7-19 SLA Devices > Add



You return to Figure 7-18 and the newly added source device(s) appear. The information about this source device is specified in the following columns:

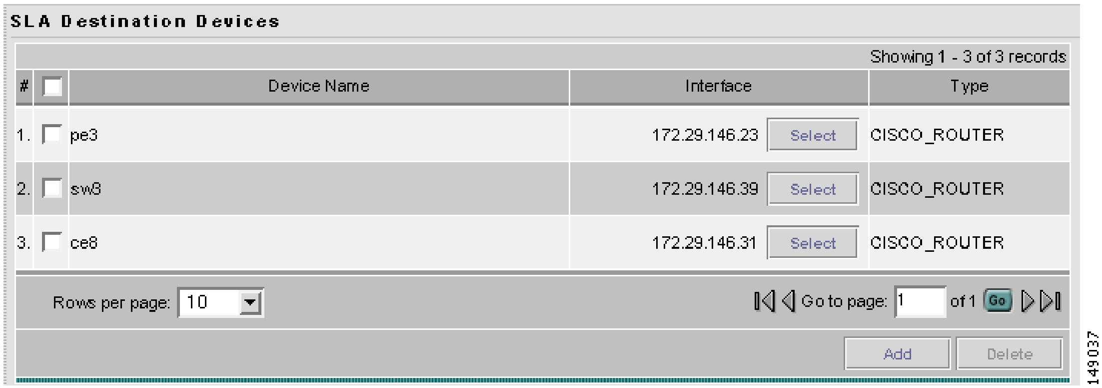
- **Device Name**—You can click this heading and the device names are organized alphabetically.
- **Interface**—You can click **Select** and from the resulting window, you can update the IP address. Select one radio button for an interface and click **Select** and the IP address changes in Figure 7-18.
- **Type**—Gives you the type of the source device.

Step 3 You can repeat Step 2 to to add more devices, or you can delete any of the currently selected source devices. To delete, check the check box next to each row for the device you want to delete and then click **Delete**.

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

Step 4 Click **Next**. The next window to appear is as shown in Figure 7-20, "SLA Destination Devices."

Figure 7-20 SLA Destination Devices



Step 5 Click the **Add** button and a window appears as shown in Figure 7-19, "SLA Devices > Add." Check the check box next to each row for the device you want to select. Then click **Select**.

Step 6 You return to Figure 7-20 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. Select one radio button for an interface and click **Select** and the IP address changes in Figure 7-20.
- **Type**—Gives you the type of the source device.

Step 7 You can repeat Step 5 to Step 6 to add more devices, or you can delete any of the currently selected destination devices. To delete, check the check box next to each row for the device you want to delete and then click **Delete**.

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

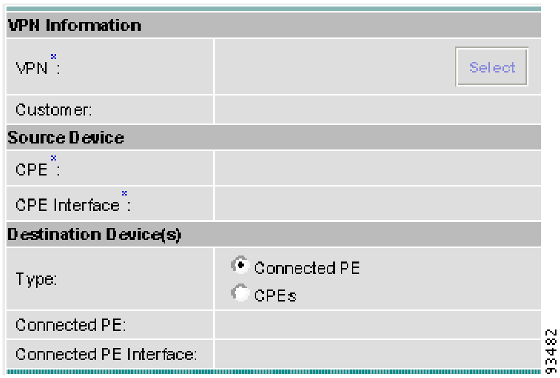
Step 8 Click **Next**. Proceed to the "Protocols" section on page 7-25."

Create from MPLS CPE

After you have completed the steps in Create Common Parameters, page 7-14, follow these steps:

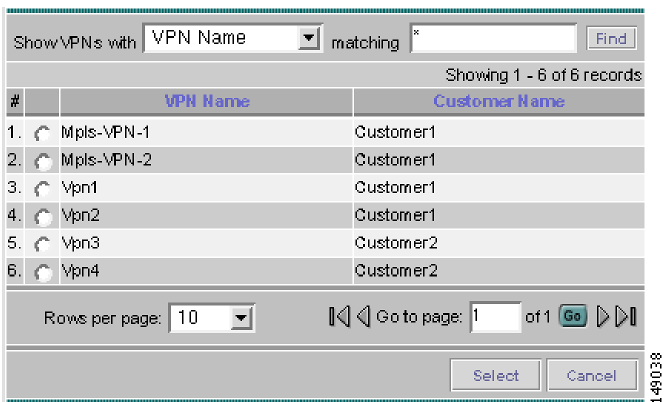
Step 1 Complete the steps in the "Create Common Parameters" section on page 7-14 and the next window to appear is as shown in Figure 7-21, "SLA CPE Parameters."

Figure 7-21 ***SLA CPE Parameters***



Step 2 Click the **Select** button for **VPN** and a window appears as shown in Figure 7-22, "Select VPN," which lists all the VPNs in the database.

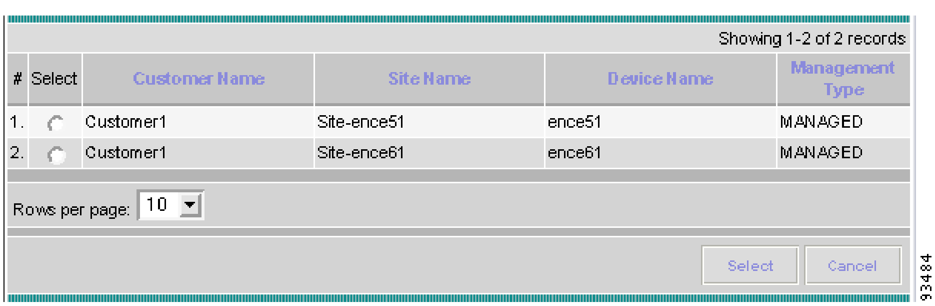
Figure 7-22 ***Select VPN***



Step 3 Click the radio button for the VPN you want to select. Then click **Select**. You return to Figure 7-21 and the newly added VPN and Customer information appear and a **Select** button appears for **CPE**. You can change the VPN by repeating Step 2.

Step 4 Click the **Select** button for **CPE** and a window appears as shown in Figure 7-23, "Select CPE," which lists the CPEs associated with the selected VPN. Click the radio button for the CPE you want to select. Then click **Select**.

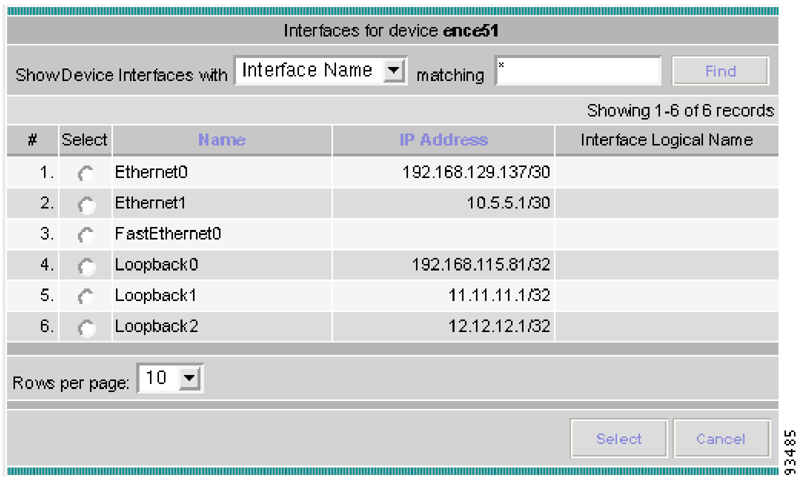
Figure 7-23 ***Select CPE***



Step 5 You return to Figure 7-21 and the newly added **CPE** and its first interface appear and a **Select** button appears for **CPE Interface**. You can change the CPE by repeating Step 4.

Step 6 If you want to change the default **CPE Interface** information that appears, click **Select** and you receive a window as shown in Figure 7-24, "Interfaces."

Figure 7-24 Interfaces



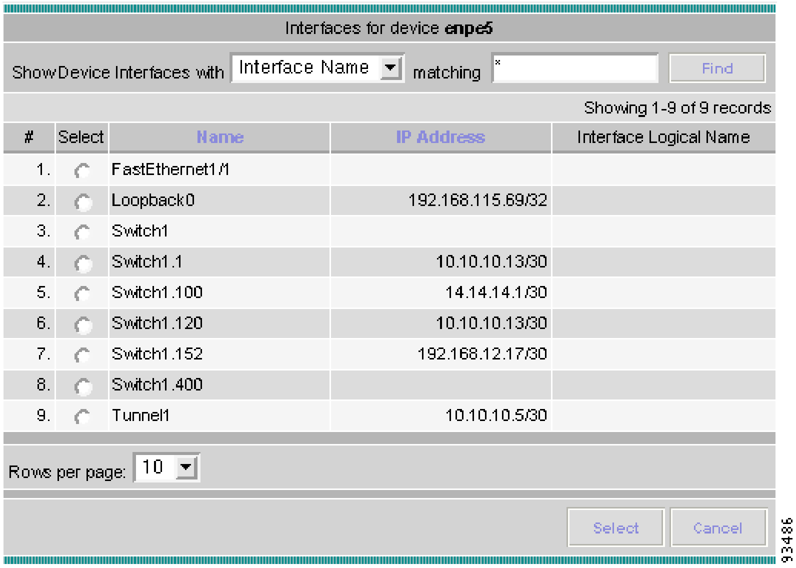
Step 7 Click the radio button next to the row for the interface you want to select. Then click **Select**. You return to Figure 7-21 and the newly added **CPE Interface** appears.

