CHAPTER 12

Deploying, Monitoring and Auditing Service Requests

This chapter describes how to deploy, monitor and audit L2VPN, L2TPv3 or VPLS service requests, and how to access task logs. It contains the following sections:

Deploying Service Requests

To apply L2VPN or VPLS policies to network devices, you must deploy the service request. When you deploy a service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a configlet.

Pre-Deployment Changes

You can change the Dynamic Component Properties Library (DCPL) parameter **actionTakenOnUNIVlanList** before you deploy an L2VPN or VPLS service request. This will be necessary if the **trunk allowed vlan** list is not present on the User Network Interface (UNI). To make this change, perform the following steps.

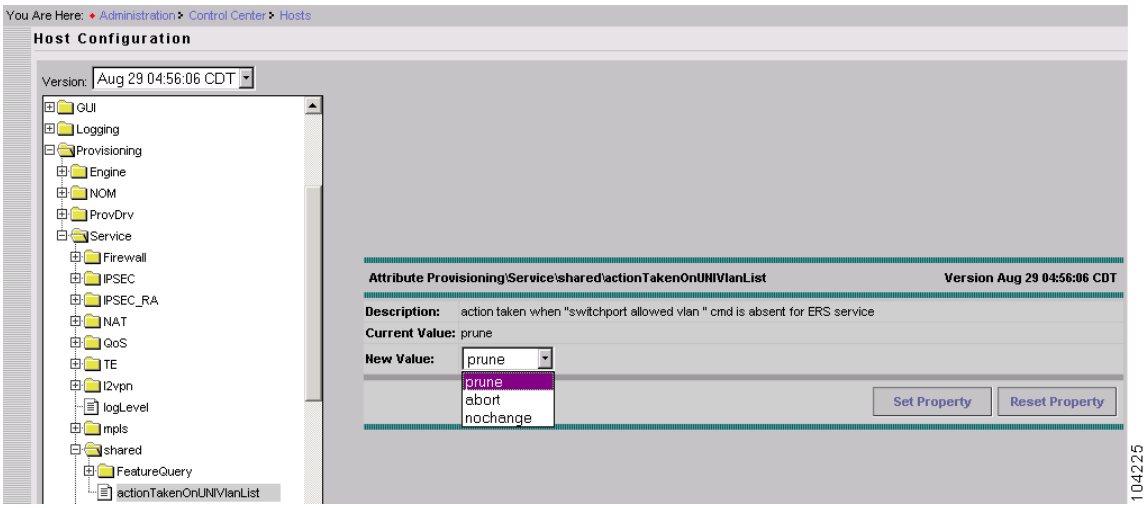
Step 1 Select **Administration > Control Center**.

Step 2 Choose the host that you want to change.

Step 3 Click **Config**.

Step 4 Select **Provisioning > Service > shared > actionTakenOnUNIVlanList**. The window shown in Figure 12-1 appears.

Figure 12-1 Change DCPL Parameter



Step 5 Choose one of the following:

- **prune** to have ISC create the minimum VLAN list. This is the default.
- **abort** to have ISC stop the L2VPN or VPLS service request provisioning with the error message: **trunk allowed vlan list is absent on ERS UNI**.
- **nochange** to have ISC allow all VLANs.

Step 6 Click **Set Property**.

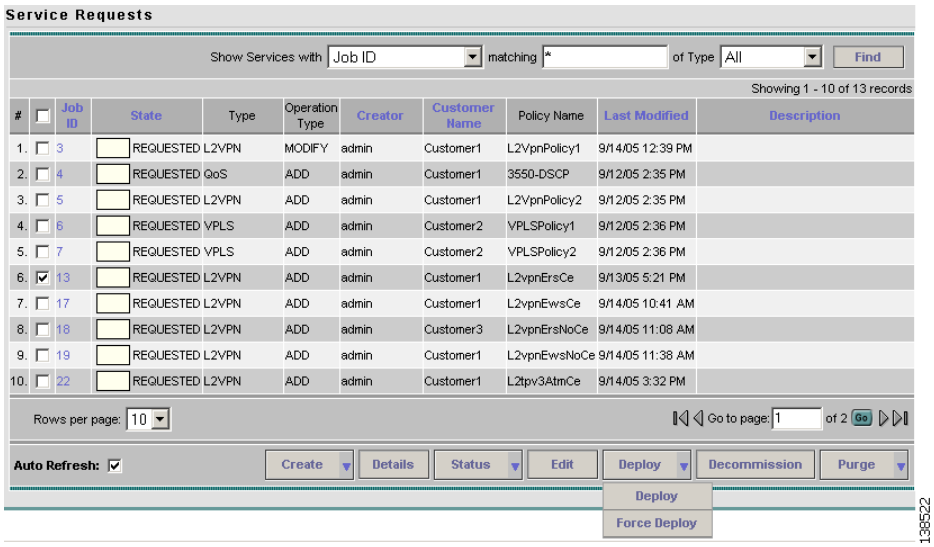
Service Deployment

After you create an L2VPN, L2TPv3, or VPLS service request and save it in the ISC repository, you can deploy or force-deploy it.

Step 1 Select **Service Inventory > Inventory and Connection Manager > Service Requests**.

The Service Requests window appears as shown in Figure 12-2.

Figure 12-2 Deploy a VPLS Service Request



Step 2 Choose a service request.

