Administration

A number of administrative features in Cisco IP Solution Center Traffic Engineering Management (ISC TEM) are common to ISC. Instructions on how to use these features are described in detail in *Cisco IP Solution Center Infrastructure Reference, 4.0*.

In this chapter, only TE-specific administrative features are described.

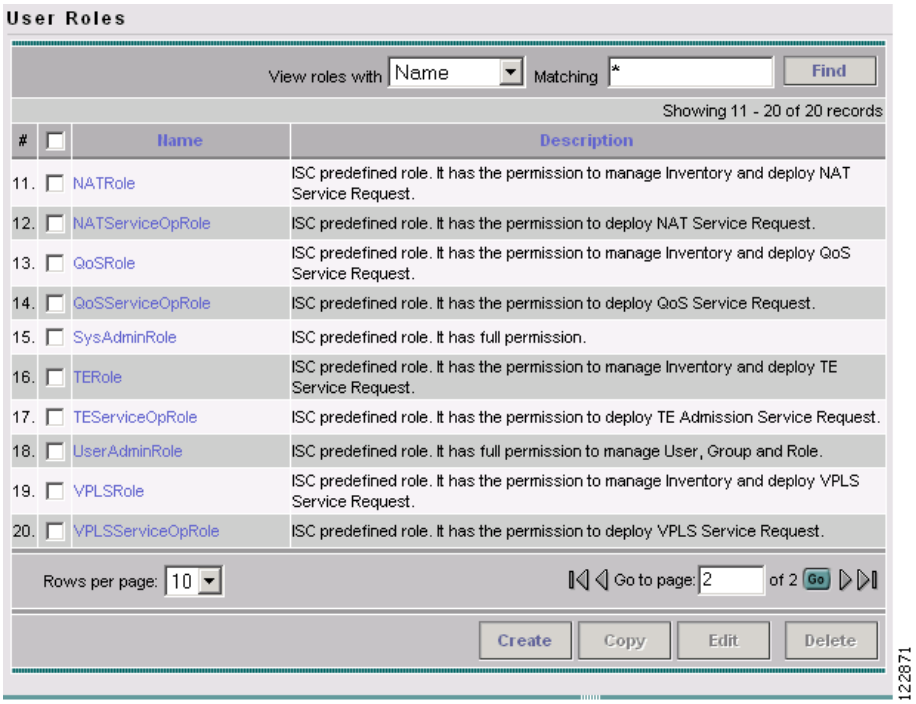
This chapter contains the following sections:

TE User Roles

A TE user role can be a predefined or a user-specified role defining a set of permissions. For a detailed description of user roles in ISC and how to use them, see the *Cisco IP Solution Center Infrastructure Reference, 4.0*.

To access the User Roles window and locate the TE user roles, navigate **Administration > Security > User Roles**. The User Roles window in Figure 9-1 appears.

Figure 9-1 User Roles



For a description of the various window elements, see *Cisco IP Solution Center Infrastructure Reference, 4.0*.

There are two pre-defined TEM user roles:

- **TERole**—Grants full permission to TEM operations.
- **TEServiceOpRole**—Grants permission only to manage the TE Admission SR.

TE Policies

Policies are used to define common tunnel attributes. Attributes such as bandwidth pools, hold and setup priority, and affinity bits, are set manually during policy creation as described below.

This section describes the following policy operations:

- Create Policy, page 9-2
- Edit Policy, page 9-4
- Delete Policy, page 9-5

Create Policy

ISC TEM allows you to create TE-specific policies in a manner similar to other ISC policies.

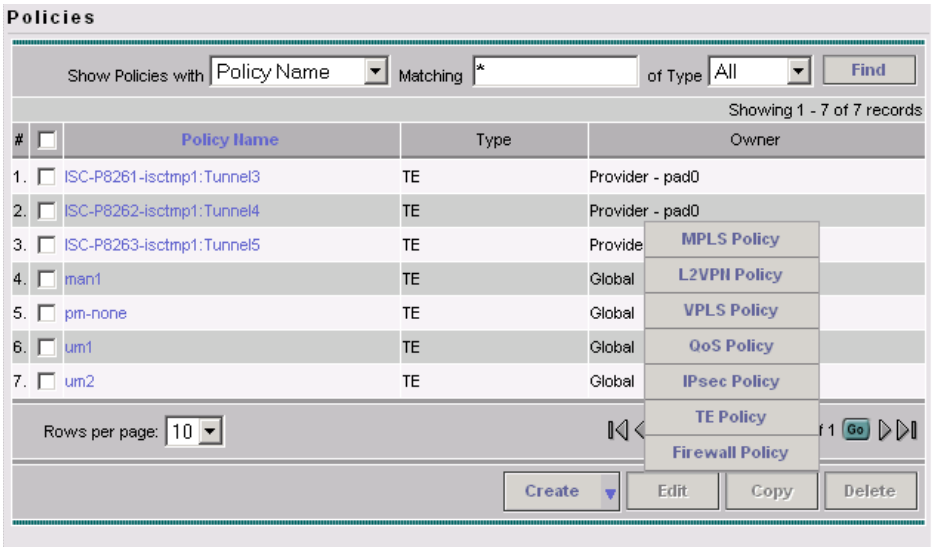
To create a TE policy, you must access the Policy Manager. Use the following steps:

Step 1 Navigate **Service Design > Policy Manager**.

Step 2 Click the **Policy Manager** icon.

The Policies window in Figure 9-2 appears.

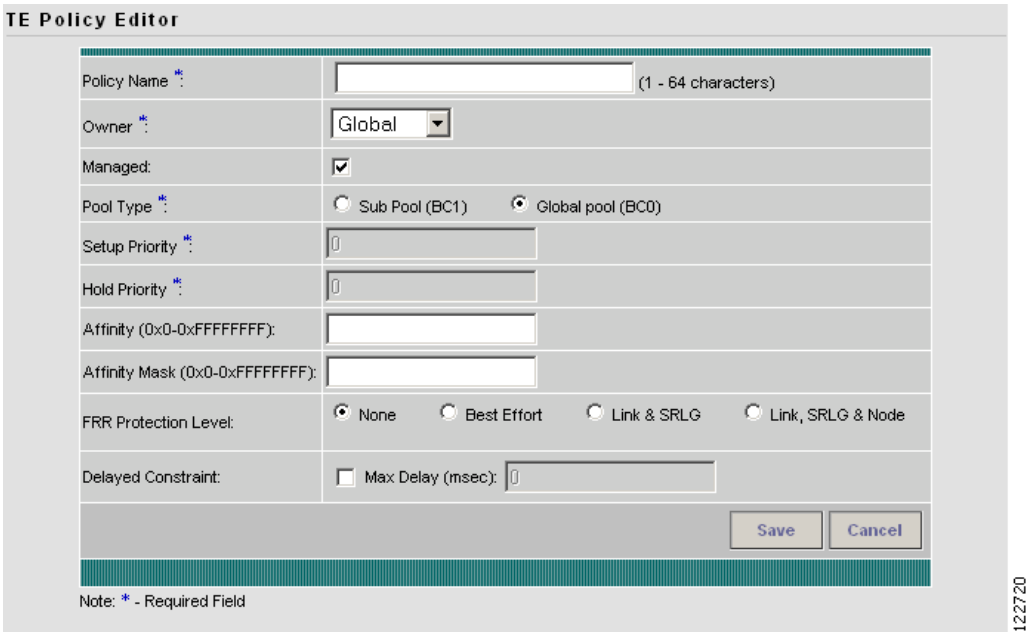
Figure 9-2 Policies Window



Step 3 Click **Create** and select **TE Policy** to set up a new TE policy.