Step 8 You can change the CPE Interface by repeating Step 6.

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 7-25, "Connected PE Interface."

Figure 7-25 Connected PE Interface



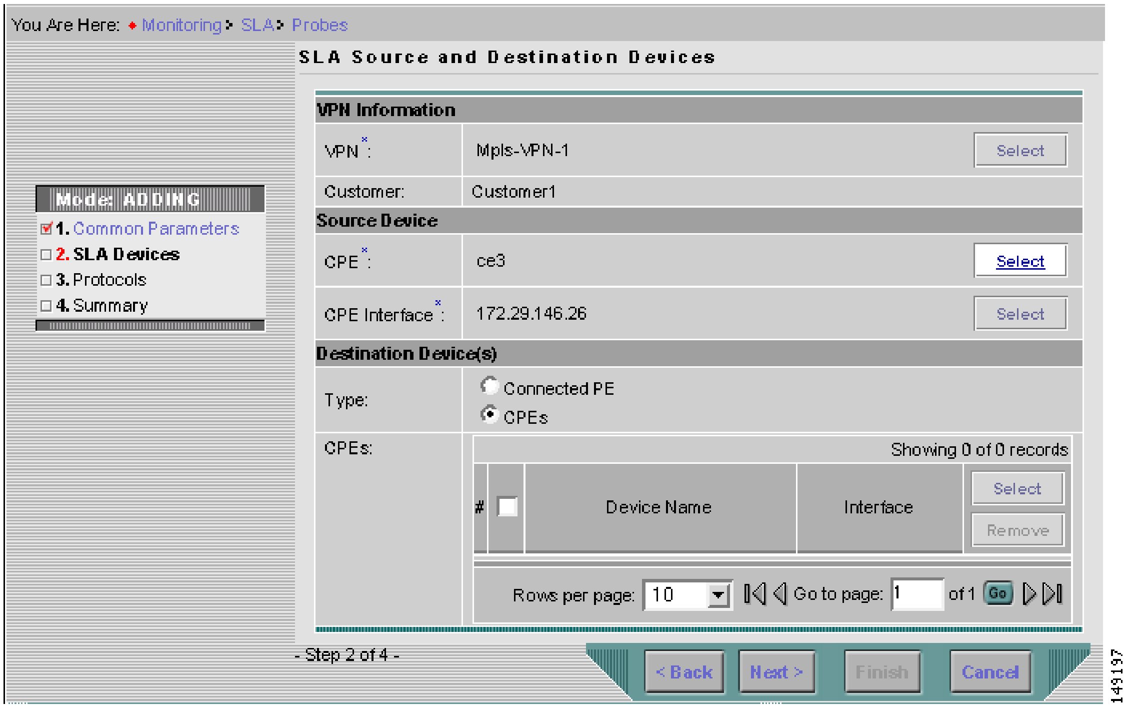
Click the radio button next to the row for the interface you want to select. Then click **Select**.

Step 11 You return to Figure 7-21 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 7-25.

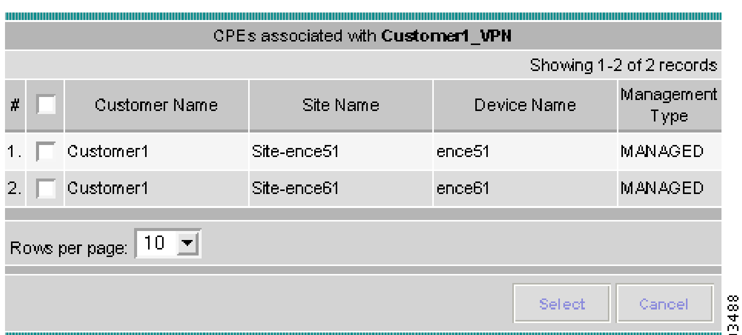
Step 13 When you click **CPEs**, the window is as shown in Figure 7-26, "CPEs."

Figure 7-26 CPEs



Step 14 Click the **Select** button for **CPEs** and a window appears as shown in Figure 7-27, "Select CPE Associated with the Specified VPN," which lists all the CPEs associated with the specified VPN in the database.

Figure 7-27 Select CPE Associated with the Specified VPN



Check the check box next to the row(s) for the CPE(s) you want to select. Then click **Select**.

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

You return to Figure 7-26 and the newly added **Device Name** appears.

Step 15 Click **Select** in the **Interface** column and a window appears as in Figure 7-24.

Step 16 Click the radio button next to the row for the CPE you want to select. Then click **Select**.

Step 17 You return to Figure 7-26 and the newly added **CPE Interface** appears. You can change the CPE Interface by repeating Step 15.

Step 18 Check the check box next to each row for the Devices you want to remove. Then click the **Remove** button and a window as shown in Figure 7-26 appears without the removed Device(s).

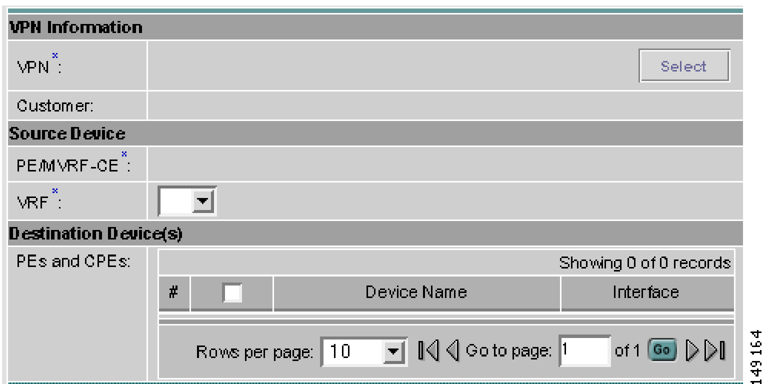
Step 19 When Figure 7-26 reflects what you want, click **Next** and proceed to the "Protocols" section on page 7-25.

Create From MPLS PE or MVRF-CE

After you have completed the steps in Create Common Parameters, page 7-14, follow these steps:

Step 1 Complete the steps in the "Create Common Parameters" section on page 7-14 and the next window to appear is as shown in Figure 7-28, "SLA Source and Destination Devices."

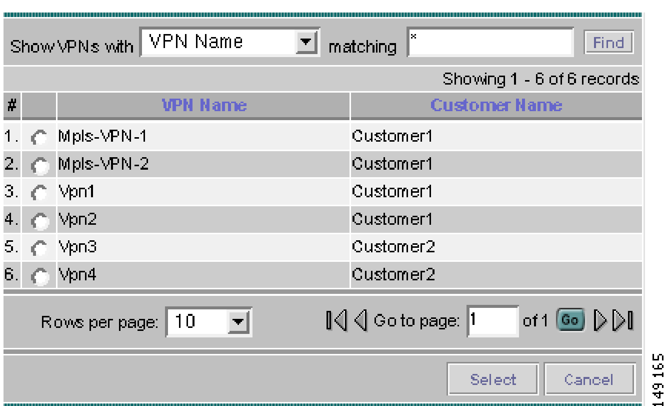
Figure 7-28 SLA Source and Destination Devices



Step 2 Click the **Select** button for **VPN** and a window appears as shown in Figure 7-29, "Select VPN," which lists all the VPNs in the database. Click the radio button next to the row for the VPN you want to select.

Step 3 Then click **Select**.

Figure 7-29 Select VPN



Step 4 You return to Figure 7-28 and the newly added VPN and Customer information appears. You can change the VPN and Customer by repeating Step 2.

Step 5 Click the new **Select** button for **PE/MVRF-CE** and you receive a drop-down list from which you can choose **PE** or **MVRF-CE**. If you choose **PE**, a window appears as shown in Figure 7-30, "Select PE," which lists all the PEs associated with the selected VPN. If you choose MVRF-CE, a window appears as shown in Figure 7-31, "Select CPE," which lists all the MVRF-CEs associated with the selected VPN. Click the radio button next to the row for the PE or MVRF-CE you want to select. Then click **Select** or **OK**.

Figure 7-30 Select PE

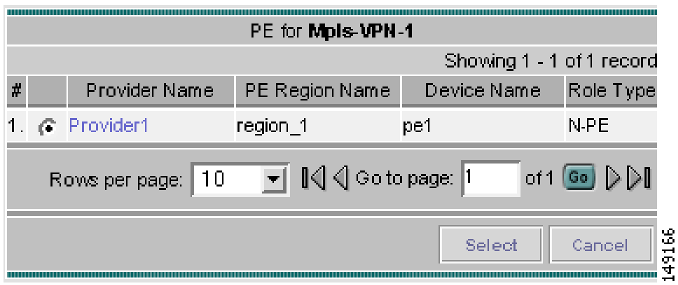
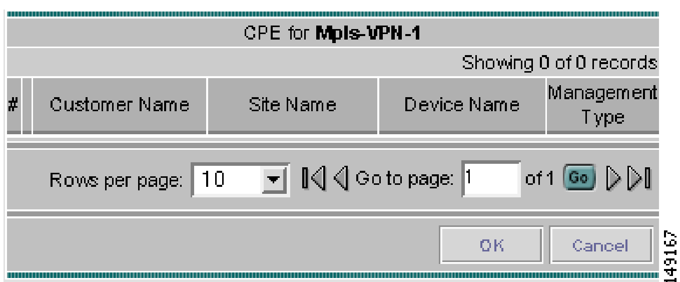


Figure 7-31 Select CPE



Step 6 You return to Figure 7-28 and the newly added PE or MVRF-CE information appears. You can change this selection by repeating Step 5.