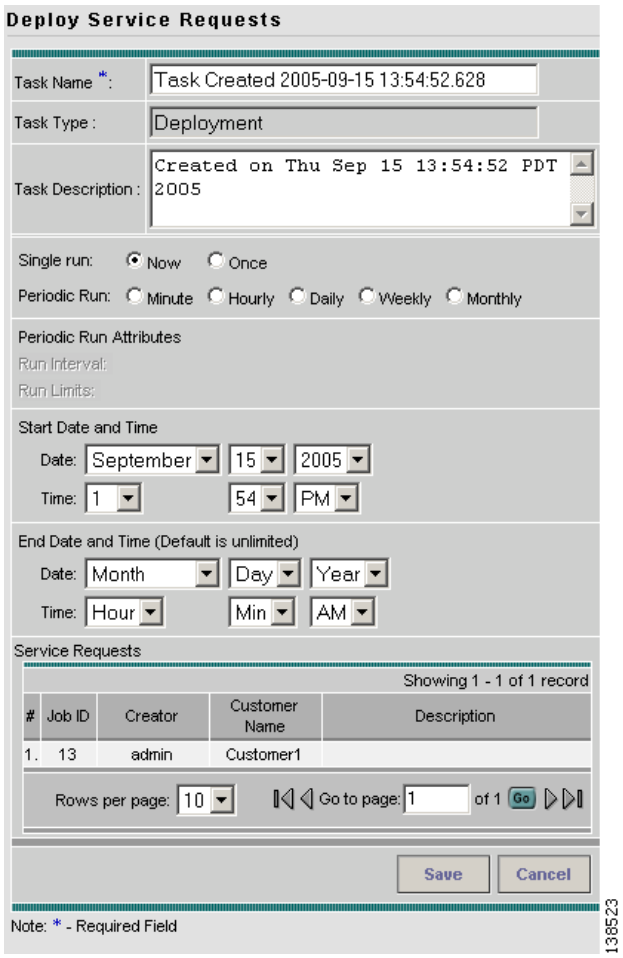
Step 3 Click **Deploy** and choose **Deploy** or **Force-Deploy**.

Use **Deploy** when the service request state is Requested or Invalid.

Use **Force Deploy** when the service request state is Deployed, Failed Deployed, or Failed Audit.

The Deploy Service Requests window appears as shown in Figure 12-3.

Figure 12-3 Schedule Service Activation



Step 4 Choose a schedule for the activation of the service.

Step 5 After you schedule the service request, click **Save**.

After you schedule the VPLS service request, you can monitor the service request that is being deployed. See Verifying L2VPN or VPLS Service Requests, page 12-4 and Monitoring Service Requests, page 12-11 for more information.

Verifying L2VPN or VPLS Service Requests

After you deploy an L2VPN or VPLS service request, you should verify that there were no errors.

You can verify an L2VPN or VPLS service request through the following:

- Transition state—The transition state of an L2VPN or VPLS service request is listed on the Service Requests window in the State column. See Service Request States, page 12-5 for more information.

- View service request details—From the Service Requests Details window, you can view the L2VPN or VPLS link endpoints and the L2VPN or VPLS configlets for this service request. See Viewing L2VPN or VPLS Service Request Details, page 12-7 for more information.
- Task Logs—Access the task logs from the Monitoring tab to help you troubleshoot a failed service request or to view more details about a service request. See Monitoring Service Requests, page 12-11 for more information.

Service Request States

A service request transition state describes the different stages a service request enters during the L2VPN or VPLS provisioning process.

For example, when you deploy an L2VPN or VPLS service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates an L2VPN or VPLS configlet. When the configlet is generated and downloaded to the device, the L2VPN or VPLS service request enters the **Pending** state. When the device is audited, the L2VPN or VPLS service request enters the **Deployed** state.

Figure 12-4 illustrates which service request states relate to the L2VPN or VPLS configuration auditing process, and which states relate to the provisioning process.