The TE Policy Editor window in Figure 9-3 appears.

Figure 9-3 TE Policy Editor



The TE Policy Editor window contains the following fields:

- **Policy Name**—Name of the TE policy chosen by the user.
- **Owner**—The owner of the TE policy:
  - **Global**—A global policy.
  - **Provider**—A provider policy.
  - **Customer**—A customer policy.
- **Managed**—Check this box to make the policy to be used by managed tunnels. When clicked, both the setup and hold priorities are set to zero and these are not editable. If the box s unchecked, the setup/hold priorities can be set to a value between 1 and 7.

  Clicking the **Managed** check box will add some extra fields in the TE Policy Editor corresponding to two additional protection levels for **FRR Protection Level** (Fast Re-Route) and a new field, **Delay Constraint**.
- **Pool Type**—Tunnel bandwidth pool type.
  - **Sub Pool (BC1)**—Bandwidth section nested inside the Global Pool part of the total bandwidth.
  - **Global Pool (BC0)**—Section of the total link bandwidth containing all Sub Pools for the link.
- **Setup Priority**—Priority used when signaling an LSP for the tunnel to determine, which of the existing tunnels can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 hold priority.
- **Hold Priority**—Priority associated with an LSP for the tunnel to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority.
- **Affinity**—Attribute values required for links carrying the tunnel (bit values are either 0 or 1).
- **Affinity Mask**—Which attribute values should be checked. If a bit in the mask is 0, a link's attribute value of that bit is irrelevant. If a bit in the mask is 1, the link's attribute value and the tunnel's required affinity for that bit must match.
- **FRR Protection Level**—Level of Fast Reroute protection required on the primary tunnel.
  - **None**—No backup tunnel needed.
  - **Best Effort**—Use backup tunnel if available.
  - **Link & SRLG**—Requires the path used by the tunnel to have link and SRLG protection.
  - **Link, SRLG & Node**—Requires the path used by the tunnel to have link, SRLG, and node protection.
- **Delay Constraint**—The path used by the tunnel is required to meet the delay constraint specified.
  - **Max Delay (msec)**—Maximum delay allowed.

Two actions are available:

- **Save**—Save the TE policy with the current data.
- **Cancel**—Quit the TE Policy Editor and discard any changes.

Edit Policy

A policy can be edited only if it is not associated with a tunnel.

To edit a TE policy, use the following steps:

Step 1 Navigate **Service Design > Policy Manager**.

Step 2 Click the **Policy Manager** icon.

The Policies window in Figure 9-2 appears.

Step 3 Select the desired policy and click **Edit**.

The TE Policy Editor window in Figure 9-3 appears. The TE Policy Editor window in Figure 9-3 appears. The policy editor is described in Create Policy, page 9-2. The only difference between the create and edit processes is that the policy name and owner are not editable when editing a policy.

Step 4 Make the desired changes to the policy attributes and click **Save**. If the save operation succeeds, the new TE policy now appears in the Policies window. If not, the **Status** box will indicate the type of error that occurred and, when possible, the corrective action required.

Delete Policy

A policy can be deleted only if it is not associated with a tunnel.

To delete a TE policy, use the following steps:

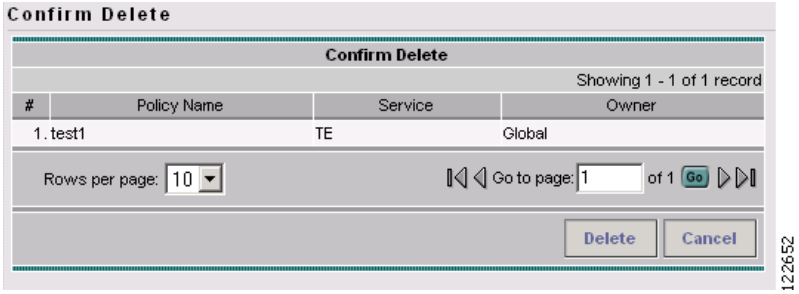
Step 1 Navigate **Service Design > Policy Manager**.

Step 2 Click the **Policy Manager** icon.

The Policies window in Figure 9-2 appears.

Step 3 Select the desired policy and click **Delete**. The Confirm Delete window in Figure 9-4 appears

Figure 9-4 Policies - Confirm Delete



Step 4 Check the policy marked for deletion and click **OK**.

Step 5 The Policies window refreshes and the selected policy disappears.

TE Tasks

ISC TEM currently offers three TE-specific tasks that are used in a manner similar to other ISC tasks:

- **TE Discovery**—Populates the repository with data from the TE network. Discrepancies are reconciled and/or reported.
- **TE Functional Audit**—Performs functional audit on TE Primary or Backup SRs in certain states.
- **TE Interface Performance**—Calculates the interface/tunnel bandwidth utilization.

This section focuses on describing how to create TE Functional Audit and TE Interface Performance tasks. Instructions on how to create a TE Discovery task are included in Chapter 3, "TE Network Discovery".

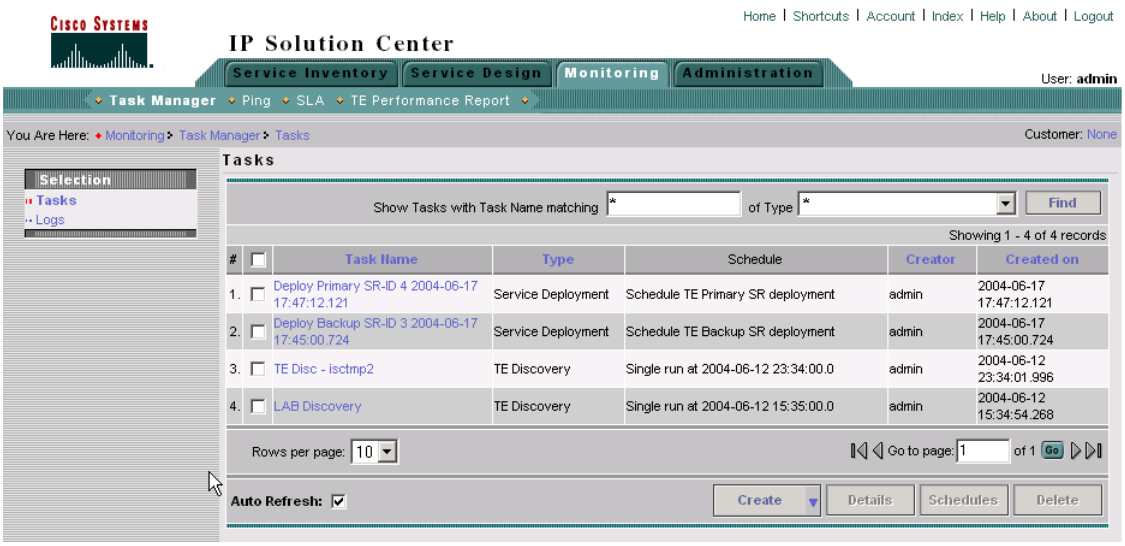
Creating a TE Task

TE tasks are managed in the ISC **Task Manager**, which is accessed as follows:

Step 1 Navigate **Monitoring > Task Manager**.