Step 7 If in Step 5 you chose MVRF-CE information, you can click the **VRF** drop-down list.

Step 8 Click the new **Select** button for **Destination Device(s)—PEs and CPEs** and from a drop-down list, choose **PEs** or **CPEs**. If you choose **PEs**, a window appears as shown in Figure 7-32, "Select PEs," which lists all the PE Interfaces in the database. If you choose **CPEs**, a window appears as shown in Figure 7-33, "Select CPEs," which lists all the CPE Interfaces in the database. Click the radio button next to the row for the Device Interface you want to select. Then click **Select**.

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

Figure 7-32 ***Select PEs***

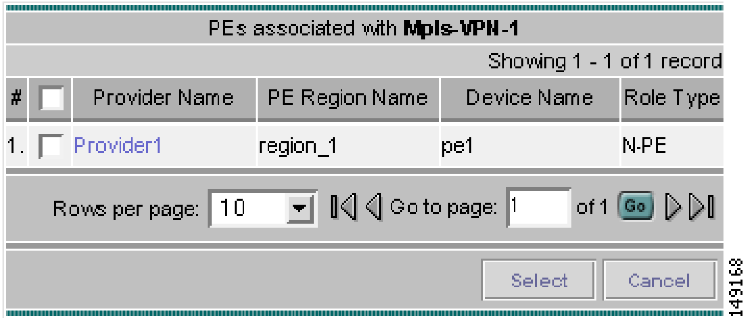
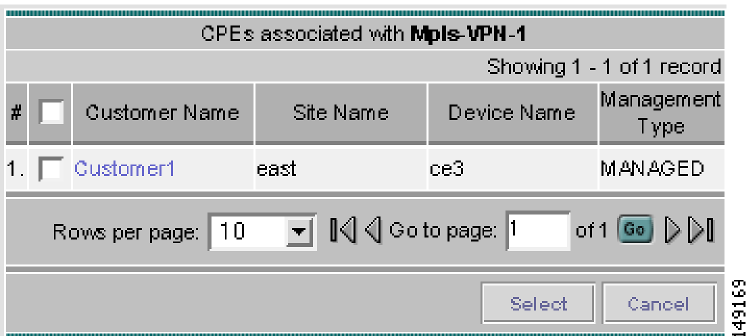


Figure 7-33 ***Select CPEs***



Step 9 You return to Figure 7-28 and you receive interface information. Click **Select** and you get a window from which you can click a radio button next to a different interface. Click **Select** and the new interface replaces the old interface. You can change the Interface by repeating this step.

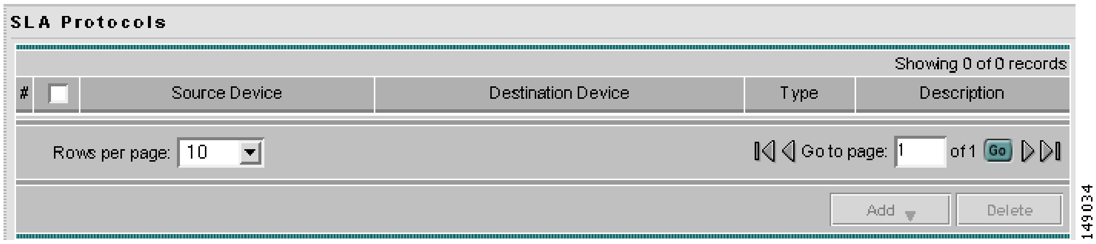
Step 10 Click **Next** and proceed to the "Protocols" section on page 7-25.

Protocols

You choose this location after you have completed all the steps in one of the **Creat**e functions: Create Common Parameters, page 7-14; Create from MPLS CPE, page 7-18; or Create From MPLS PE or MVRF-CE, page 7-23. Follow these steps:

Step 1 Complete the steps in the "Create Common Parameters" section on page 7-14 and the next window to appear is as shown in Figure 7-34, "Protocols."

Figure 7-34 Protocols

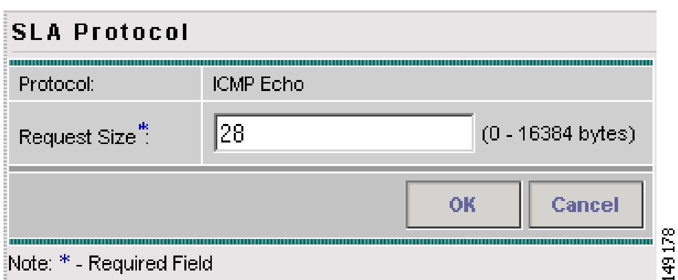


Step 2 Click the **Add** drop-down list and select:

- **ICMP Echo** (only available if destination devices are available)—Proceed to Step 3.
- **TCP Connect** (not available for Create From MPLS PE or MVRF-CE; 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 or MVRF-CE)—Proceed to Step 7.
- **DNS** (not available for Create from MPLS PE or MVRF-CE)—Proceed to Step 8.
- **HTTP** (not available for Create from MPLS PE or MVRF-CE)—Proceed to Step 9.
- **DHCP** (not available for Create from MPLS PE or MVRF-CE)—Proceed to Step 10.

Step 3 From Step 2, if you chose **ICMP Echo**, you receive a window as shown in Figure 7-35, "Protocol ICMP Echo."

Figure 7-35 Protocol ICMP Echo

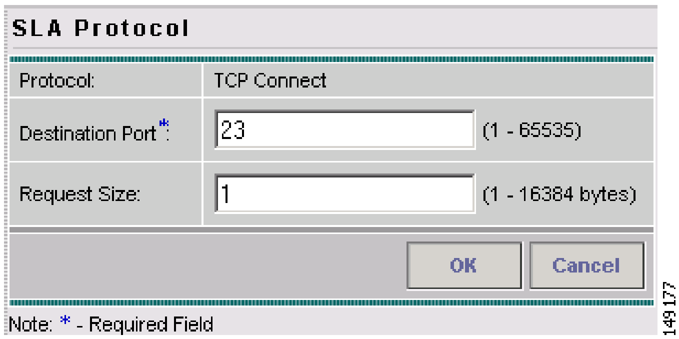


Enter the required information as follows, click **OK**, and then proceed to Step 11.

- Request Size (0 - 16384) (required)—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 7-36, "Protocol TCP Connect."

Figure 7-36 Protocol TCP Connect

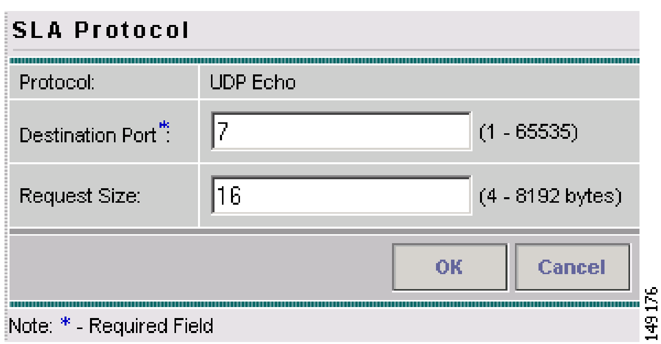


Enter the required and optional information as follows, click **OK**, and then proceed to Step 11.

- **Destination Port (1 - 65535)** (required)—Port number on the target where the monitoring packets is sent. If you do not specify a specific port, port **23** is used.
- **Request Size (1 - 16384)** (optional)—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 7-37, "Protocol UDP Echo."

Figure 7-37 Protocol UDP Echo

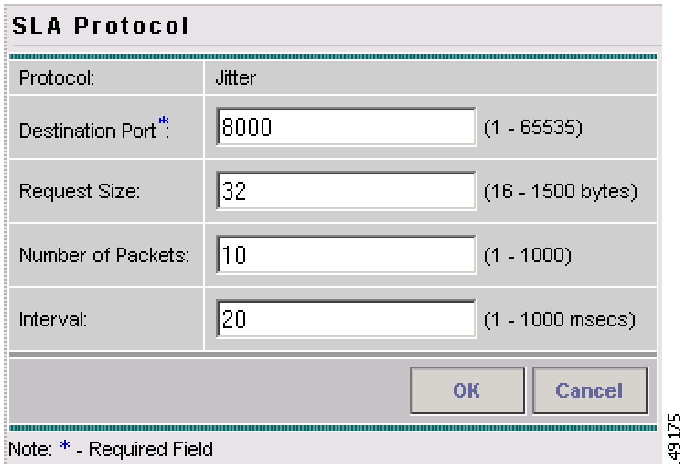


Enter the required and optional information as follows, click **OK**, and then proceed to Step 11.

- **Destination Port (1 - 65535) (required)**—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)—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 7-38, "Protocol Jitter."