Figure 12-4 Service Requests States

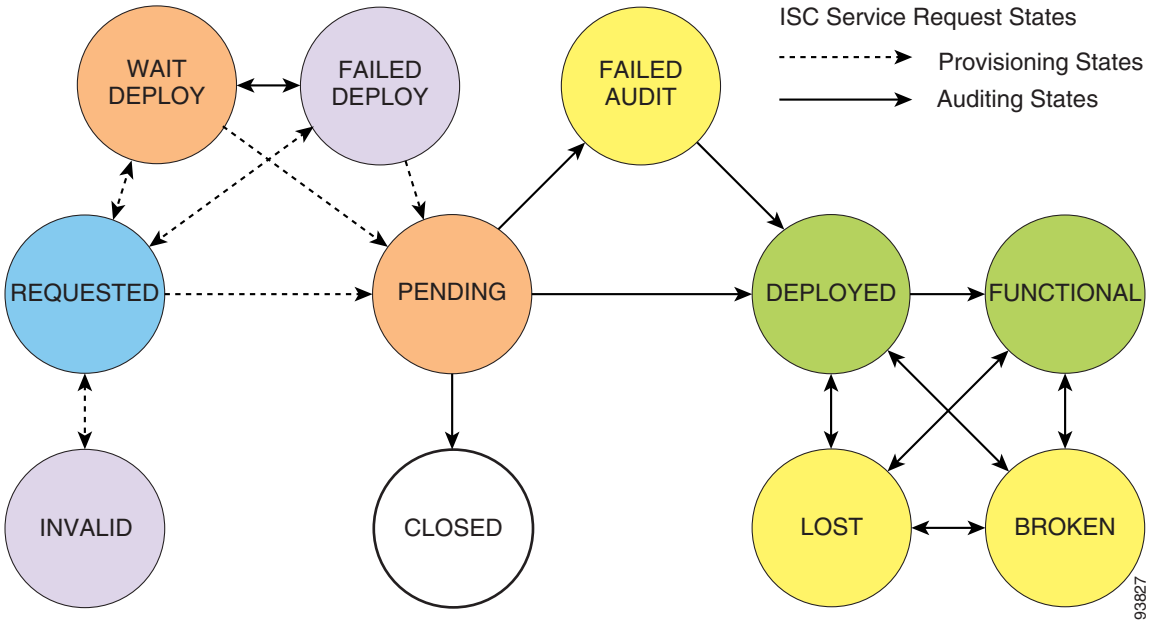


Table 12-1 describes the functions of each ISC service request state. They are listed in alphabetic order.

Table 12-1 Cisco IP Solution Center Service Request States

Service Request Type	Description
Broken (valid only for L2TPv3 and MPLS services)	The router is correctly configured but the service is unavailable (due to a broken cable or Layer 2 problem, for example). An MPLS service request moves to **Broken** if the auditor finds the routing and forwarding tables for this service, but they do not match the service intent.
Closed	A service request moves to **Closed** if the service request should no longer be used during the provisioning or auditing process. A service request moves to the **Closed** state only upon successful audit of a decommission service request. ISC does not remove a service request from the database to allow for extended auditing. Only a specific administrator purge action results in service requests being removed.
Deployed	A service request moves to **Deployed** if the intention of the service request is found in the router configuration file. **Deployed** indicates that the configuration file has been downloaded to the router, and the intent of the request has been verified at the configuration level. That is, ISC downloaded the configlets to the routers and the service request passed the audit process.
Failed Audit	This state indicates that ISC downloaded the configlet to the router successfully, but the service request did not pass the audit. Therefore, the service did not move to the **Deployed** state. The **Failed Audit** state is initiated from the **Pending** state. After a service request is deployed successfully, it cannot re-enter the **Failed Audit** state (except if the service request is redeployed).
Failed Deploy	The cause for a **Failed Deploy** status is that DCS reports that either the upload of the initial configuration file from the routers failed or the download of the configuration update to the routers failed (due to lost connection, faulty password, and so on).
Functional (valid only for L2TPv3 and MPLS services)	An MPLS service request moves to **Functional** when the auditor finds the VPN routing and forwarding tables (VRF) for this service and they match with the service intent. This state requires that both the configuration file audit and the routing audit are successful.
Invalid	**Invalid** indicates that the service request information is incorrect in some way. A service request moves to **Invalid** if the request was either internally inconsistent or not consistent with the rest of the existing network/router configurations (for example, no more interfaces were available on the router). The Provisioning Driver cannot generate configuration updates to service this request.
Lost	A service request moves to **Lost** when the Auditor cannot find a configuration-level verification of intent in the router configuration files. The service request was in the **Deployed** state, but now some or all router configuration information is missing. A service request can move to the **Lost** state *only* when the service request had been **Deployed**.

Table 12-1 Cisco IP Solution Center Service Request States (continued)

Service Request Type	Description
Pending	A service request moves to **Pending** when the Provisioning Driver determines that the request looks consistent and was able to generate the required configuration updates for this request. **Pending** indicates that the service request has generated the configuration updates and the configuration updates are successfully downloaded to the routers. The Auditor regards pending service requests as new requests and begins the audit. If the service has been freshly provisioned and not yet audited, it is not an error (pending audit). However, if an audit is performed and the service is still pending, it is in an error state.
Requested	If the service is newly entered and not yet deployed, it is not an error. However, if a Deploy is done and it remains **Requested**, the service is in an error state.
Wait Deploy	This service request state pertains only when downloading configlets to a Cisco CNS-CE server, such as a Cisco CNS IE2100 appliance. **Wait Deploy** indicates that the configlet has been generated, but it has not been downloaded to the Cisco CNS-CE server because the device is not currently online. The configlet is staged in the repository until such time as the Cisco CNS-CE server notifies ISC that it is up. Configlets in the **Wait Deploy** state are then downloaded to the Cisco CNS-CE server.

Viewing L2VPN or VPLS Service Request Details

The L2VPN or VPLS service request details include the link endpoints for the service request, the history, and the configlet generated during the service request deployment operation. Use the service request details to help you troubleshoot a problem or error with the service request or to check the L2VPN or VPLS commands in the configlet.

From the Service Request Details page, you can view more information about:

- Links—the link endpoint details
- History—Service request history report
- Audit—Audit reports for the link IDs
- Configlets—View the ISC generated configlet for the L2VPN or VPLS service request

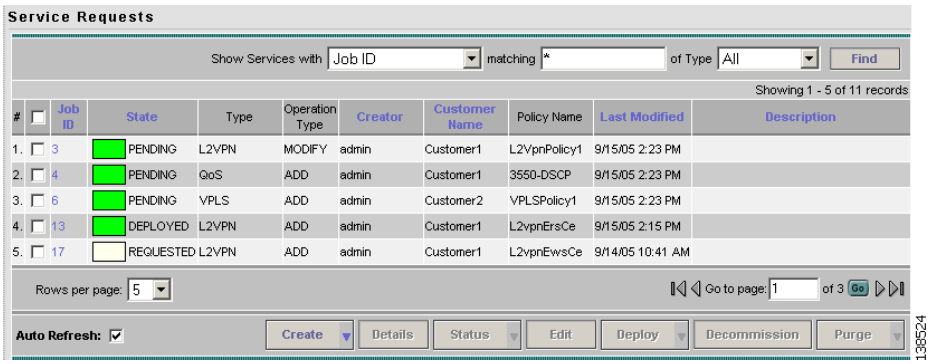
The following sections describe the links, history, and configlet details for an L2VPN or VPLS service request. The audit details are described in Auditing Service Requests, page 12-13.