The Tasks window in Figure 9-5 appears.

Figure 9-5 Tasks Window



For a detailed description of the window elements in the Tasks window, see *Cisco IP Solution Center Infrastructure Reference, 4.0*.

This page shows all collection and deployment tasks that have been executed. Note that a task could be scheduled to happen once or there could be several scheduled runs of a task. The schedule can be viewed by selecting a task and clicking **Schedules**.

Creating a TE Functional Audit Task

For each tunnel in the SR, the TE Functional Audit task checks the LSP currently used on a router against the LSP stored in the repository:

- tunnel down—Ignore (do not check)
- tunnel up—Check the LSP used on the router against the one stored in the repository:

  - If they are the same, the tunnel and the SR are both set to **Functional**.
  - If they are different, both the tunnel and the SR are set to **Broken**.
- tunnel missing from router—SR left untouched. The tunnel state is set to **Lost**.

This task only performs functional audit on TE Primary or Backup SRs, which are not in one of the following states:

- **Closed**
- **Requested**
- **Invalid**
- **Failed Deploy**

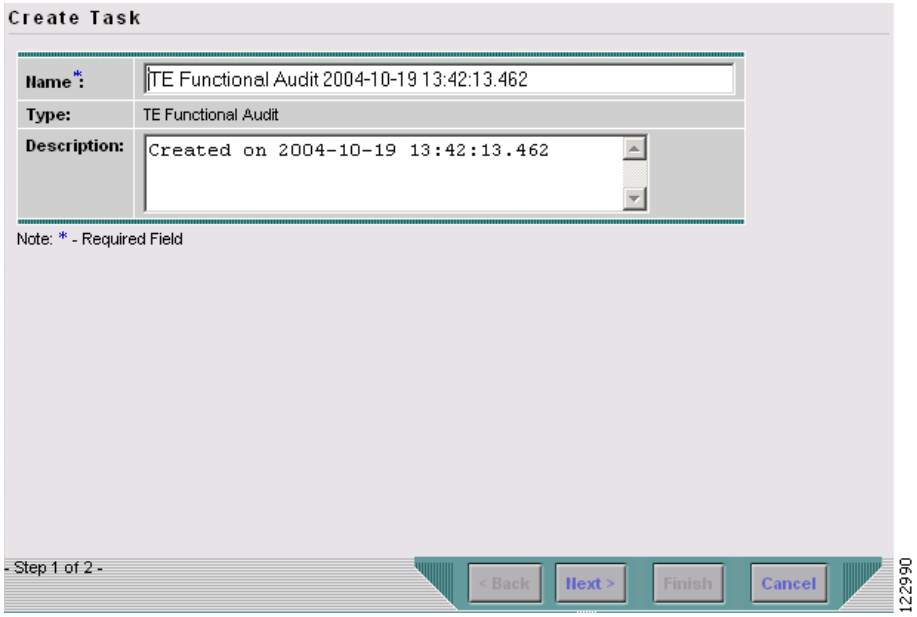
For a detailed explanation of the various states, see *Cisco IP Solution Center Infrastructure Reference, 4.0*.

To create a TE Functional Audit task, use the following steps:

Step 1 Navigate **Monitoring > Task Manager**.

Step 2 Click **Audit > TE Functional Audit** to open the Create Task window in Figure 9-6.

Figure 9-6 Create a TE Functional Audit Task

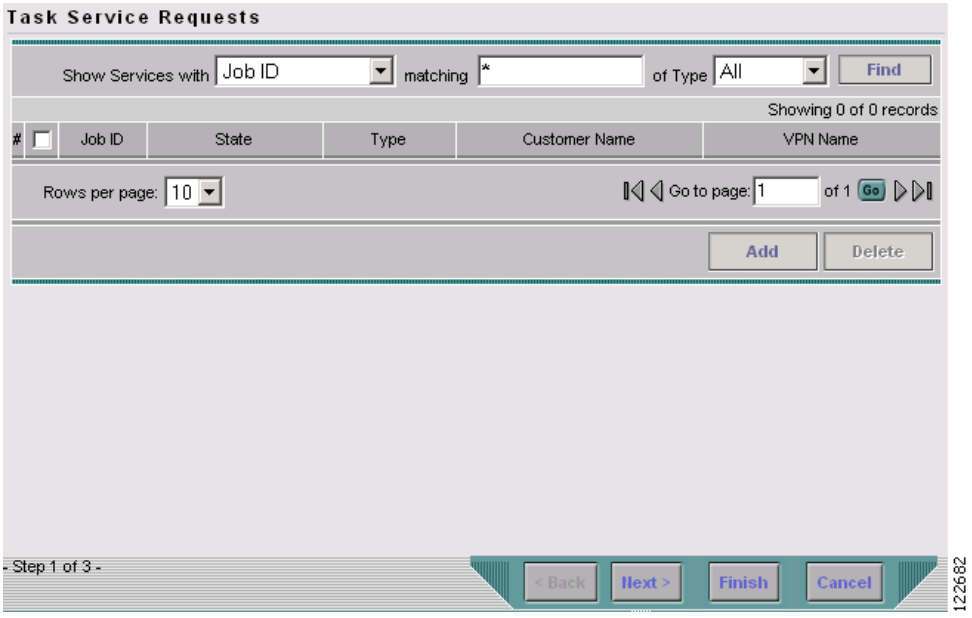


For a detailed description of the window elements in the Create Task window, see *Cisco IP Solution Center Infrastructure Reference, 4.0*.

Step 3 Modify the **Name** or **Description** fields as desired and click **Next**.

