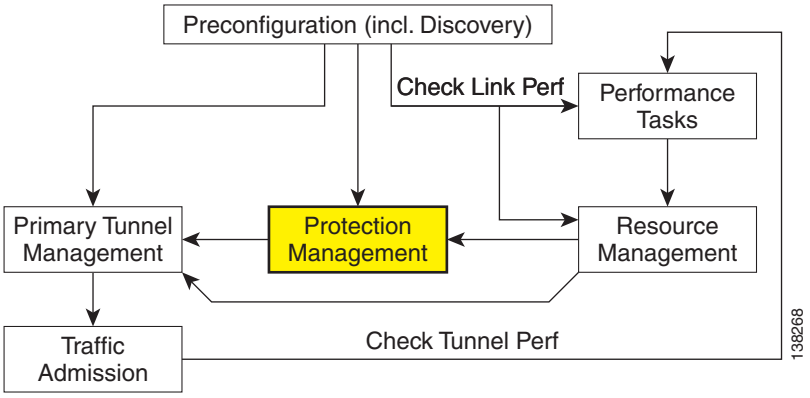
CHAPTER 40

Protection Planning

This chapter describes the process of creating and managing the protection of network elements using automated protection tools. See Chapter 38, "Basic Tunnel Management" for a description of the process using the basic tools.

The highlighted box in Figure 40-1 shows where in Prime Fulfillment protection management occurs.

Figure 40-1 Prime Fulfillment Process Diagram - Protection Management



This chapter includes the following sections:

Overview

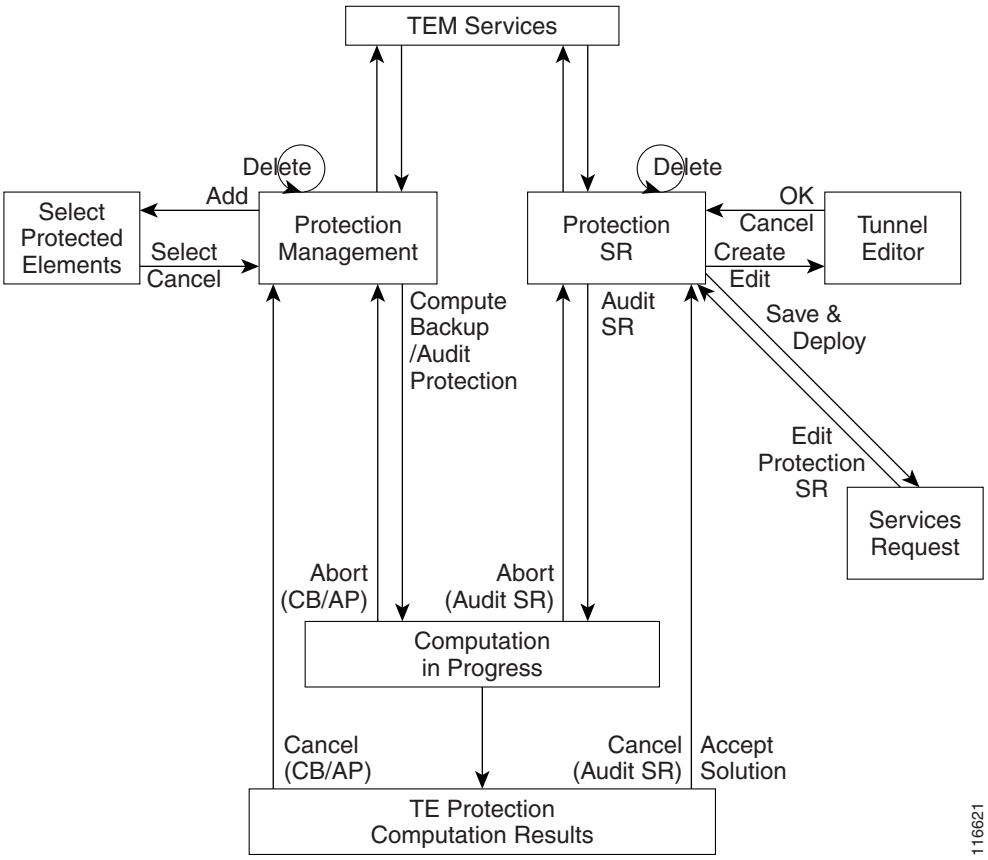
The purpose of protection planning is to protect selected elements in the network (links, routers, or SRLGs) against failure.