Figure 7-38 Protocol Jitter

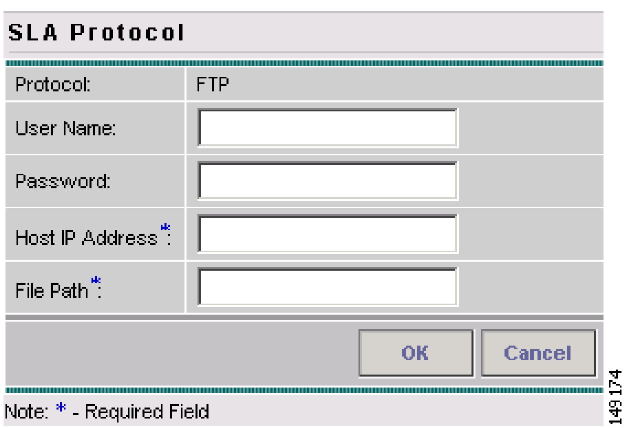


Enter the required and optional information as follows, click **OK**, and then proceed to Step 11.

- **Destination Port (1 - 65535)** (required)—Port number on the target where the monitoring packets are sent. If you do not specify a specific port, port **8000** is used.
- **Request Size (16 - 1500)** (optional)—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)—Integer that represents the number of packets that must be transmitted. The default value is **10**.
- **Interval (1 - 1000)** (optional)—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 7-39, "Protocol FTP."

Figure 7-39 Protocol FTP

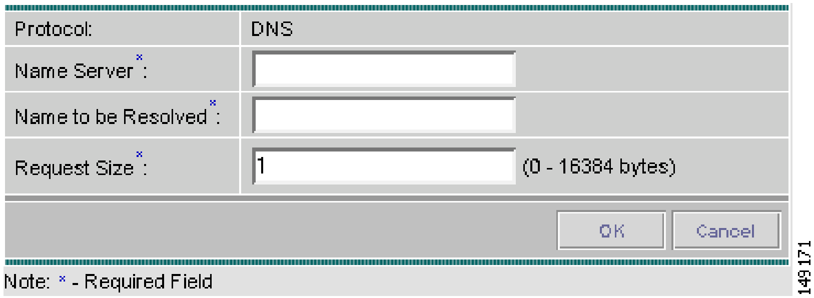


Enter the required and optional information as follows, click **OK**, and then proceed to Step 11.

- **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 7-40, "Protocol DNS."

Figure 7-40 Protocol DNS

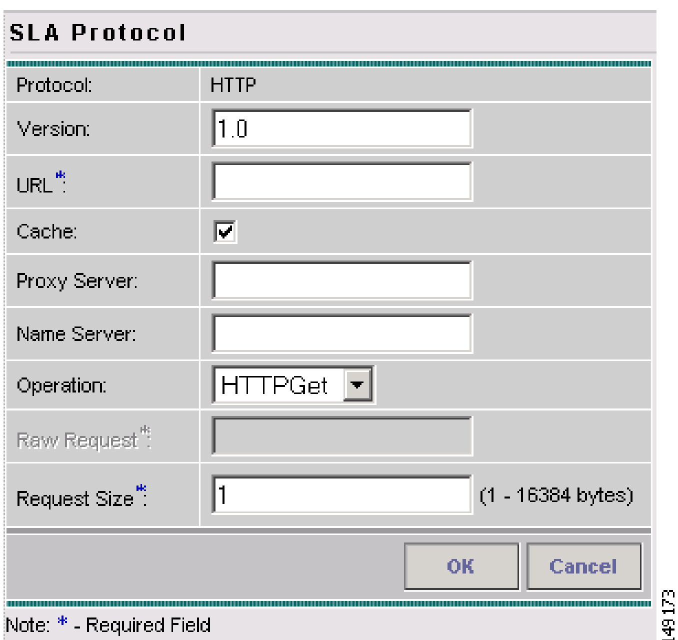


Enter the required information as follows, click **OK**, and then proceed to Step 11.

- **Name Server** (required)—String that specifies the IP address of the name server. The address is in dotted IP address format.
- **Name to be Resolved** (required)—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)—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 7-41, "Protocol HTTP."

Figure 7-41 Protocol HTTP



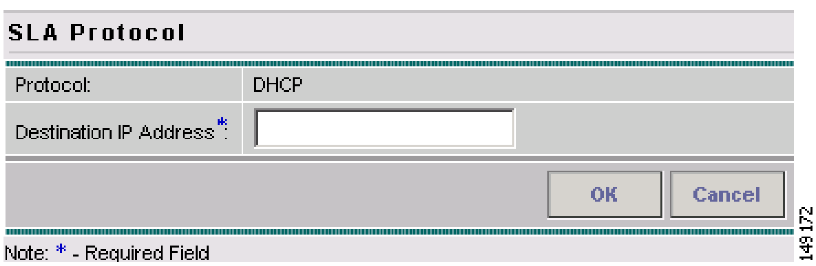
Enter the optional and required information as follows, click **OK**, and then proceed to Step 11.

- **Version** (default: 1.0)—String that specifies the version of the HTTP server. Do not change this. ISC only supports version 1.0.

- **URL** (required)—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 an unchecked check box, the HTTP request should not download cached pages. For a checked check box, the HTTP request downloads cached pages if available, otherwise the request is forwarded to the HTTP server.
- **Proxy Server** (optional)—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)—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 list and make that choice.
- **Raw Request** (required if the **Operation** is **HTTPRaw**; not available if the **Operation** is **HTTPGet**)—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)—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 receive a window as shown in Figure 7-42, "Protocol DHCP."

Figure 7-42 Protocol DHCP



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

- **Destination IP Address** (required)

Step 11 You return to Figure 7-34 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.

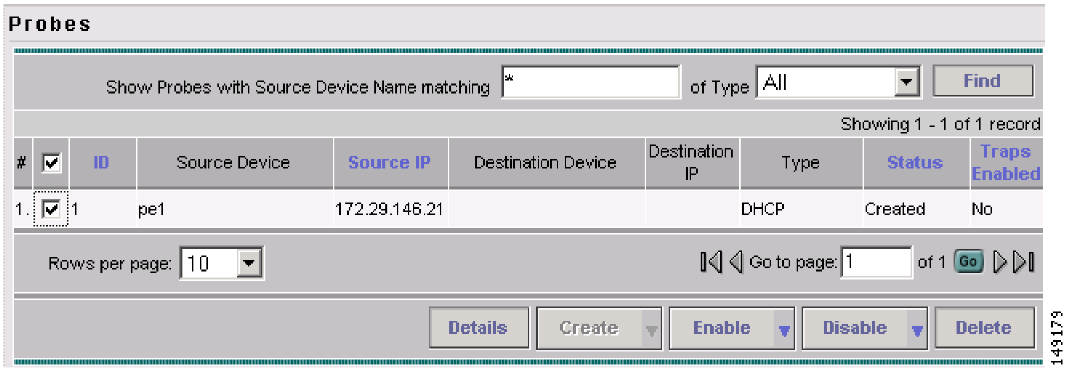
Step 12 The next window to appear is a Probe Creation Task Summary window that shows the **Description** (date and time created), **Common Parameters**, **Source Devices**, **Destination Devices**, and **Protocols** that you have defined. If all exists the way you want it, click **Finish**. Otherwise,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

Details

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

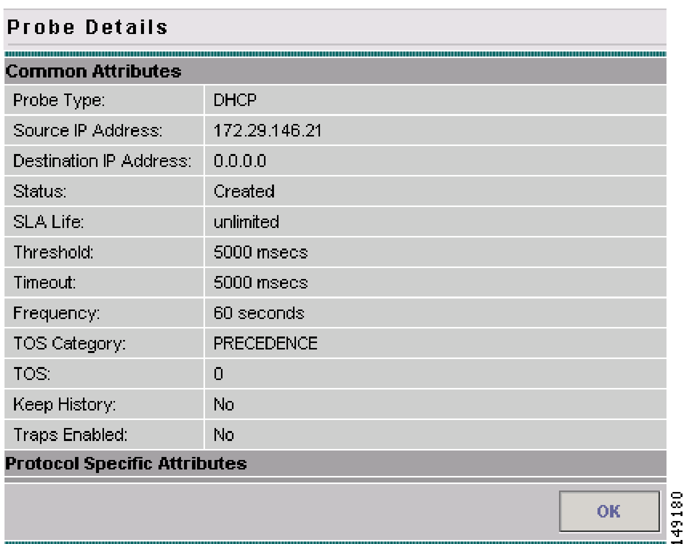
Step 1 Select an existing probe by checking the corresponding check box for which you want details. Then you have access to the **Details** button, as shown in Figure 7-43, "SLA Probes > Details."

