Setting Up the Network

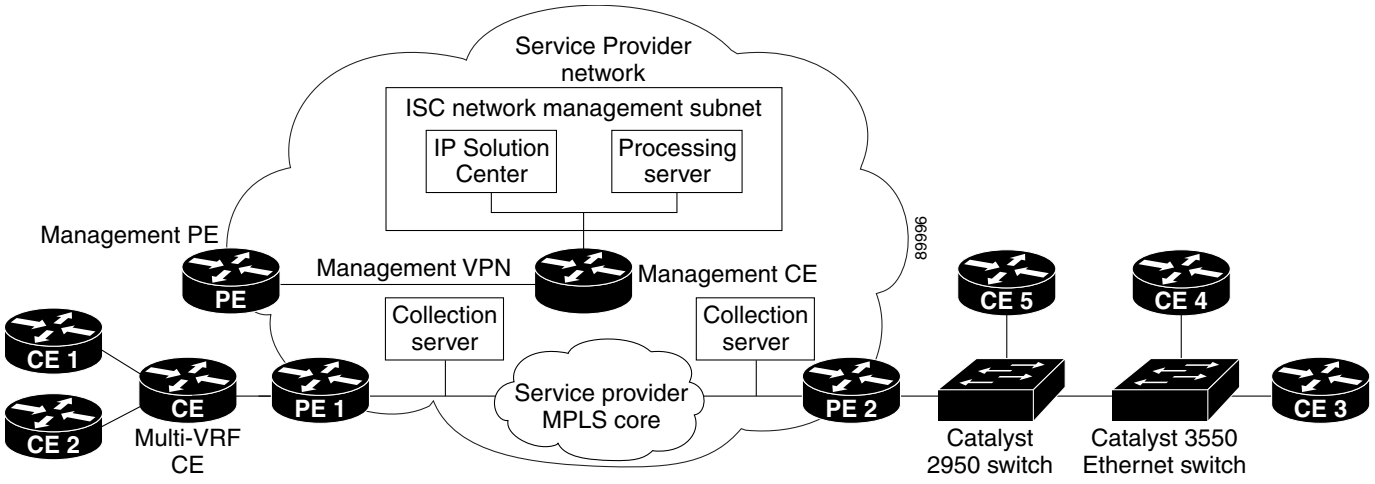
The Cisco IP Solution Center (ISC) MPLS VPN Management feature is an MPLS VPN provisioning and auditing tool. It focuses on the provider edge routers (PEs), customer edge routers (CEs), and the link between them. ISC can use either a Telnet gateway or Cisco Configuration Center software to transport configuration file information to and from target routers. Additional features include Class of Service (CoS) provisioning, VPN-aware NetFlow traffic profiling, and Service Level Agreement (SLA) monitoring.

ISC also provides external access to its provisioning, traffic profiling, and SLA monitoring features through CORBA/XML APIs.

In an MPLS network, a customer edge router (CE) is connected to a provider edge router (PE) in such a way that the customer's traffic is encapsulated and transparently sent to other CEs, thus creating a virtual private network. The Cisco ISC provisioning engine for MPLS accesses the configuration files on both the CE and PE to compute the necessary changes to the configuration files to support the service on the PE-CE link.

As shown in Figure A-1, Cisco requires that the Cisco ISC software is installed on its own dedicated system. The Cisco ISC workstation is optionally connected on a LAN to one or more Processing servers and Collection servers.

Figure A-1 Cisco ISC: MPLS VPN Management in the Service Provider Network



The principal Cisco ISC network elements are as follows:

- *ISC Network Management Subnet*

The *ISC Network Management Subnet* is required when the service provider's service offering entails the management of CEs. The management subnet consists of the IP Solution Center workstation where ISC is installed on a Sun Solaris 8 system. On the same LAN, the service provider can optionally install one or more Processing servers.

The Processing servers are responsible for executing tasks such as provisioning, auditing, SLA data collection, and so on. There can be one or more Processing server machines.

- *The Management VPN*

  The Management VPN is a special VPN employed by the ISC Network Management Subnet to manage the CEs in a service provider network. Once a CE is in a VPN, it is no longer accessible by means of conventional IPv4 routing, unless the CEs are part of the Management VPN. To communicate with the PEs, the link between the Management PE (MPE) and the Management-CE (MCE) uses a parallel IPv4 link. The Management VPN connects to the managed CEs.

- *Multi-VRF CE*

  The Multi-VRF CE is a feature that provides for Layer 3 aggregation. Multiple CEs can connect to a single Multi-VRF CE (typically in an enterprise network); then the Multi-VRF CE connects directly to a PE. Figure A-1 shows CE 1 and CE2 connected to the Multi-VRF CE, and the Multi-VRF CE is connected directly to the PE. For details, see Multi-VRF CE, page 1-18.