The first step is to identify the elements that must be protected and then invoke the protection tools to compute the protected tunnels. From the computation, the system responds for each element with either a set of tunnels that protect the element or a set of violations and warnings that help you determine why it could not be protected.

For successfully protected elements the tunnels can be deployed on the network. For elements that could not be protected, the protection is either ignored or the constraints are altered on the protection case. More specifically, this can involve changing the TE bandwidth settings of the links associated to the element and then rerunning the protection computation on the altered network.

An overview of the protection management processes is provided in Figure 40-2.

Figure 40-2 Protection Management Processes



SRLG Operations

It is not uncommon for links to have identical physical characteristics, such as being physically located in the same conduit, or being connected to the same hardware. As a result, they could fail as a group during a single failure event. A Shared-Risk Link Group (SRLG) addresses this problem by identifying links that could fail together.

After SRLG modifications (create, edit, delete), use the protection planning functions in the **TE Protection Management** window to ensure that adequate protection is available on the network.

Create SRLG

Creating an SRLG is only necessary if a shared risk link group has been identified and it must be protected.

To create an SRLG, use the following steps:

Step 1 Choose **Traffic Engineering > SRLGs**.

The TE SRLG List window appears.

Step 2 To create an SRLG in the **TE SRLG List**, click **Create**.

The TE SRLG Editor window appears.

Step 3 Specify an **SRLG Name**.

Step 4 Click **Add Link**.

The Links associated with SRLG window appears.

Step 5 Select one or more links and click **Select**.

The corresponding link information is added to the link list and the Select window closes and returns to the SRLG editor.

Step 6 Click **Save** to save the SRLG.

This closes the SRLG editor and brings back the TE SRLG List as the active window, where the newly created SRLG is listed.

Edit SRLG

To edit an SRLG, use the following steps:

Step 1 Choose **Traffic Engineering > SRLGs**.

The TE SRLG List window appears.

Step 2 To edit an SRLG in the TE SRLG List, from the TE SRLG List window select the SRLG that you want to modify and click **Edit**.

The TE SRLG Editor window appears.

Step 3 Use **Add Link** and **Remove Link** to adjust to the desired set of links for the selected SRLG.

Step 4 Click **Save** to save the changes.

Delete SRLG

To delete an SRLG, use the following steps:

Step 1 Choose **Traffic Engineering > SRLGs**.

The TE SRLG List window appears.

Step 2 To delete an SRLG in the TE SRLG List, from the TE SRLG List window select the SRLG(s) that you want to delete and click **Delete**. The Delete Confirm window appears.

Step 3 Click **Delete** to confirm.

The Delete Confirm window closes. After the TE SRLG List window has been updated, the deleted SRLG no longer appears in the SRLG list.

Configure Element Protection

Before a protection computation can be performed, it is necessary to configure the network element protection.

To do so, use the following steps:

Step 1 Choose **Traffic Engineering > Protected Elements**.

The TE Protection Management window appears.

Explanation of the **Protection Status** field:

Protection Status—The protection status displayed is determined from the last time an audit was performed. The audit is performed either explicitly by the user or when the protection SR is deployed. The protection status is stated for each network element as either **Protected**, **Not Fully Protected**, or **Unknown**. Click on the column header, **Protected**, to sort elements according to protection status

Step 2 First, decide which network elements must be protected.