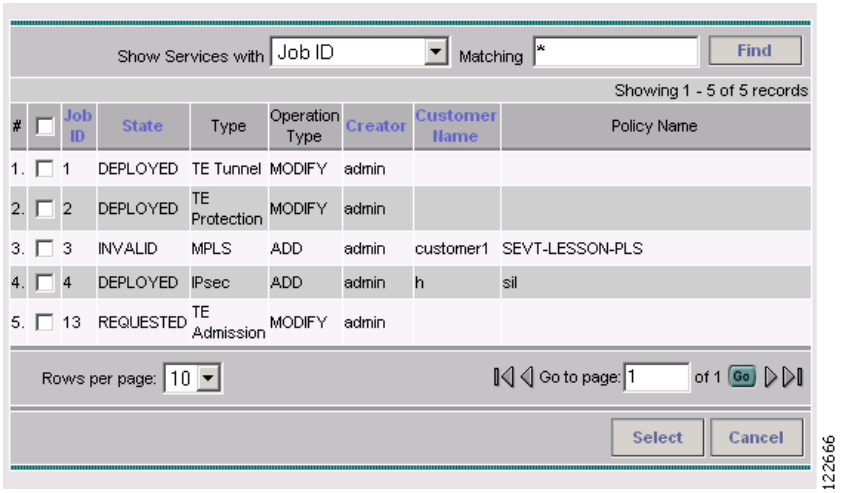
The Task Service Requests window in Figure 9-7 appears.

Figure 9-7 Task Service Requests



Step 4 Click **Add** to add a task service request. The Select Service Request(s) window in Figure 9-8 appears.

Figure 9-8 Select Service Request(s)

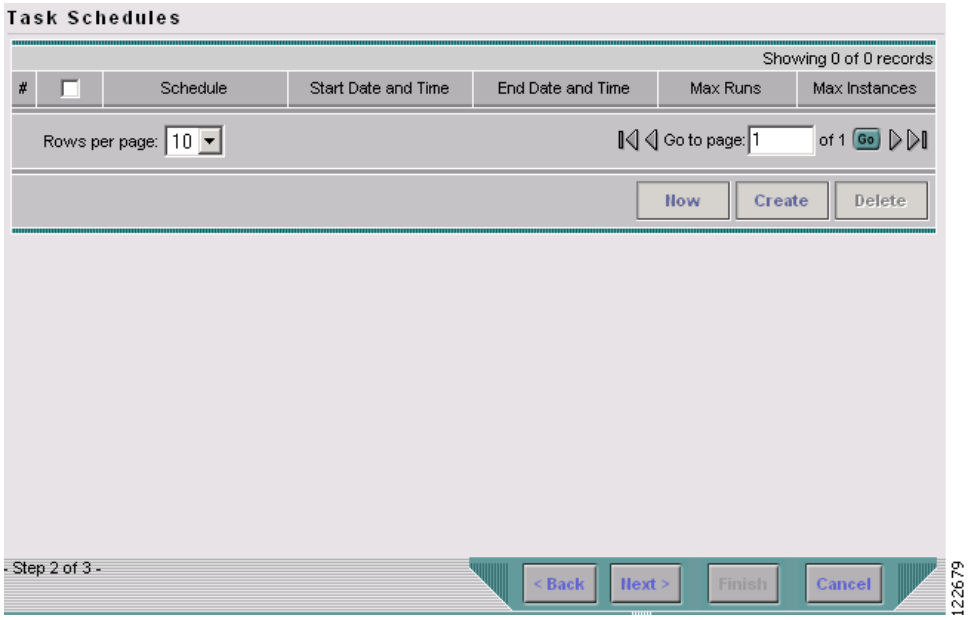


Step 5 Select an SR using the **Select** button.

The Selected Service Request(s) window closes and the selected task(s) now appears in the Task Service Requests window. To add other SRs, repeat the procedure in Step 4 and Step 5.

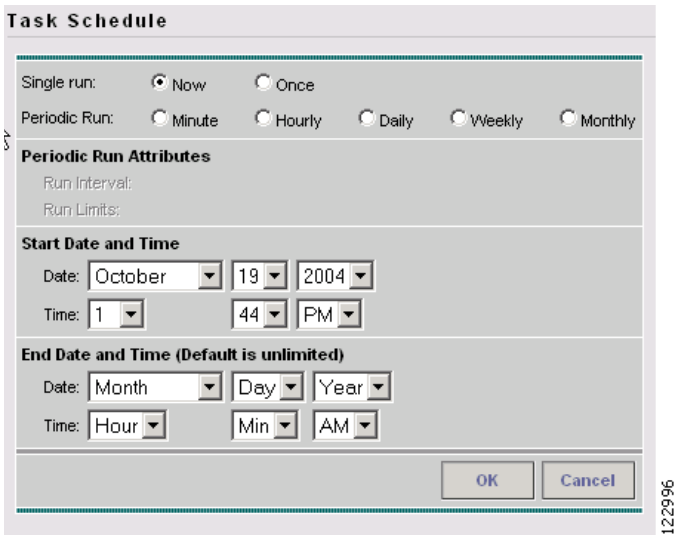
Step 6 In the Task Service Requests window, click **Next**. The Task Schedules window in Figure 9-9 appears.

Figure 9-9 Task Schedules



Step 7 Click **Now** to start the task immediately or **Create** to create a task schedule. The Task Schedule window in Figure 9-10 appears.

Figure 9-10 Task Schedule



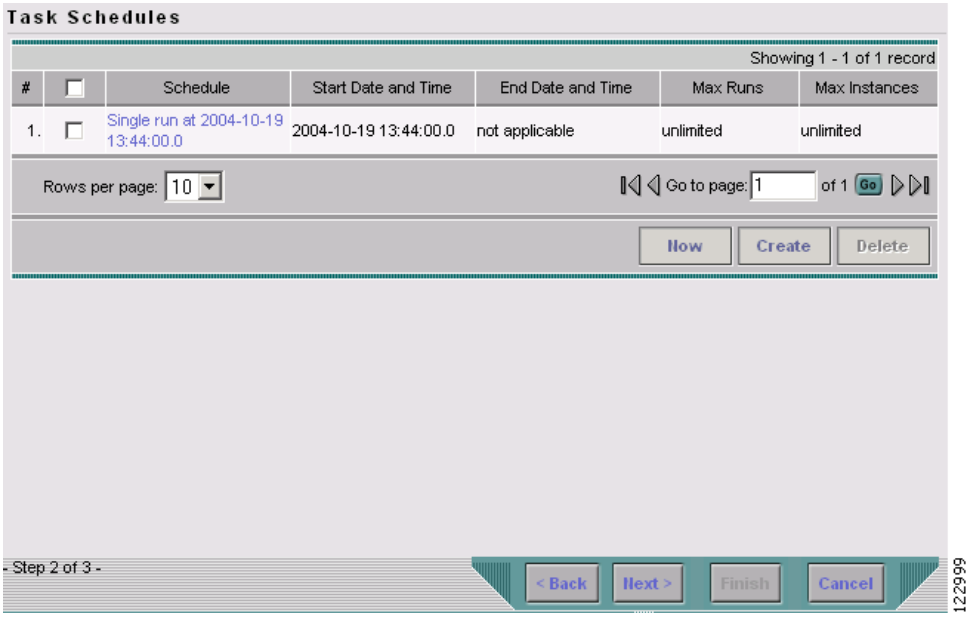
Step 8 In the Task Schedule window, indicate when and how often to run the task.