To view L2VPN or VPLS service request details:

Step 1 Select **Service Inventory > Inventory and Connection Manager > Service Requests**.

The Service Requests window appears as shown in Figure 12-5.

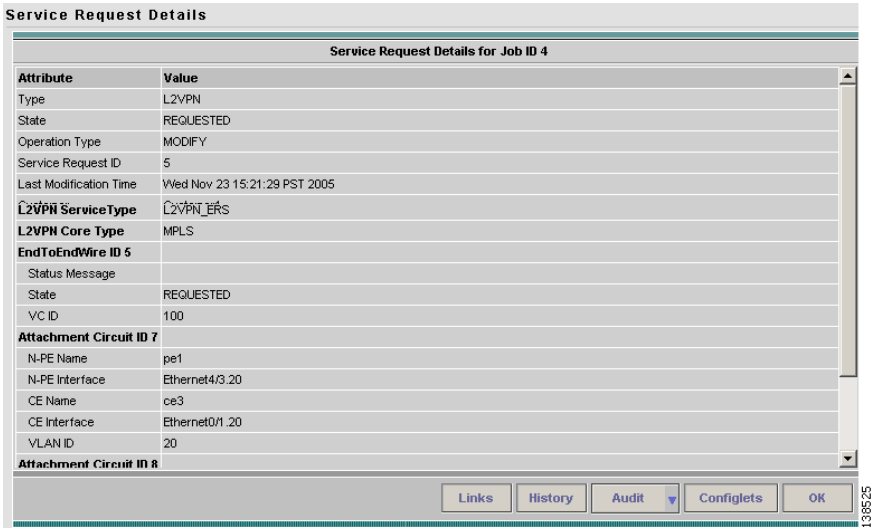
Figure 12-5 Service Requests Window



Step 2 Select the L2VPN, L2TPv3, or VPLS service request and click **Details**.

Step 3 The Service Request Details window appears (Figure 12-6).

Figure 12-6 Example Service Request Details Window



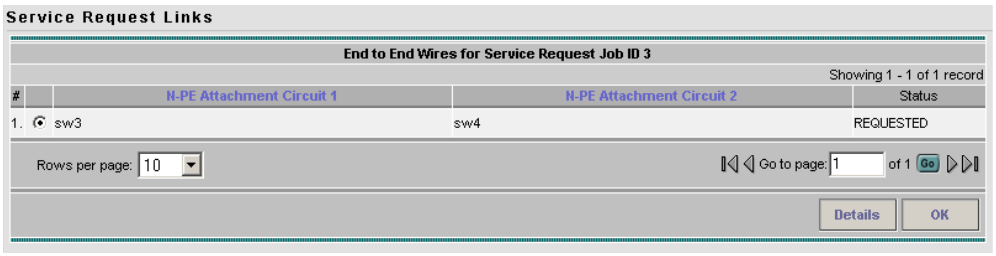
The service request attribute details include the type, transition state, operation type, ID, modification history, customer, and policy name.

Links

The service request link details include the link endpoints, PE secured interface, VLAN ID, and whether a CE is present.

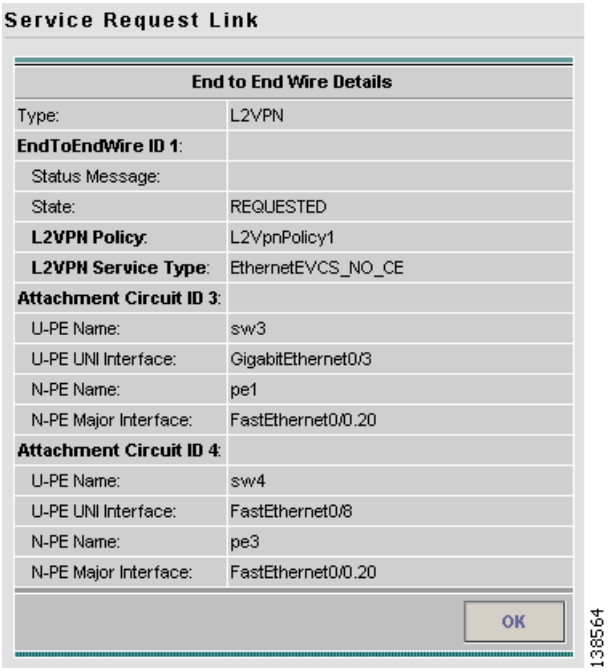
Step 1 Click **Links** on the Service Request Details window (see Figure 12-6). The Service Request Links window appears (Figure 12-7).

Figure 12-7 Service Request Links



Step 2 Choose a link and click **Details**. The Link Details window appears as shown in Figure 12-8.

Figure 12-8 Link Details Window



Step 3 Click **OK** to return to the Service Request Links window.