Figure 7-43 SLA Probes > Details



Step 2 After you click the **Details** button, you receive a window as shown in Figure 7-44, "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 7-44 SLA Probes Details



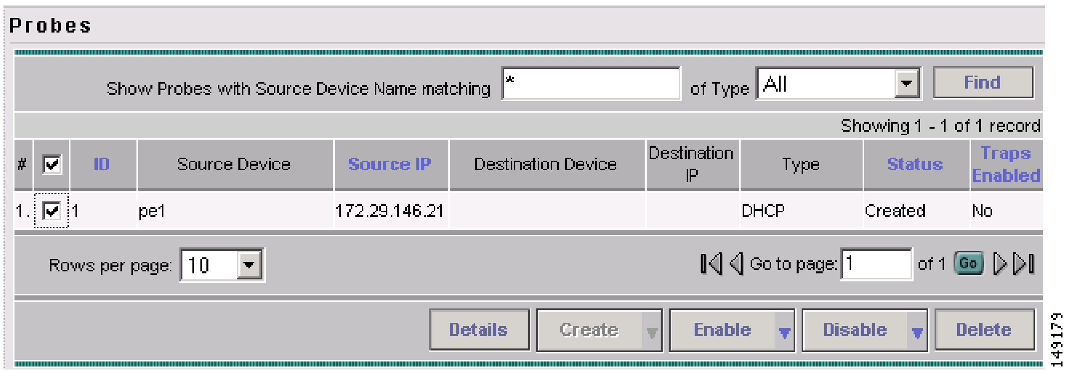
Step 3 Click **OK** to return to a window as shown in Figure 7-43. You can continue to select more **Details** or complete another function.

Delete

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

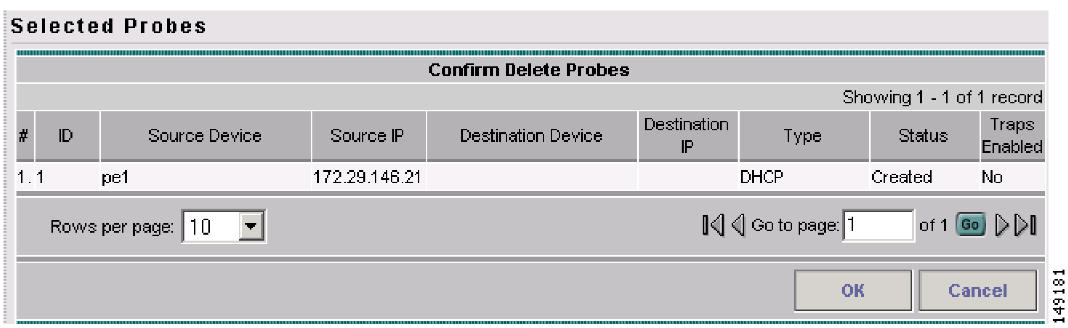
Step 1 Select one or more existing probes by checking the check box(es) for the row(s) of existing probe(s). Then you have access to the **Delete** button, as shown in Figure 7-45, "SLA Probes > Delete."

Figure 7-45 SLA Probes > Delete



Step 2 After you click the **Delete** button, a window as shown in Figure 7-46, "Confirm Delete Probes," appears.

Figure 7-46 Confirm Delete Probes



Step 3 Click **OK** if Figure 7-46 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.

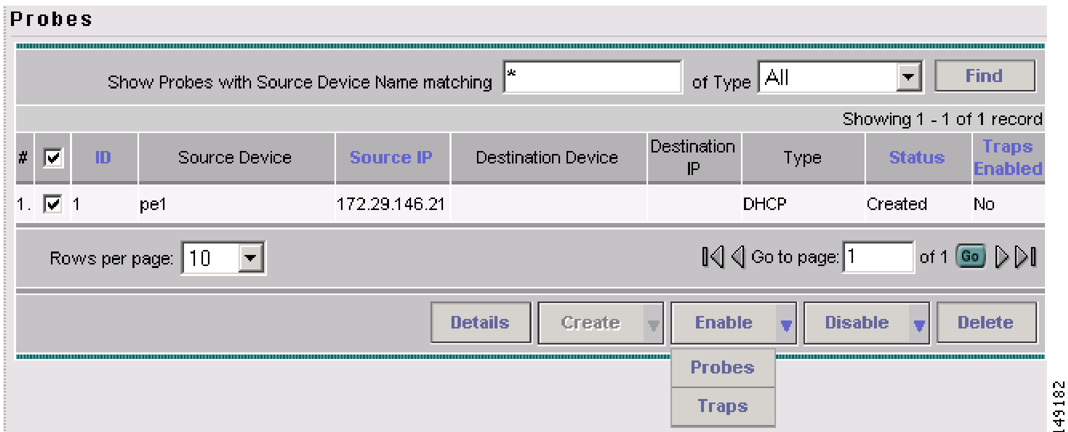
Step 4 You return to Figure 7-45 with updated information.

Enable Probes

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

Step 1 Select one or more existing probes by checking the check box(es) for the row(s) of existing probe(s). Then you have access to the **Enable** button. From the **Enable** drop-down list, you have access to **Probes**, as shown in Figure 7-47, "SLA Probes > Enable > Probes."

Figure 7-47 SLA Probes > Enable > Probes



Step 2 After you choose **Enable > Probes,** a window as shown in Figure 7-48, "Confirm Enable Probes," appears.

Figure 7-48 Confirm Enable Probes

Step 3 Click **OK** if Figure 7-48 reflects the probes you want to enable or click **Cancel** if it does not. In both cases, you return to Figure 7-47.

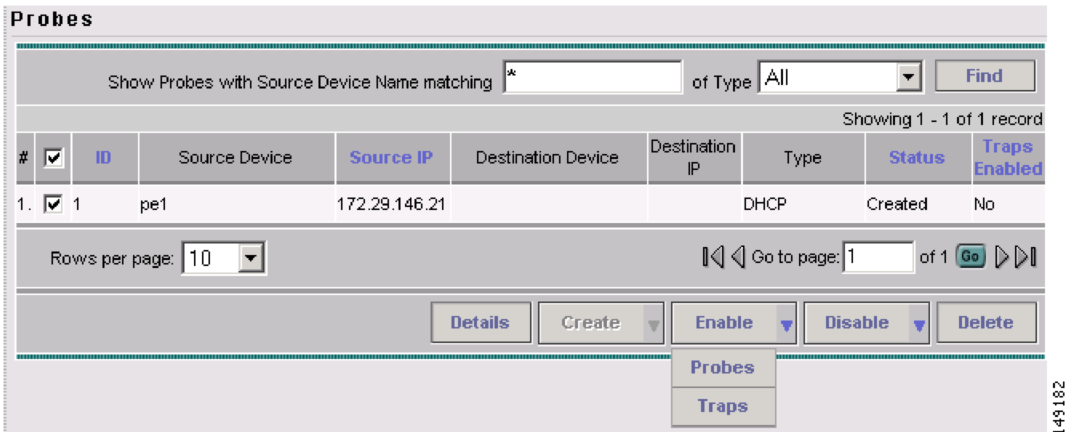
Step 4 If this was successful, you receive a Status window with a green check mark for **Succeeded**. The Status column is set to **Active** when the probe is created successfully on the router.

Enable Traps

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

Step 1 Select one or more existing probes by checking the check box(es) for the row(s) of existing probe(s). Then you have access to the **Enable** button. From the **Enable** drop-down list, you have access to **Traps**, as shown in Figure 7-49, "SLA Probes > Enable > Traps."

Figure 7-49 SLA Probes > Enable > Traps



Step 2 After you choose **Enable > Traps**, a window as shown in Figure 7-50, "Confirm Enable Traps," appears. All the traps have 3000 ms as the falling threshold set automatically

Figure 7-50 Confirm Enable Traps

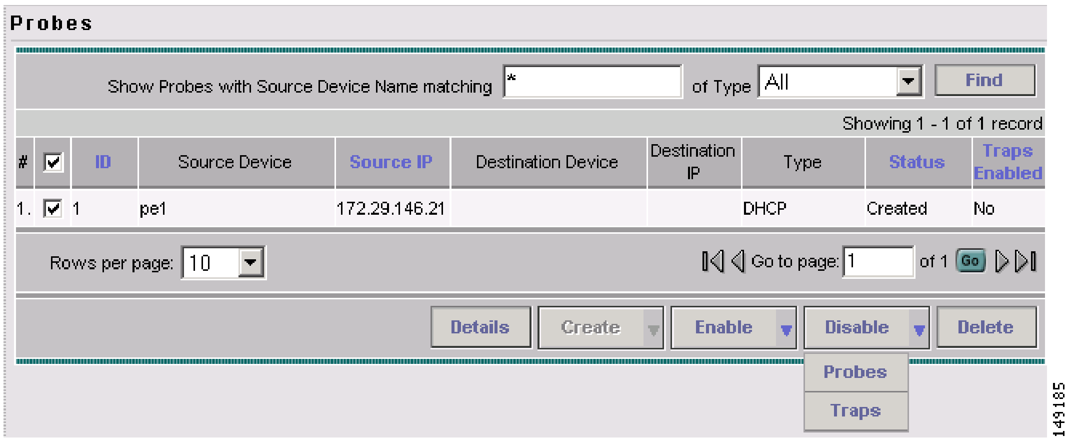
Step 3 Click **OK** if Figure 7-50 reflects the traps you want to enable or click **Cancel** if it does not. In both cases you return to Figure 7-49. If this was successful, you receive a Status window with a green check mark for **Succeeded**. The Traps Enabled column is set to **yes** when the probes on the router are successfully changed.

Disable Probes

When you choose **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 checking the check box(es) for the row(s) of existing probe(s). Then you have access to the **Disable** button. From the **Disable** drop-down list, you have access to **Probes**, as shown in Figure 7-51, "SLA Probes > Disable > Probes."

Figure 7-51 SLA Probes > Disable > Probes



Step 2 After you choose **Disable > Probes,** a window as shown in Figure 7-52, "Confirm Disable Probes," appears.