Step 9 Click **OK**. The scheduled task should now appear in the **Task Schedules** table.

Note The default setting is to schedule a single TE Functional Audit task to take place immediately ("**Now**").

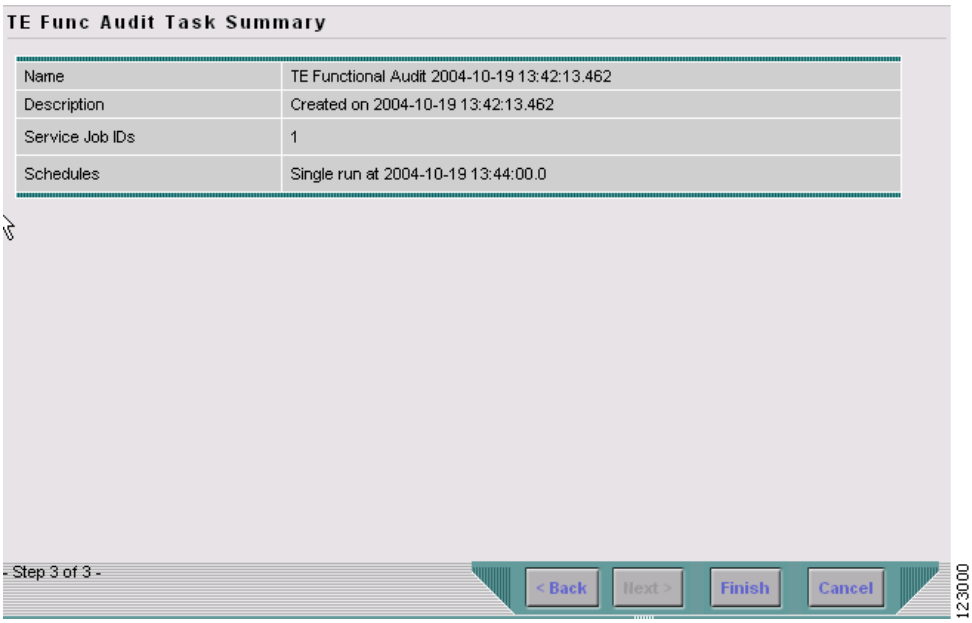
Step 10 Click **Next**. The Task Schedule window now shows the new task in its list of created tasks as shown in Figure 9-11.

Figure 9-11 Task Schedule with Scheduling Data



Step 11 A summary of the scheduled task appears as shown in Figure 9-12.

Figure 9-12 TE Functional Audit Task Summary



Step 12 Click **Finish**. This adds the task to the list of created tasks in the Tasks window (Figure 9-5).

To view the task logs for the created tasks, see Viewing a Task Log, page 10-2.

Creating a TE Interface Performance Task

This task calculates interface/tunnel bandwidth utilization using the Simple Network Management Protocol (SNMP).

Calculating utilization depends on how data is presented for the object you want to measure. Interface utilization is the primary measure used for network utilization. Because MIB-II variables are stored as counters, you must take two poll cycles and figure the difference between the two (hence, the delta used in the equation).

Three variables are required:

- task duration—how long the task will run (in secs)
- frequency—how frequent the data will be collected (in secs)
- interval—the distance between two poll cycles (in ms).

The following explains the variables used in the formulas:

- delta(ifInOctets)—the delta between two poll cycles of collecting the SNMP ifInOctets object, which represents the count of inbound octets of traffic
- delta(ifOutOctets)—the delta between two poll cycles of collecting the SNMP ifOutOctets object, which represents the count of outbound octets of traffic
- IfSpeed—the speed of the interface, as reported in the snmpifSpeed object.

A more accurate method is to measure the input utilization and output utilization separately, using the following formula:

$$\text{Input utilization} = \frac{\text{delta(ifInOctets)} \times 8 \times 100}{(\text{number of seconds in delta}) \times \text{ifSpeed}}$$

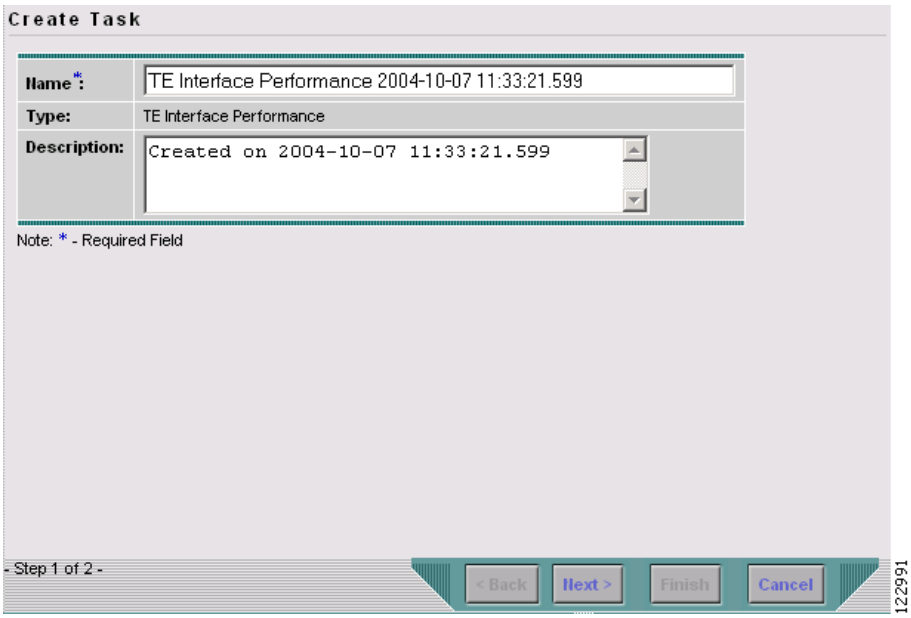
$$\text{Output utilization} = \frac{\text{delta(ifOutOctets)} \times 8 \times 100}{(\text{number of seconds in delta}) \times \text{ifSpeed}}$$

To create a TE Interface Performance task, use the following steps:

Step 1 Navigate **Monitoring > Task Manager**.

Step 2 Click **Create** to open the Create Task window in Figure 9-13.