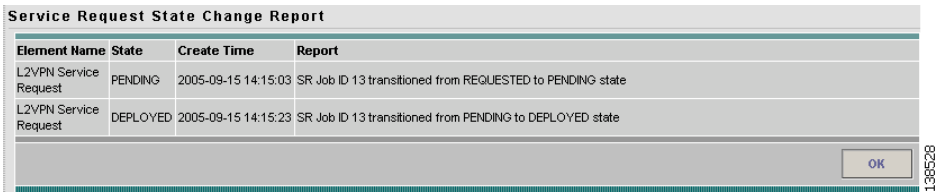
Step 4 Select another link to view or click **OK** to return to the Service Request Details window.

History

You can view history information about the service request.

Step 1 Click **History** on the Service Request Details window (see Figure 12-6). The Service Request State Change Report window appears (Figure 12-9).

Figure 12-9 Service Request State Change Report



The history reports lists the following information about the service request:

- Element Name—the device, interface, and subinterfaces participating in this service request
- State—the transition states the element has gone through
- Create Time—the time the element was created for this service request
- Report—the action taken by ISC for the element in this service request

Step 2 Click **OK** to return to the Service Request Details window.

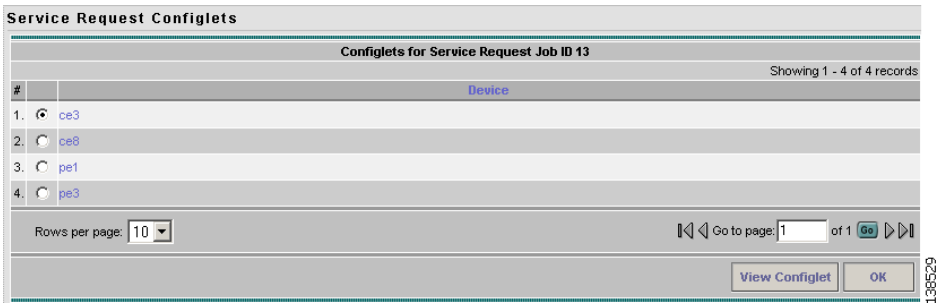
Configlets

After you deploy the service request, ISC generates Cisco IOS commands to turn on L2VPN or VPLS Services on all the network devices that participate in the service request.

To view the configlets that are generated, perform the following tasks.

Step 1 Click **Configlets** on the Service Request Details window (see Figure 12-6). You see a list of network devices for which a configlet was generated (see Figure 12-10).

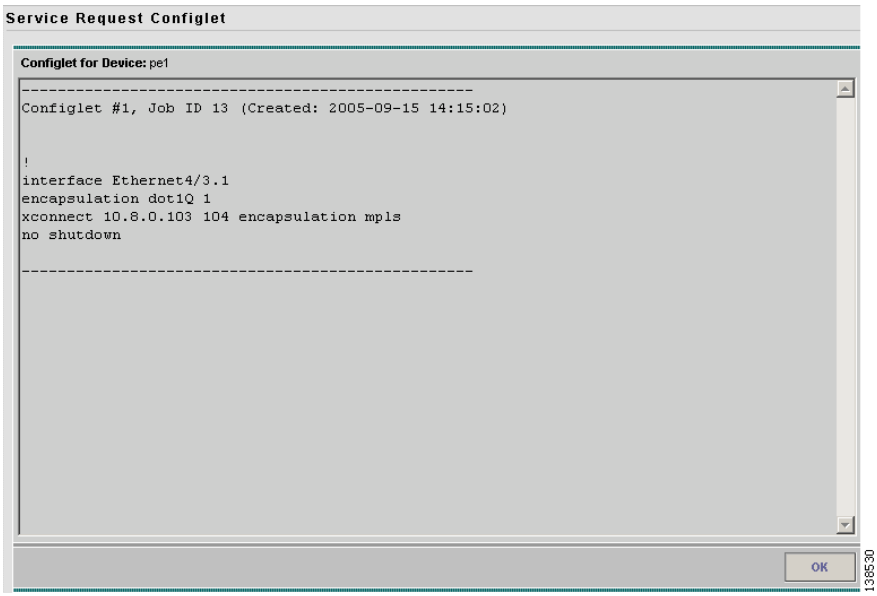
Figure 12-10 Service Request Configlets



Step 2 Select the device for which you want to view the configlet.

Step 3 Click **View Configle**t. The Configlet for Device window appears (Figure 12-11).

Figure 12-11 L2VPN, L2TPv3, or VPLS Configlet Example



The device configlet shows all commands downloaded to the device configuration during the service request deployment operation.

Step 4 Click **OK** to exit.

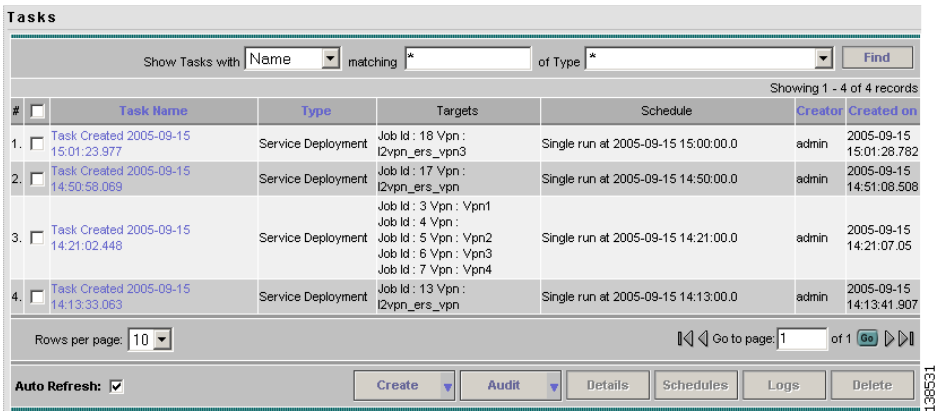
Monitoring Service Requests

To monitor an L2VPN or VPLS service request that is being deployed, you must use the task logs to help you troubleshoot why a service request has failed or to find more details about a service request.