In the TE Protection Management window, click **Add** to add a protection element (link, node, or SRLG). The Select Protection Elements window appears.

Links that are connected to non-Cisco devices cannot be protected and will, therefore, not show in the Select protection elements window. Likewise, non-Cisco devices and SRLGs that contain links to non-Cisco devices cannot be protected and are excluded from the selection.

Step 3 Select one or more elements to be protected and click **Select.**

The Select Protection Element window closes and the TE Protection Management window reappears.

Next, decide which protection tools should be applied. These are described in Protection Tools, page 40-5.

Protection Tools

Relying on manual creation of backup tunnels as described in Chapter 38, "Basic Tunnel Management" has its limitations, not just for larger and more complicated networks.

The protection tools available in Prime Fulfillment provide a number of tools that automatically compute and verify protection of specified network elements.

Note Certain attributes, such as Description, that do not impact the computation carried out by these tools and updates to these are, therefore, not displayed in the computation results window.

Compute Backup

Compute Backup is used to let Prime Fulfillment automatically compute the necessary backup tunnels to protect specified network elements. The manual process is described in Chapter 38, "Basic Tunnel Management"

To run Compute Backup, use the following steps:

Step 1 Choose **Traffic Engineering > Protected Elements**.

Step 2 Configure the necessary protection elements as described in Configure Element Protection, page 40-4.

Step 3 If you only want to perform Compute Backup on selected elements, select one or more elements on which to calculate a backup path.

Step 4 Click **Compute Backup** and select one of the following:

- All Elements
- Selected Elements

First the Computation In Progress window appears and then the TE Protection Computation Results window appears.

The **Element:** table displays the outcome of the computation for each element in the protection computation. The status for each element is indicated by at least one row per element in the table. If the status is not valid, the table will contain one row per warning or violation.

The **Element:** table contains the following columns:

- **Element Name**—Name of the network element to be protected.
- **Type**—Network element type (node, link, or SRLG).
- **Report**—Warning or violation associated with an element, if any, as reported by the computation engine.
- **Status**—Computation status of the network element:
  - Valid Tunnels—The element is fully protected by backup tunnels.
  - InvalidTunnels—An Audit Protection detected that the element was not fully protected by the existing backup tunnels.
  - No Solution Exists—A Compute Backup has proven that it is not possible to fully protect the element.

Note Certain attributes, such as Description, that do not impact the computation carried out by the protection tools and updates to these are not displayed in the computation results window.

Step 5 Select a row corresponding to a specific warning or violation and click **Detail** to display a detailed description in the right pane and backup tunnels associated with the selected item in the bottom pane.

For a description of warnings and violations, see Chapter 45, "Warnings and Violations."

Explanation of the **Protection Type** column:

- **Protection Type**—Protection side-effect from activating the tunnel. There are three protection types:
  - **Protection tunnels**—Tunnels that can be activated to provide protection for a specified element.
  - **Side-effect tunnels**—Tunnels that are activated to protect a neighboring element, but which are also activated when a specified element fails.
  - **Activated tunnels**—Tunnels that are activated when a specified element fails, and which might or might not provide protection for the specified element or its neighbors.

The **Backup Tunnel** table displays which new protection tunnels are required and any existing tunnels that should be kept or deleted for each element.

Step 6 If the proposed protection solution is acceptable, click **Accept Solution**.

The TE Protection SR window appears with all tunnel additions and deletions computed by the system.

For an explanation of the various window elements, see Create Backup Tunnel, page 38-13.

Optionally, you can make tunnel changes here and then run **Audit SR** to ensure that you have the desired level of protection before you deploy (see Audit SR, page 40-8).

Step 7 Click **Save & Deploy** to deploy the new tunnel SR to the network.

When you click **Save & Deploy**, Prime Fulfillment locks the TE routers effected, which will block any subsequent SRs which use that TE router until the SRs are finished. It is safe to try and deploy other SRs in the system. If there is any conflict with the SR currently being processed, Prime Fulfillment will simply ask you to wait until it is complete. To see the state of deployment, go to the Service Requests window under Inventory and Connection Manager or open the Task Manager under Monitoring.