- *Layer 2 Access to MPLS VPNs*

  The service provider can install multiple Layer 2 switches between a PE and CE, as shown in Figure A-1. This feature provides Layer 2 aggregation. Additional CEs can be connected to the switches as well. Cisco supports two switches for the Layer 2 access to MPLS: either a Cisco Catalyst 2950 Switch or a Cisco Catalyst 3550 Intelligent Ethernet Switch.

- *Collection Servers*

  Cisco ISC is designed to provision a large number of devices through its distributed architecture. If the Master server (equivalent to the ISC workstation) cannot keep up with the number of devices, Collection servers can be added to off load the work of the Master server. Among other tasks, Collection servers are responsible for uploading and downloading configuration files to and from Cisco routers. For more information, see Defining Collection Zones and Assigning Devices to Zones, page A-12.

Tasks to Be Completed Before Using ISC Software

Before you use Cisco ISC: MPLS VPN Management software to provision an MPLS network, the Service Provider must complete the following tasks:

1. IPv4 connectivity must be operational among all the routers in the MPLS VPN network before provisioning can take place.
2. The Service Provider or Customer must create a loopback interface on each router.
3. Each router must have a routable IP address.
4. Optionally, you can set up the Secure Shell (SSH) on the CE routers (see the next section for details).
5. Set up SNMP on all the edge routers in the network—see the Setting Up SNMPv1 and SNMPv2 on the Routers in the Service Provider Network, page A-4 and the Setting the SNMPv3 Parameters on the Routers in the Service Provider Network, page A-5.
6. Enable SA Agent on all edge devices that you want to collect SLA data from—see Enabling SA Agent on Edge Routers for SLA Jitter Probes, page A-7.

7. If you choose to use TFTP (Trivial File Transfer Protocol) as the default configuration transport method, you must enable TFTP on the Cisco ISC workstation—see Enabling TFTP in Cisco ISC, page A-8.
8. If you are installing and using Collection servers, complete the procedures described in Defining Collection Zones and Assigning Devices to Zones, page A-12.
9. If you are using terminal servers to access routers in the network, you must enable at least as many Telnet sessions on the terminal server as there are terminal server ports. For details, see Enabling Telnet Sessions for Terminal Server Ports, page A-8.

Caution Make sure that the file descriptor limit is *not* set in the Cisco ISC workstation login shell file (which can be the *.login* file, the *.cshrc* file, or the *.kshrc* file). If the login shell file contains a line with the **ulimit -n** command (for example, "`ulimit -n <number>`"), comment out this command line in the file.

Cisco ISC cannot override the file descriptor limitation setting in the login shell file. If the value is set incorrectly, Cisco ISC may experience operational problems.

Configuring Devices in the ISC MPLS Environment

This section describes the tasks the Service Provider should complete to set up devices in the Cisco IP Solution Center MPLS environment.

Setting Up the Secure Shell (SSH) on Edge Routers

Service providers need a mechanism to deploy VPN configuration files to remote edge routers in a secure manner. The basic requirements for secured management are as follows:

- The edge device routers and Cisco ISC must be able to authenticate each other.
- An encrypted channel for uploading and downloading router configuration information must be in place.

Cisco ISC uses TGS as the configuration file download mechanism. One of the modes that TGS can operate in is *Secure Shell (SSH) mode*. The Telnet Gateway Server uses SSH for both authentication and encryption. In this scheme, the edge device router functions as an SSH server, while Cisco ISC functions as the SSH client.

Note This configuration procedure assumes that the router's authentication database is stored locally on the router and not on a TACACS (Terminal Access Controller Access Control System) server.

The procedure for configuring SSH on edge device routers is as follows:

	Command	Description
Step 1	`Router#` **configure terminal**	Enter global configuration mode.
Step 2	`Router(config)#` **ip domain-name** *domain_name*	Specify the IP domain name.

	Command	Description

Step 3	`Router(config)# crypto key generate rsa`	Generate keys for the SSH session.
		The **crypto key generate rsa** command is interactive. You will see the following prompt:
		`Choose the size of the key modulus in the range of 360 to 2048 for your general purpose keys.`
		`How many bits in the modulus (nnn):`

Step 4		Press **Enter** to accept the default number of bits.
Step 5	`Router(config)# username` *username* `password` *password*	Configure the user ID and password. Enter the ISC workstation username and password you are logged in as. For example, **username admin password isc**.
Step 6	`Router(config)# line vty 0 4`	Enable SSH as part of the vty login transport.
Step 7	`Router(config-line)# login local`	The **login** command can take either **local** or **tacacs** as its value. This command indicates that the router stores the authentication information locally.
Step 8	`Router(config-line)# transport input telnet ssh`	
Step 9	`Router(config-line)# Ctrl+Z`	Return to Privileged Exec mode.
Step 10	`Router# copy running startup`	Save the configuration changes to NVRAM.