Perform the following steps to monitor a service request.

Step 1 Select **Monitoring > Task Manager**. The Tasks window appears as shown in Figure 12-12.

Figure 12-12 Tasks Window

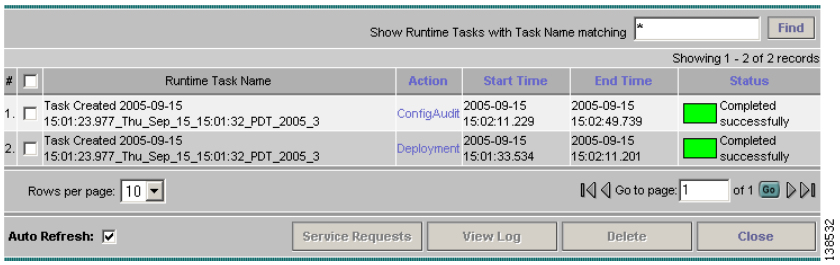


Step 2 Click **Find** to refresh the window.

The task that is executing will be the first in the list of tasks that being performed in ISC.

Step 3 Select the task you want to monitor and click **Logs**. The Task Logs window appears as shown in Figure 12-13.

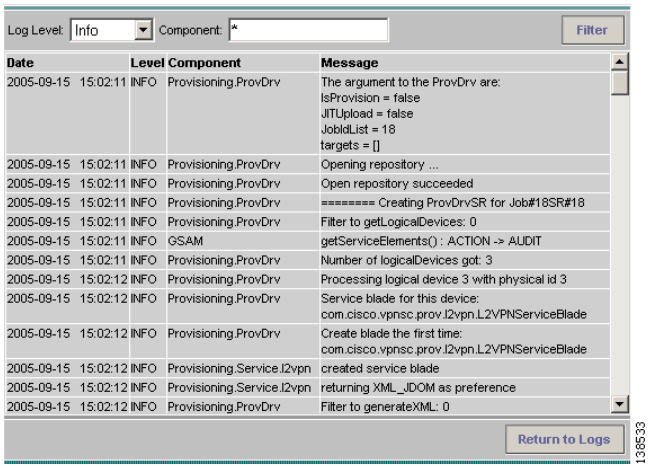
Figure 12-13 Task Logs



Step 4 Select the run-time task that you want to monitor and click **View Logs**.

A window like the one shown in Figure 12-14 appears.

Figure 12-14 Task Logs



Step 5 Select the log level from the drop-down list and click **Filter**. The log levels are All, Severe, Warning, Info, Config, Fine, Finer, and Finest.

Step 6 Click **Return to Logs**.

Step 7 Click **Close** in the Task Logs window.

Auditing Service Requests

Each time an L2VPN (including L2TPv3) or VPLS service request is deployed in the Cisco IP Solution Center (ISC), a configuration audit occurs. You can view the results of these in L2VPN or VPLS configuration audit reports. Use configuration audits and reports to verify that the network devices have the correct configuration for the services provided.

A functional audit is part of the post-provisioning check. It is only available for L2TPv3 service requests. It lets you validate the L2TPv3 circuit and session status. If the L2TPv3 wire state is functional, it indicates that traffic can be passed through successfully.

Note A functional audit can be performed only after a configuration audit is performed successfully on the service request.

Configuration Audit

A configuration audit occurs automatically each time you deploy an L2VPN or VPLS service request. During this configuration audit, ISC verifies that all Cisco IOS commands are present and that they have the correct syntax. An audit also verifies that there were no errors during deployment.

The configuration audit verifies the service request deployment by examining the commands configured by the L2VPN or VPLS service request on the target devices. If the device configuration does not match what is defined in the service request, the audit flags a warning and sets the service request to a **Failed Audit** or **Lost** state.

You can create audit reports for new or existing L2VPN or VPLS service requests.

- Audit new services—This type of audit is for service requests that have just been deployed. The audit identifies problems with the configuration files downloaded to the devices.
- Audit existing services—This type of audit checks and evaluates the configuration of deployed service requests to see if the service request is still in effect.

We recommend that you schedule a service request audit on a regular basis to verify the state of the network provisioning requests.