Note With the exception of TE Traffic Admission SRs, TE SRs are always deployed immediately from the specific TE SR window, not from the **Service Requests** page in **Inventory and Connection Manager**.

The Service Requests window (**Operate > Service Request Manager)** opens and displays the state of the deployed SR.

For more information on working with service requests, see the managing service requests part elsewhere in this guide.

If the SR does not go to the **Deployed** state, go to the Task Logs window to see the deployment log (**Monitoring > Task Manager > Logs**) as described in SR Deployment Logs, page 56-1.

Audit Protection

As opposed to the Compute Backup tool described on page 5, Audit Protection does not attempt to create a backup solution. It seeks to verify protection of specified network elements with the current set of backup tunnels and reports any warnings or violations that are discovered. It is recommended that any time a change has been committed on the TE topology such as resources on TE links or SRLG memebership, a protection audit be run to verify the protection status on all elements.

The computation will display the same computation results page as for Compute Backup. When you return from the computation results page, the Protection Status column in the TE Protection Management window is updated to show the level of protection for each element.

This section describes the necessary steps to perform Audit Protection on one or more network elements.

To run Audit Protection, use the following steps:

Step 1 Choose **Traffic Engineering > TE Protected Elements**.

The TE Protection Management window appears.

Explanation of the **Protection Status** field:

Protection Status—The protection status displayed is determined from the last time an audit was performed. The audit is performed either explicitly by the user or when the protection SR is deployed. The protection status is stated for each network element as either **Protected**, **Not Fully Protected**, or **Unknown**. Click on the column header, **Protected**, to sort elements according to protection status

Step 2 If you only want to perform Audit Protection on selected elements, select one or more tunnels on which to calculate a backup path.

Click **Audit Protection** and select one of the following:

- All Elements
- Selected Elements

The Computation In Progress window appears.

Then the TE Protection Computation Results window appears.

For an explanation of the various window elements, see Compute Backup, page 40-5.

Note Certain attributes, such as Description, that do not impact the computation carried out by the protection tools and updates to these are not displayed in the computation results window.

Step 3 To view the backup tunnels for a particular element, select the element and click **Details**.

The TE Protection Computation Results window appears.

For an explanation of the various window elements, see Compute Backup, page 40-5.

Step 4 Select a row corresponding to a specific warning or violation and click **Details** to display a detailed description in the right pane and backup tunnels associated with the selected item in the bottom pane.

Tunnels associated with a warning or violation are flagged in the **Report** column in the **Backup Tunnels** table in the bottom pane.

The **Accept Solution** button is greyed out because the audit does not provide a solution but rather an evaluation.

For a description of warnings and violations, see Chapter 45, “Warnings and Violations.”

Step 5 Click **Cancel** to return to the TE Protection Management window.

The protection status is updated in the Protection Status column.

Audit SR

Audit SR audits protection of all elements in the **TE Protection Management** window against backup tunnels in the TE Protection SR window.

This feature can be used to audit the protection for manually added, modified, and deleted tunnels in the TE Protection SR window before deploying them.

To audit a TE backup tunnel SR, use the following steps:

Step 1 Choose **Traffic Engineering**.

Step 2 Click **Create TE Backup Tunnel**.

The **TE Protection SR** window appears. For an explanation of the various window elements, see Create Backup Tunnel, page 38-13.

Step 3 To audit the protection SR, click **Audit SR**.

Note Audit SR will only be enabled if there are elements in the TE Protection Management window. If this is not the case, the **Audit SR** button will be disabled (grayed out).

The FRR Audit process begins and the TE Protection Computation Results window appears.

See Audit Protection, page 40-7 for a description of the rest of the process. Detail and report windows are identical in these two processes.