Figure 9-13 Create TE Interface Performance Task

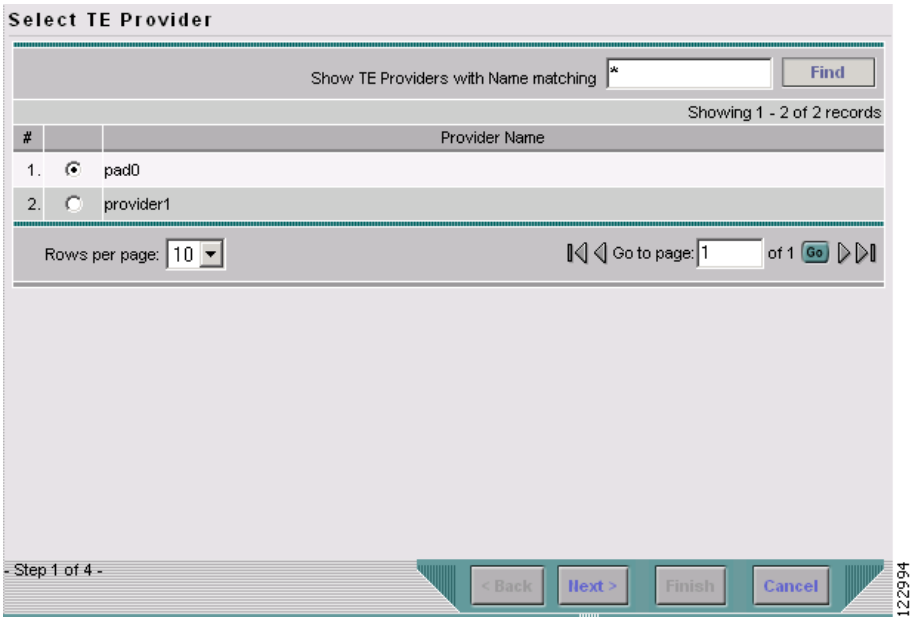


For a detailed description of the window elements in the Create Task window, see *Cisco IP Solution Center Infrastructure Reference, 4.0*.

Step 3 Select **TE Interface Performance** in the drop-down list of the **Type** field.

The Select TE Provider window in Figure 9-14 appears.

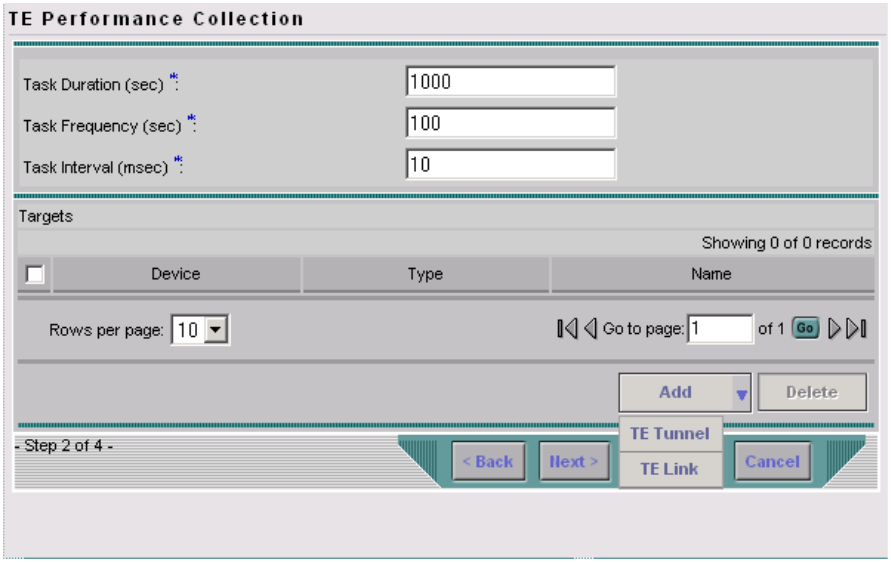
Figure 9-14 Select TE Provider



Step 4 Click a radio button to select a TE provider.

Step 5 Click **Next**. The TE Performance Collection window in Figure 9-15 appears.

Figure 9-15 TE Performance Collection



Step 6 Enter desired values in the **Duration**, **Frequency**, and **Interval** fields.

Step 7 Use the **Add** button to select a tunnel or link on which to run the interface performance task:

- **TE Tunnel**—Add a TE tunnel. The Select Tunnel(s) window in Figure 9-16 appears.
- **TE Link**—Add a TE link. The Select Link(s) window in Figure 9-17 appears.

Figure 9-16 Select Tunnel(s) - Interface Performance

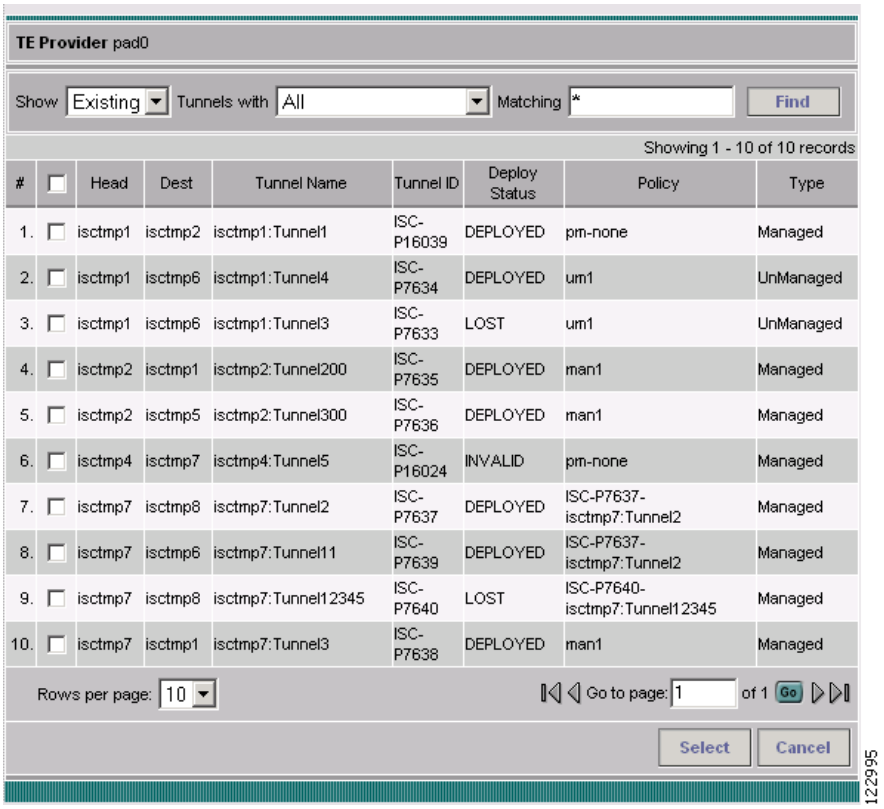
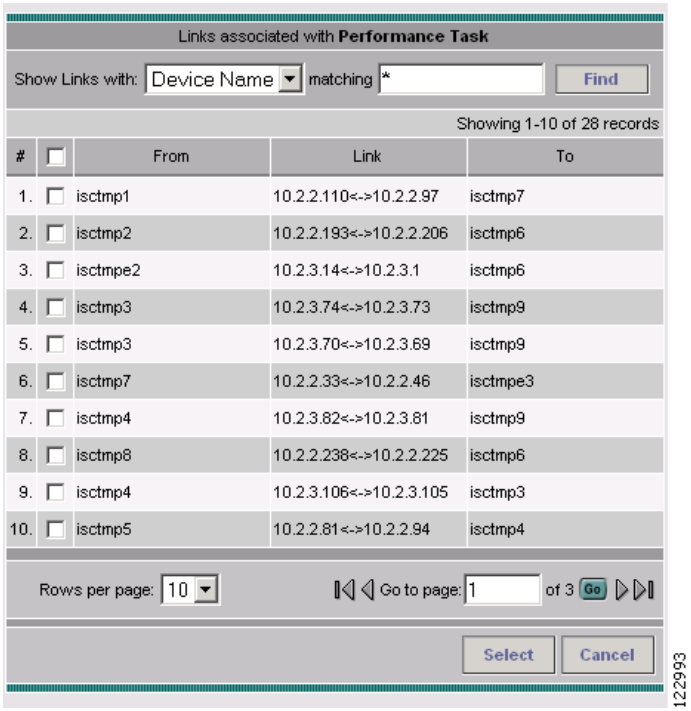