Figure 7-52 Confirm Disable Probes

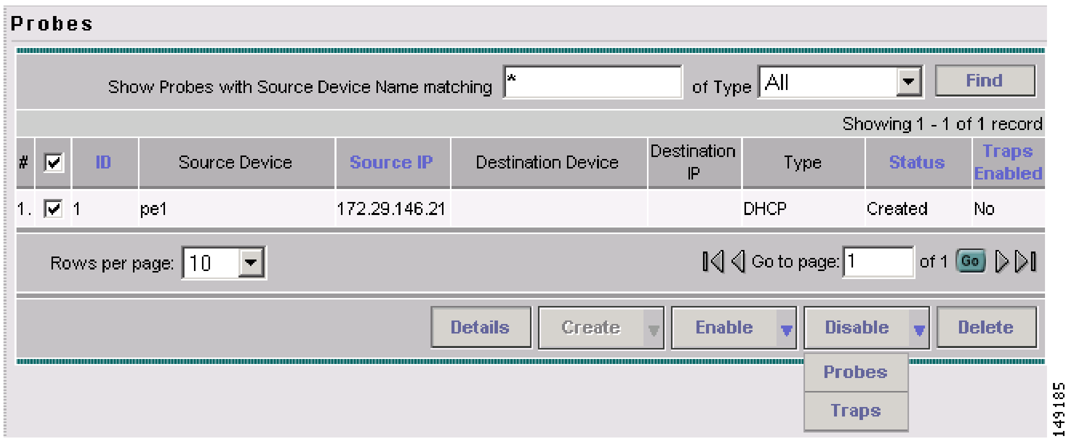
Step 3 Click **OK** if Figure 7-52 reflects the probes you want to disable or click **Cancel** if it does not. In both cases you return to Figure 7-51. If this was successful, you receive a Status window with a green check mark for **Succeeded**, and the probe's status becomes Disabled when the probe on the router is successfully removed.

Disable Traps

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

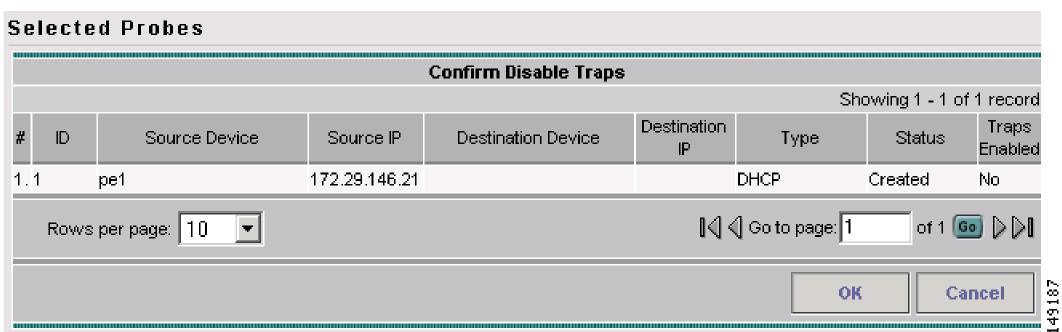
Step 1 Select one or more existing probes by checking the check box(es) for the row(s) of existing probe(s). Then you have access to the **Disable** button. From the **Disable** drop-down list, you have access to **Traps**, as shown in Figure 7-53, "SLA Probes > Disable > Traps."

Figure 7-53 SLA Probes > Disable > Traps



Step 2 After you choose **Disable > Traps,** a window as shown in Figure 7-54, "Confirm Disable Traps," appears.

Figure 7-54 Confirm Disable Traps

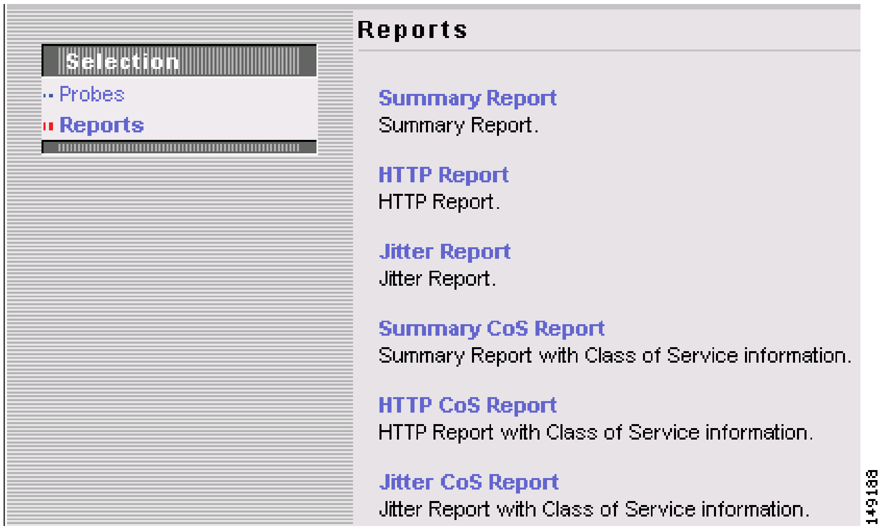


Step 3 Click **OK** if Figure 7-54 reflects the traps you want to disable or click **Cancel** if it does not. In both cases you return to Figure 7-53. If this was successful, you receive a Status window with a green check mark for **Succeeded**. The traps are disabled when the probes on the router are successfully changed.

Reports

When you choose **Monitoring > SLA > Reports**, you receive a window as shown in Figure 7-55, "SLA Reports."

Figure 7-55 SLA Reports



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

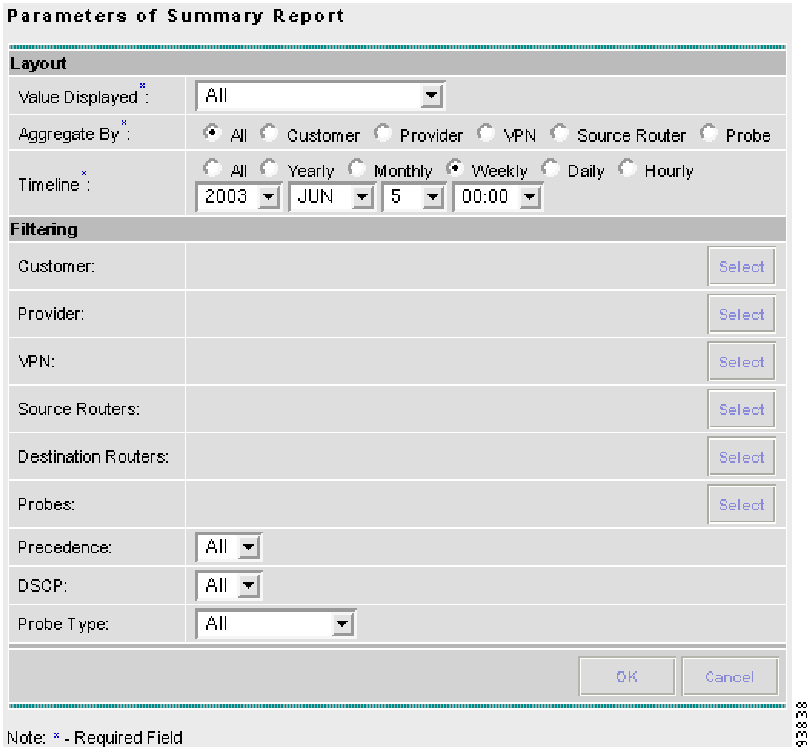
- Summary Report, page 7-37—This report summarizes all the information other than for HTTP and Jitter (ICMP Echo, TCP Connect, UDP Echo, FTP, DNS, and DHCP).
- HTTP Report, page 7-40—This is a summary report for HTTP information.
- Jitter Report, page 7-40—This is a summary report for Jitter information.
- Summary CoS Report, page 7-41—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 7-42—This report is for HTTP CoS information.
- Jitter CoS Report, page 7-42—This report is for Jitter CoS information.

Summary Report

From Figure 7-55, choose **Summary Report** and follow these steps:

Step 1 Choose **Summary Report,** and the resulting window is shown in Figure 7-56, "Parameters of Summary Report."

Figure 7-56 ***Parameters of Summary Report***



Step 2 For Figure 7-56, fill in the **Layout** fields, as follows:

- **Value Displayed** (required) (default: **All**) Click the drop-down list and choose 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 lists for the year, month, day of the month, and time of day for which to start the report.

Step 3 For Figure 7-56, 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 7-56 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 7-56 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 7-56 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, check the check box(es) for device(s). Then click **Select**. The result is that you return to Figure 7-56 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, check the check box(es) for device(s). Then click **Select**. The result is that you return to Figure 7-56 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, check the check box(es) for source probe(s). Then click **Select**. The result is that you return to Figure 7-56 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 list 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 choose a ToS value of 5, then choose 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 list 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.

- **Probe Type** (default: **All**)—Click the drop-down list 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 7-25.

Step 4 Click **OK** in Figure 7-56 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 7-56 in which you can modify your selections as explained in the previous steps.

HTTP Report

From Figure 7-55, choose **HTTP Report** and proceed similarly to the "Summary Report" section on page 7-37, with the following exceptions:

- **Value Displayed** has different drop-down choices.
- There is no **Destination Routers** selection.
- There is no **Probe Type** drop-down list in the equivalent of Figure 7-56, because the probe type is automatically **HTTP**. The result is an HTTP Report.