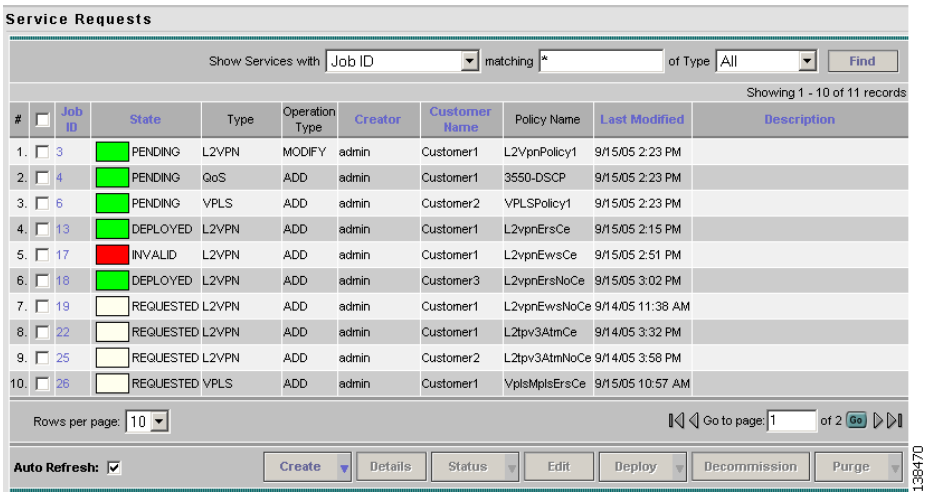
This section describes how to manually generate a configuration audit and view the audit report.

To view a configuration audit report perform the following steps.

Step 1 Select **Service Inventory > Inventory and Connection Manager > Service Requests**.

The Service Requests window appears as shown in Figure 12-15.

Figure 12-15 Service Requests Window

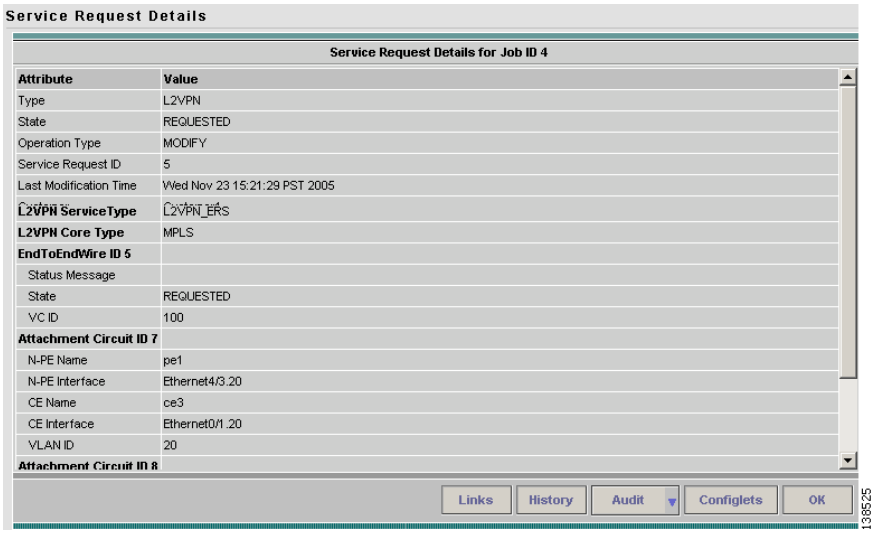


Step 2 Select an L2VPN or VPLS service request for the configuration audit.

Step 3 Click **Details**.

The Service Request Details window appears as shown in Figure 12-16.

Figure 12-16 Service Request Details

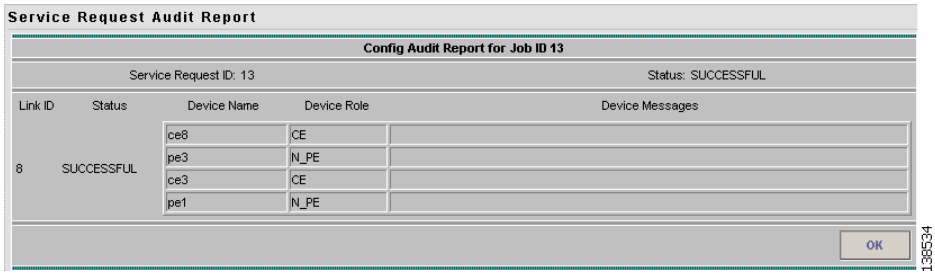


Step 4 Click **Audit**.

Step 5 Click **Config.**

The Service Request Audit window appears. Figure 12-17 shows an example of a successful configuration audit.

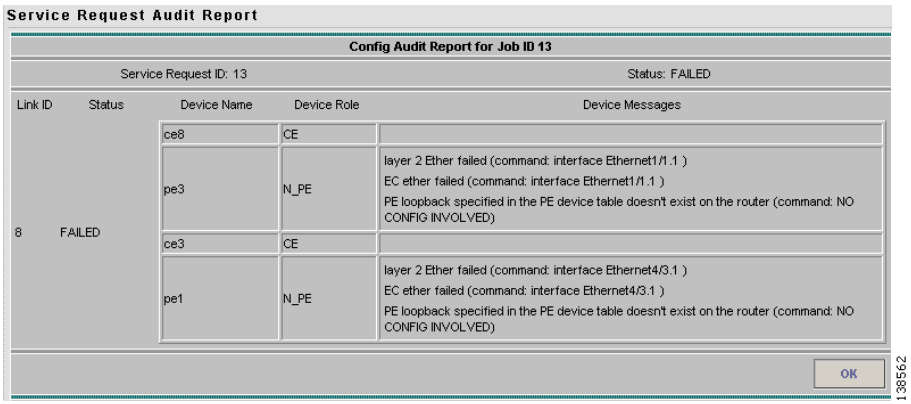
Figure 12-17 Service Request Audit Report—Successful



This window lists the device name and role, and a message regarding the status of your configuration audit.