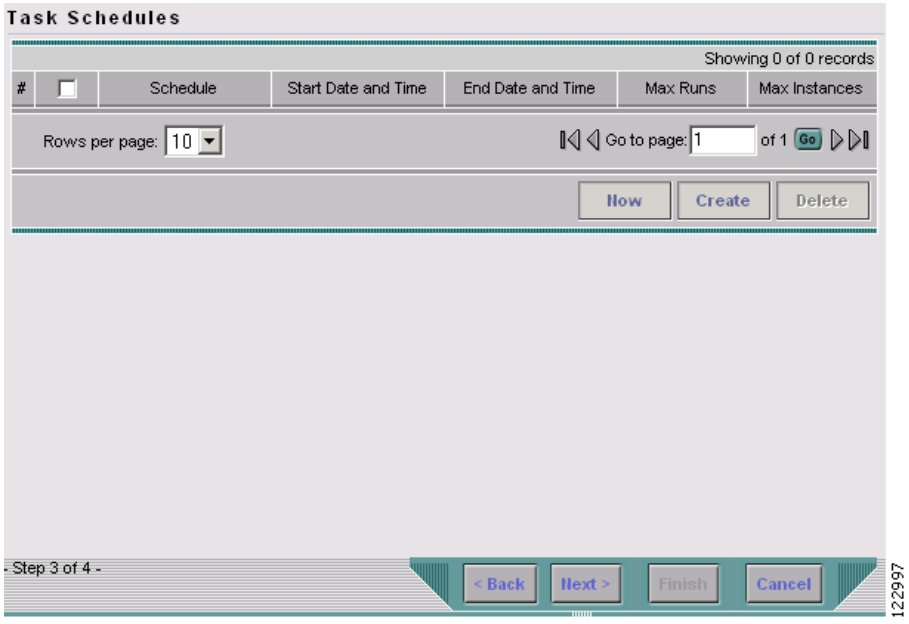
Figure 9-17 Select Link(s)



Step 8 Select one or more of tunnels and links and click **Next**.

Step 9 The Task Schedules window in Figure 9-18 appears.

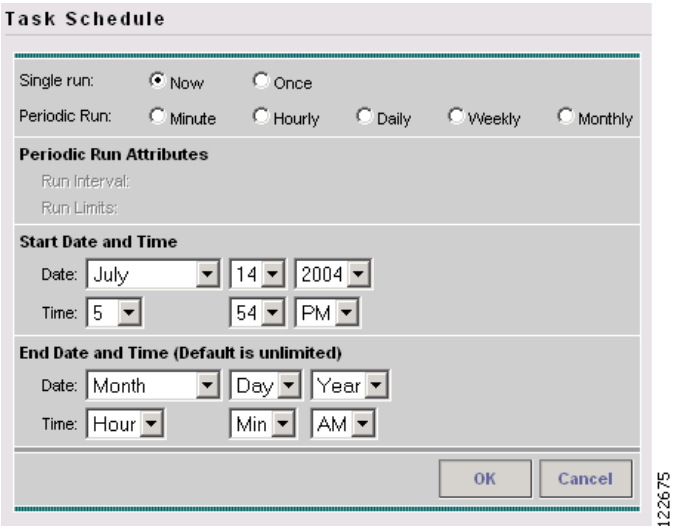
Figure 9-18 Task Schedules



Step 10 Click **Now** or **Create** to create a task schedule. When you select **Create** to customize the schedule, the Task Schedule window in Figure 9-19 appears (with **Now**, this step is skipped).

Note The default setting is to schedule a single TE Interface Performance task to take place immediately ("**Now**").

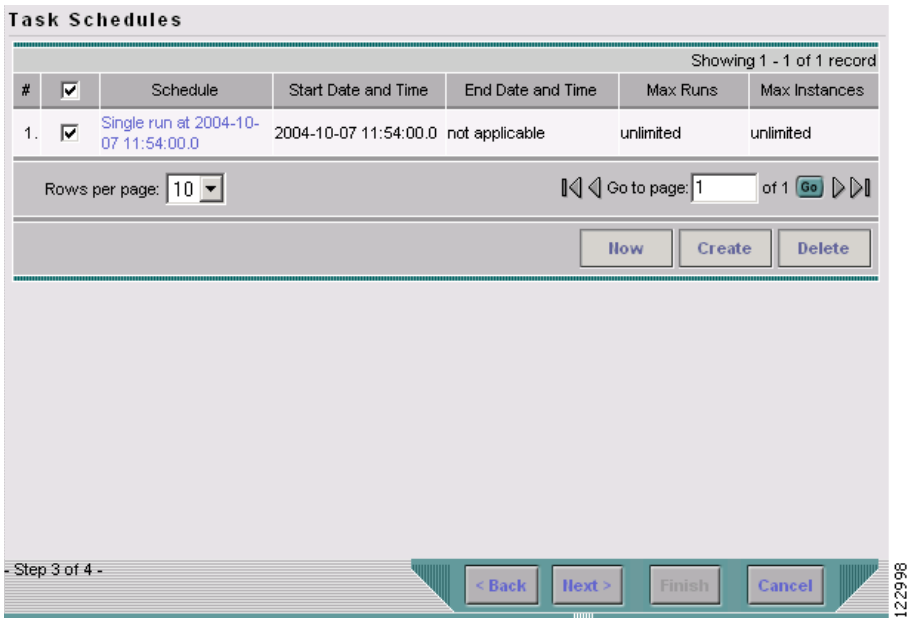
Figure 9-19 Task Schedule



Step 11 In the Task Schedule window, make your selections to define when and how often to run the task.