Jitter Report

From Figure 7-55, choose **Jitter Report** and proceed similarly to the "Summary Report" section on page 7-37, with the following exceptions:

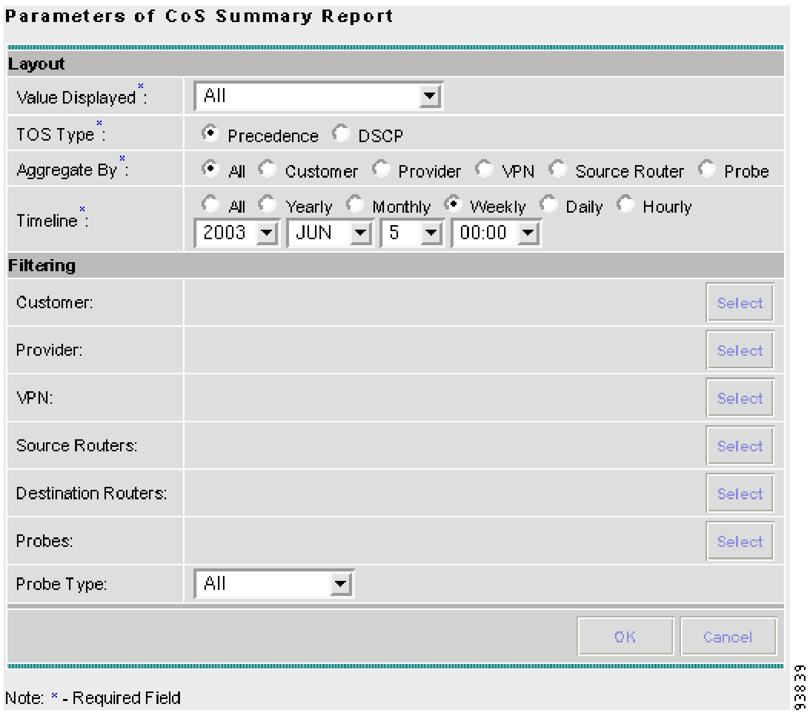
- **Value Displayed** has different drop-down choices.
- There is no **Destination Routers** selection.
- There is no **Probe Type** drop-down list in the equivalent of Figure 7-56, because the probe type is automatically **Jitter**. The result is a Jitter Report.

Summary CoS Report

From Figure 7-55, choose **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 follow these steps:

Step 1 Choose **Summary CoS Report**, and the resulting window is shown in Figure 7-57, "Parameters of CoS Summary Report."

Figure 7-57 Parameters of CoS Summary Report



Step 2 For Figure 7-57, fill in the **Layout** fields, as shown in Step 2 of the "Summary Report" section on page 7-37, 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 7-37.

Step 3 For Figure 7-57, fill in the **Filtering** fields, as shown in Step 3 of the "Summary Report" section on page 7-37, with the exception that there are no **Precedence** or **DSCP** drop-down lists. They are now in the **Layout** fields, as explained in Step 2 in this section.

Step 4 Click **OK** in Figure 7-57 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 7-57 in which you can modify your selections as explained in the previous steps.

HTTP CoS Report

From Figure 7-55, choose **HTTP Report** and proceed exactly as in the "Summary CoS Report" section on page 7-41, with the following exceptions:

- **Value Displayed** has the same drop-down choices as **HTTP Report**.
- There is no **Destination Routers** selection.
- There is no **Probe Type** drop-down list in the equivalent of Figure 7-57, because the probe type is automatically **HTTP CoS**. The result is a CoS HTTP Report. This CoS HTTP report is based on the TOS values of the SLA probes.

Jitter CoS Report

From Figure 7-55, choose **Jitter Report** and proceed exactly as in the "Summary CoS Report" section on page 7-41, with he following exceptions:

- **Value Displayed** has the same drop-down choices as **Jitter Report**.
- There is no **Destination Routers** selection.
- There is no **Probe Type** drop-down list in the equivalent of Figure 7-57, because the probe type is automatically **Jitter CoS**. The result is a CoS Jitter Report. This CoS Jitter report is based on the TOS values of the SLA probes.

TE Performance Report

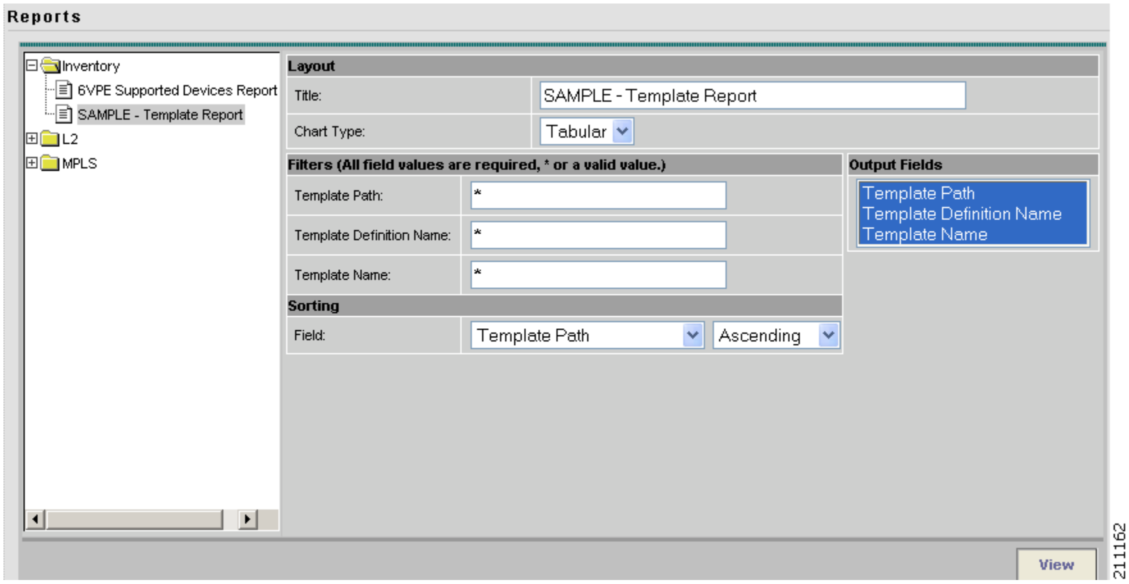
TE Performance Report for Traffic Engineering Management is explained in detail in the *Cisco IP Solution Center Traffic Engineering Management User Guide, 5.1.*

Reports

When you choose **Monitoring > Reports**, a tree of reports appears in the data pane. Click on the **+** sign for each folder in the data pane and you receive a listing of all the provided reports. The non-SAMPLE reports in the L2VPN folder are explained in the *Cisco MPLS Diagnostics Expert 2.1.3 Failure Scenarios Guide on ISC 5.1* and the non-SAMPLE reports in the MPLS folder are explained in the *Cisco IP Solution Center MPLS VPN User Guide, 5.1*.

Click on any of the specific reports and you can define how to set up the report. Figure 7-58, "Inventory > SAMPLE - Template Report - Report Window," shows the sample file under the folder **Inventory**.

Figure 7-58 Inventory > SAMPLE - Template Report - Report Window



This section explains the Reports feature and how to use it in the following areas:

- Introducing Reports, page 7-43
- Accessing Reports, page 7-44
- Using Reports GUI, page 7-44
- Running Reports, page 7-45
- Using the Output from Reports, page 7-46
- Creating Custom Reports, page 7-48

Introducing Reports

Network operators often want to have detailed reports on the services provisioned. For example, for a given customer, you might want to see a list of the PE-CE connections and their detailed PE-CE configuration parameters or you might want to see specific Layer2 or Layer3 service requests on a PE. These reports help network operators by providing a centralized location for finding Service Requests (SRs) and VPN information.

When you choose **Monitoring > Reports**, reports are grouped by type to allow for easy navigation. ISC displays only predefined (canned) reports for which the user has RBAC permission.

You can select the filtering criteria and the outputs to be displayed in the report. You can save reports to a variety of formats.

In addition to the predefined reports that are documented in the *Cisco IP Solution Center Carrier Ethernet and L2VPN User Guide, 5.1* and the *Cisco IP Solution Center MPLS VPN User Guide, 5.1*, ISC provides additional sample reports. Sample reports are provided for informational purposes only and are untested and unsupported.

The data structures that ISC uses to provide reports in the GUI are defined in an XML format.

Accessing Reports

To access the reports, follow these steps:

Step 1 To access the reports framework in the ISC GUI, choose **Monitoring > Reports**.

Step 2 Click on the folders to display the available reports.

The Reports window appears, as shown in Figure 7-58.

Step 3 From the reports listed under one of the folders in the left navigation tree, click on the desired report to bring up the window associated with that report.

Note Several sample reports are provided in the each of the reports folders. These reports begin with the title **SAMPLE-**. These reports are provided for informational purposes only. They are untested and unsupported. You might want to use them, along with the supported reports, as a basis for creating your own custom reports. See the "Creating Custom Reports" section on page 7-48 for information about custom reports.

Using Reports GUI

This section provides some general comments on using the reports GUI. This information applies to all reports. When you invoke a report, you see a window like the one shown in Figure 7-58.

The window is divided into several areas:

Layout

This area displays the title of the report and allows you to select the chart type. You can enter your own report title by overwriting the Title field.

Note Only tabular output is supported.