If the audit is unsuccessful, the message field lists details on the failed audit. Figure 12-18 shows an example of a failed audit message for an L2VPN or VPLS service request.

Figure 12-18 Service Request Audit Report—Failed



The audit failure message indicates missing commands and configuration issues. Carefully review the information in the message field. If the audit fails, you must correct all errors and redeploy the service request.

Step 6 Click **OK** to return to the Service Request Details window.

Functional Audit

A functional audit verifies that the links in a service request or VPN are working correctly. The audit checks that the circuit and session between two PEs are set up correctly to pass traffic through.

Note Functional audits are performed by ISC for only L2TPv3 service requests.

Performing a Functional Audit

You perform a functional audit after a configuration audit is performed successfully. You can perform a functional audit on service requests that have states in either deployed, functional, or broken. Wait at least two minutes after a service is deployed to allow time for the circuit and session to be established. If you prematurely perform a functional audit action, a broken service request state will be the result because the session is not established yet.

To perform a functional audit, follow these steps.

Step 1 Select **Service Inventory > Inventory and Connection Manager > Service Requests**.

Step 2 Select a service request.

Step 3 Click **Details**.

On the service request details page, the **Audit** button has two choices:

- **Config**
- **Functional**

Step 4 Click **Functional** to display the Functional audit report.

Creating a Task to Perform a Functional Audit

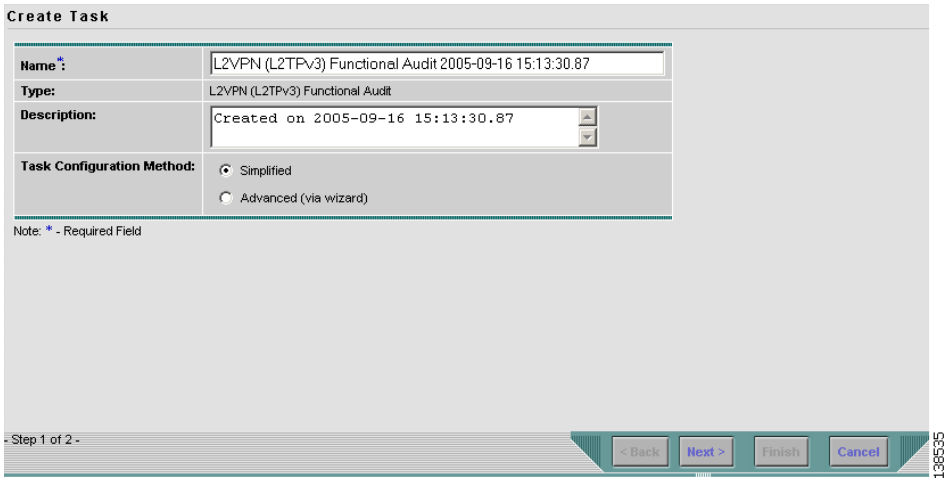
You can create a task to do a functional audit for one or more L2TPv3 service requests. To create a task to do a functional audit, perform the following steps.

Step 1 Select **Monitoring > Task Manager > Tasks.**

Step 2 Click **Audit**

Step 3 Choose **L2VPN (L2TPv3) Functional Audit** from the drop-down list. The create task window appears as shown in Figure 12-19.

Figure 12-19 Create Task



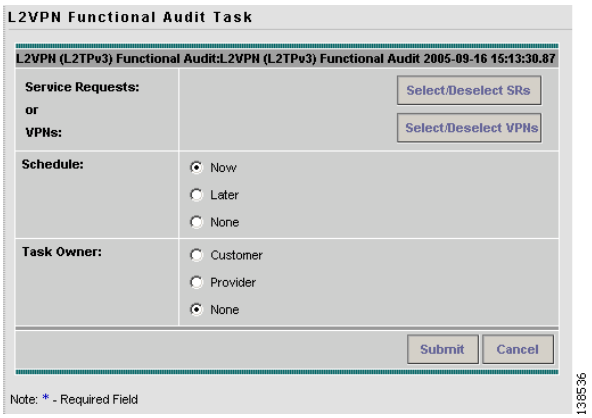
Step 4 Select a Task Configuration method. The choices are:

- **Simplified**
- **Advanced** (via wizard)

Step 5 Click **Next**.

The L2VPN Functional Audit Task window appears as shown in Figure 12-20.

Figure 12-20 L2VPN Functional Audit Task



Step 6 Click the **Select/Deselect SRs** button to select one or more service requests in Deployed, Functional, or Broken states as the targets for the task.

You can select a VPN to audit. If you select a VPN to audit, all the links that form the VPN are audited.

Note You can select either service request(s) or VPN(s) in one task, but you cannot select both in the same task.

Step 7 You can choose to schedule now or later.

Step 8 You can choose an owner for the task.

Step 9 Click **Submit**.

Step 10 You receive a Service Request Audit Report. The service request state is set to Functional if all the end-to-end wires pass the functional audit and Broken if any one of them is broken.

Why a Functional Audit Could Fail

A Functional Audit could fail for the following reasons:

- No session was found for an end-to-end wire.
- A session is not established yet.
- A UNI involved in an end-to-end wire is down.

You can also use the task logs to help you troubleshoot why a service request has failed or to find more details about a service request. It is possible to set the types of log level you want to view. Specify the Log Level and click the **Filter** button to view that information you want to view. See Monitoring Service Requests, page 12-11, for more information.