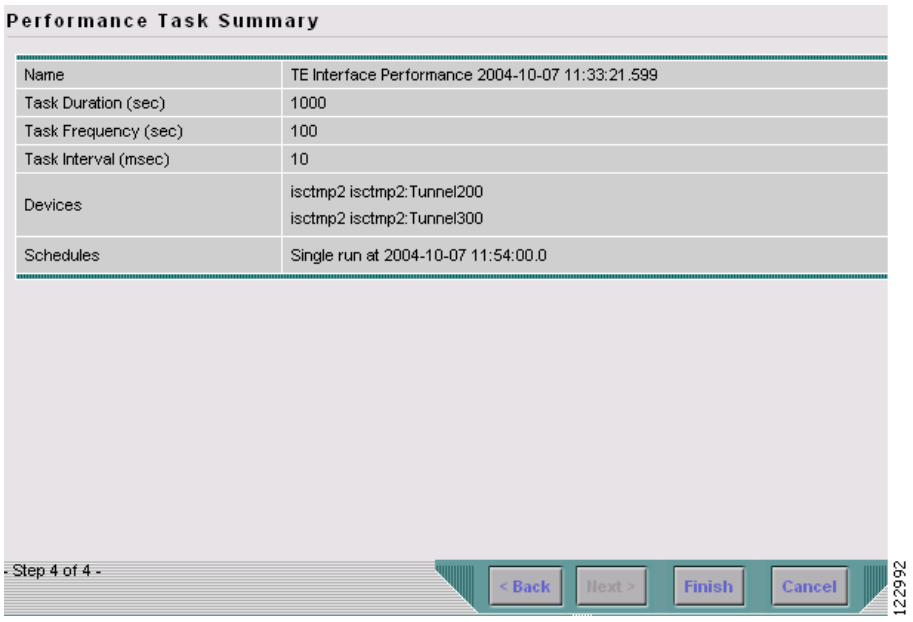
Step 12 Click **OK**. The scheduled task should now appear in the **Task Schedules** table as shown in Figure 9-20.

Figure 9-20 Task Schedules with Scheduling Data



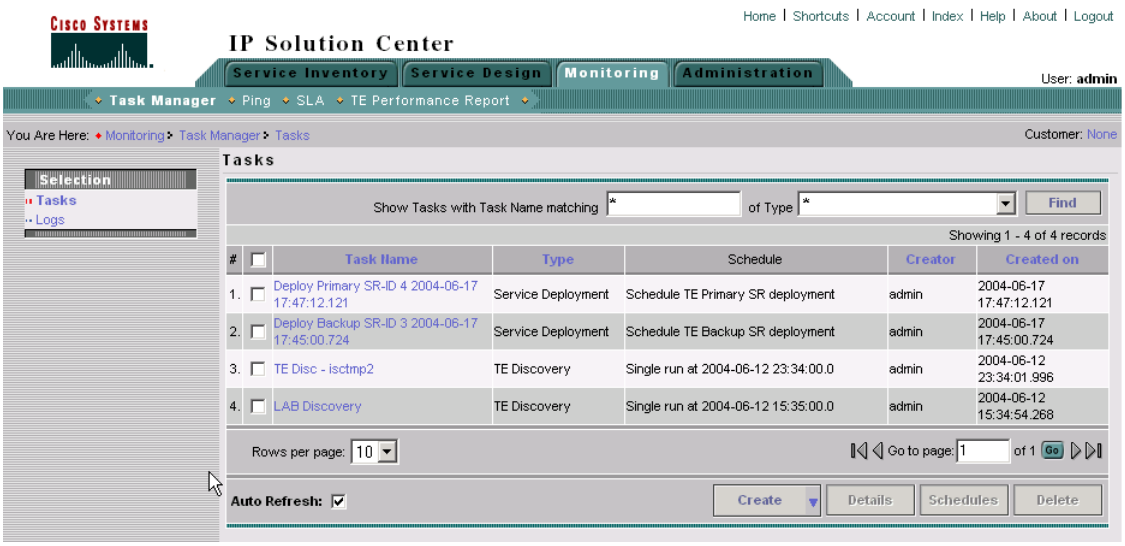
Step 13 Click **Next**. A summary of the scheduled task appears as shown in Figure 9-21.

Figure 9-21 Performance Task Summary



Step 14 Click **Finish**. This adds the task to the list of created tasks in the Tasks window (Figure 9-5).

Figure 9-22 Performance Task Summary



To view the TE Performance Report that is generated for TE Interface Performance task(s), see TE Performance Reports, page 10-4.

To view the task logs for the created tasks, see Viewing a Task Log, page 10-2.

SR History, Config Audit Report, and Configlets

The history, config audit reports, and configlets associated with individual service requests can be viewed from the Service Requests window when you click the **Details** button.

The history of an SR is essentially a state change report. It lists the various states that elements associated with an SR has transitioned between and reports relevant details pertaining to these state changes.

Configlets for devices associated with SRs are in simple scrollable text format.

Manage Lock

Whenever a task is performed that incurs a database update, which might affect the resource and hence the result of a tunnel computation, it locks the system before the update and releases it at completion of the update. If for some reason the lock is not released, other updates that require the lock are blocked.

The purpose of the lock feature is to prevent concurrent and mutually inconsistent planning activities from being committed to the database. Meaning, if each user takes the same snapshot of the the repository, performs computations, and tries to commit what he/she sees, the locking mechanism helps synchronize the commit and ensures that no commit invalidates other commits.

If the system is locked for prolonged periods of time, the administrator should check if anyone is performing long planning tasks and take note of, which process locked the system and report it. If the administrator is sure that no one is using the sytem, it can be unlocked by using the lock manager.

Each system lock is linked to a TE provider. To unlock the TE provider, use the following steps:

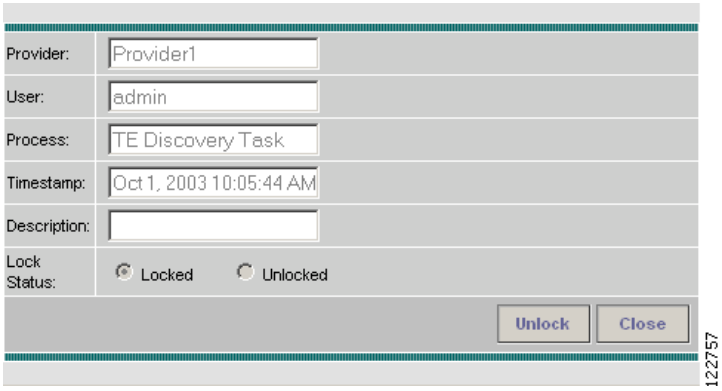
Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Providers**.

Step 2 The TE Providers window in Figure 2-3 appears.

Step 3 Select a TE provider that is locked by clicking the corresponding check box.

Step 4 Click **Manage Lock**. The System Lock Management window in Figure 9-23 appears.

Figure 9-23 System Lock Management



The text fields in this window are read-only.

Step 5 To unlock, click the **Unlock** button.

The System Lock Management window closes and the **System Lock Status** field in the TE Providers window is updated accordingly.