Filters

In this pane you can define inputs or search criteria for the reports. Values entered here are compared against corresponding values associated with data objects in the ISC repository. Values must be entered for all fields. An asterisk (*) can be used as a wild-card character for an entire string.

For each filterable field, the GUI displays a label and a text input field. For certain fields, the GUI also displays a Select button that allows you to choose an existing object (for example, customer, Service Type, SR State, and so on). All available output fields are displayed in the window, allowing you to select the fields to include in the report. All output fields are selected by default.

Note Filter values must be in the same format as the values represented within ISC. For example, a Service Request (SR) ID must be a number.

Output Fields

In this pane you can choose output fields to be displayed in the report. You can choose any or all of the output fields by selecting them with the mouse. Use the Shift key to select a continuous range of output values. Or, use the Control key to select random output values.

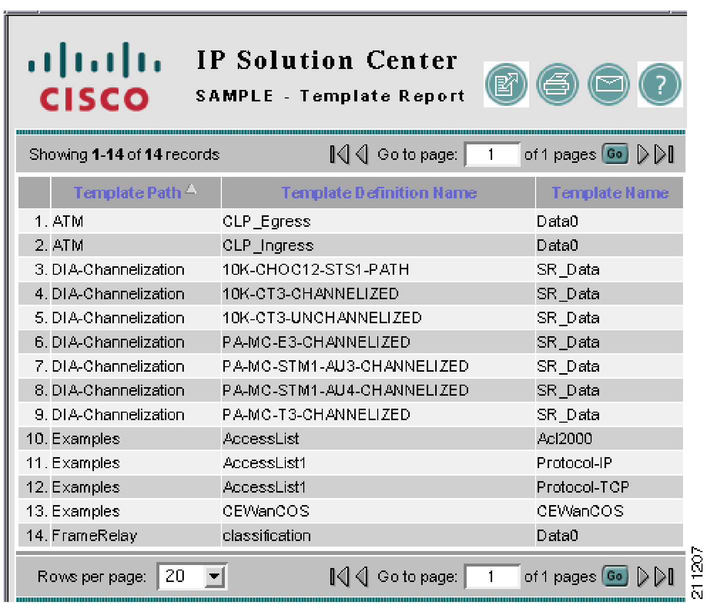
Sorting

This pane allows you to select how you want to sort the report output. For Field:, use the first drop-down list to select each filter field and then the second drop-down list to choose whether to display the report fields in ascending or descending order. The sort order can also be changed after you have the report output displayed (see Figure 7-59).

Running Reports

To run the report, click **View** in the lower right corner of the report window. This generates the report output. An example of a report output is shown in Figure 7-59.

Figure 7-59 Report Output



The reports GUI supports output in tabular format. The output is listed in columns, which are derived form the outputs you selected in the reports window.

Each row (or record) represents one match of the search criteria you set using the filter fields in the reports window.

In some cases, the value returned in a field can be displayed as one of the following:

- **-1** means no information updated for this field
- **F** means false
- **T** means true

The column heading with a triangle icon is the output by which the records are sorted. By clicking on any column heading, you can toggle between ascending and descending sort order. To sort on another output value, click on the heading for that value.

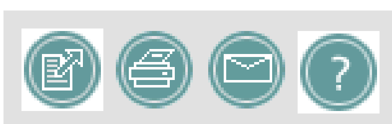
For information on working with report output, see the "Using the Output from Reports" section on page 7-46.

Using the Output from Reports

The icons at the upper right of the report output window (see Figure 7-60) provide the following functions, respectively, moving from left to right:

- Export explained in the "Exporting Reports" section on page 7-47
- Print explained in the "Printing Reports" section on page 7-47
- E-mail explained in the "E-mailing Reports" section on page 7-47
- Link to web-based product documentation explained in the "Invoking Help" section on page 7-48

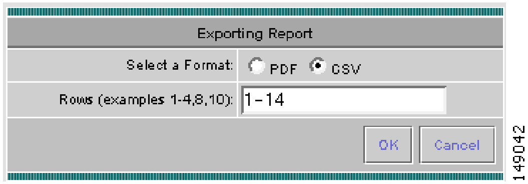
Figure 7-60 Report Output Icons



Exporting Reports

Click on the **Export** icon in Figure 7-60, "Report Output Icons," to bring up a window like the one shown in Figure 7-61 and then follow these steps.

Figure 7-61 Exporting Report Window



Step 1 Select the appropriate radio button for the format you want:

- **PDF** file—Adobe's portable document format.
- **CSV** file—Comma Separated Values format that allows for the data to be easily exported into a variety of applications.

Step 2 Select the rows you would like to save, then click **OK**.

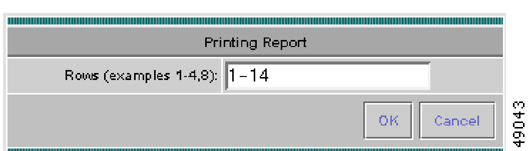
ISC generates the report in the format you selected.

> **Note** You must have the appropriate application on your system (for example, Acrobat Reader or Excel) to view and save the output.

Printing Reports

Click on the **Print** icon in Figure 7-60, "Report Output Icons," to bring up a window like the one shown in Figure 7-62.

Figure 7-62 Print Report

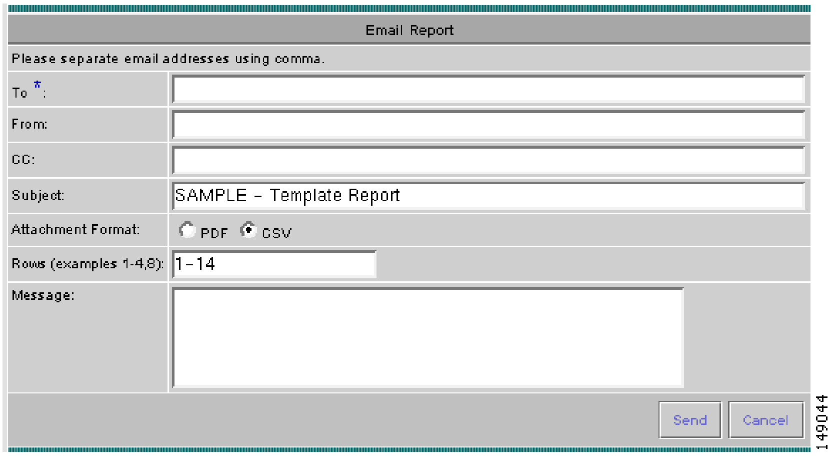


This window allows you to display the report in a form more appropriate for printing. Select the desired rows, then click **OK**. The results are displayed in your web browser, from which you can print the report.

E-mailing Reports

Click on the **E-mail** icon in Figure 7-60, "Report Output Icons," to bring up a window like the one shown in Figure 7-63 and then follow these steps.

Figure 7-63 E-mail Report



Step 1 In the To: field (required), specify one or more e-mail addresses to which the report should be sent.

Step 2 In the From: field (optional), enter an e-mail address you want to appear in the message header.

This allows a reply message to be sent to a valid e-mail address.

Step 3 In the CC: field (optional), enter e-mail addresses for recipients you want to receive copies of this report.

Step 4 The subject field shows the title of the report being sent.

You can overwrite this field to rename the report. This is what appears in the Subject field of the e-mail message.

Step 5 Select the radio button for the output format (PDF or CSV) in which you want the report sent.

Step 6 Select the number of rows you want sent.

Step 7 If applicable, in the Message field, write a message to announce the report, then click **Send**.

Invoking Help

Click on the **Help** (**?**) icon in Figure 7-60, "Report Output Icons," to link to the ISC documentation set on the Cisco Systems web site:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/tsd_products_support_series_home.html

From that location, you can choose the type of ISC document you want to see.

Creating Custom Reports

The reports listed in the ISC GUI in the each folder are derived from an underlying configuration file. The file is in XML format. You can access the file in the following location:

$ISC_HOME/resources/nbi/reports/ISC/<*folder_name*>**_report.xml**

where <*folder_name*> *is* **Inventory**, **L2**, *or* **MPLS**.

Each of the available reports (including sample reports) is defined by XML content contained within an <objectDef name> start and end tag under **packageDef name = "**<*folder_name*>**"**. The intervening XML content specifies the title of the report, all allowable filter parameters, outputs, and the default sorting behavior. You can modify existing reports or copy them to use as templates for new reports.

To do this, follow these steps:

Step 1 Stop the ISC server using the **stopall** command. See Chapter 2, "WatchDog Commands" for information on starting and stopping ISC.

Step 2 Open the **$ISC_HOME/resources/nbi/reports/ISC/**<*folder_name*>**_report.xml (where:** <*folder_name*> *is* **Inventory**, **L2**, *or* **MPLS**) configuration file using an editing tool of your choice.

Note You should backup the file before making any changes to it.

Step 3 Depending on your needs, either modify an existing report or copy one and use it as the basis for a new one.

Step 4 Save the modified **$ISC_HOME/resources/nbi/reports/ISC/**<*folder_name*>**_report.xml** file.

Step 5 Restart the ISC server using the **startwd** command. See Chapter 2, "WatchDog Commands" for information on starting and stopping ISC.

After restarting ISC, the modifications take effect, based on changes you made to the **$ISC_HOME/resources/nbi/reports/ISC/**<*folder_name*>**_report.xml** file.