Setting Up SNMPv1 and SNMPv2 on the Routers in the Service Provider Network

The Simple Network Management Protocol (SNMP) must be configured on each router and edge device in the service provider network. To determine whether SNMP is enabled and to set the SNMP community strings on a router, execute the following steps for each router.

	Command	Description
Step 1	> **telnet** *router_name*	Telnet to the router you want to configure.
Step 2	`Router>` **enable** `Router>` *enable_password*	Enter enable mode, then enter the enable password.
Step 3	`Router#` **show snmp**	Check the output of the **show snmp** command to see whether the following statement is present: "*SNMP agent not enabled.*" If SNMP is not enabled, complete the steps in this procedure.
Step 4	`Router#` **configure terminal**	Enter global configuration mode.
Step 5	`Router(config)# snmp-server community` *userstring* **RO**	Set the community read-only string.

	Command	Description
Step 6	`Router(config)# snmp-server community` *userstring* `RW`	Set the community read-write string.
Step 7	`Router(config)# Ctrl+Z`	Return to Privileged Exec mode.
Step 8	`Router# copy running startup`	Save the configuration changes to NVRAM.

Tip The SNMP strings defined in the Cisco ISC for each target device must be identical with those configured for the corresponding edge devices in the service provider network.

Setting the SNMPv3 Parameters on the Routers in the Service Provider Network

Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

This section describes how to set the SNMPv3 parameters on the routers in the service provider network. To complete the task regarding SNMPv3 parameters, you also must set a selected set of parameters in the Cisco ISC software. The SNMPv3 parameters you set on the routers must match the SNMPv3 parameters you specify in the Cisco ISC software.

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensuring that a packet has not been tampered with in-transit.
- Authentication—Determining the message is from a valid source.
- Encryption—Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

Using SNMPv3, data can be collected securely from SNMP devices without fear of the data being tampered with or corrupted. Also, using the **SNMP Set** command, packets that change a router's configuration can be encrypted to prevent its contents from being exposed on the network.

SNMPv3 provides for both security models and security levels. A *security model* is an authentication strategy that is set up for a user and the group in which the user resides. A *security level* is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3.

Table A-1 identifies the combinations of security models and levels.

Table A-1 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.

Table A-1 SNMP Security Models and Levels (continued)

Model	Level	Authentication	Encryption	What Happens
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

SNMPv3 objects have the following characteristics:

- Each user belongs to a group.
- A group defines the access policy for a set of users.
- An access policy is what SNMP objects can be accessed for reading, writing, and creating.
- A group determines the list of notifications its users can receive.
- A group also defines the security model and security level for its users.

To check the existing SNMP configuration, use these commands:

- **show snmp group**
- **show snmp user**

To set the SNMPv3 *server group* and *server users* parameters on a router, execute the following steps:

	Command	Description
Step 1	> **telnet** *router_name*	Telnet to the router you want to configure.
Step 2	`Router>` **enable** `Router>` *enable_password*	Enter enable mode, then enter the enable password.
Step 3	`Router#` **configure terminal**	Enter global configuration mode.
Step 4	`Router(config)#` **snmp-server group** [*groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}] [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	The **snmp-server group** command configures a new SNMP group or a table that maps SNMP users to SNMP views. Each group belongs to a specific security level. Example: **`snmp-server group v3auth v3 auth read v1default write v1default`**
Step 5	`Router(config)#` **snmp-server user** *username* [*groupname* **remote** *ip-address* [**udp-port** *port*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {md5 | **sha**} *auth-password* [**priv des56** *priv-password*]] [**access** *access-list*]	`The` **snmp-server user** command configures a new user to an SNMP group. Example: **`snmp-server user user1 v3auth v3 auth md5 user1Pass`**
Step 6	`Router(config)#` **`Ctrl+Z`**	Return to Privileged Exec mode.
Step 7	`Router#` **`copy running startup`**	Save the configuration changes to NVRAM.

Enabling SA Agent on Edge Routers for SLA Jitter Probes

If you want to use the (voice) jitter protocol to collect SLA data from the edge devices in your network, you must enable SA Agent on each device from which you want to collect this data.

This procedure assumes that you have already enabled SNMP and set the SNMP parameters on the edge device router, as described in the previous sections of this chapter.

To enable SA Agent on an edge router for jitter probes, execute the following steps:

	Command	Description
Step 1	> **telnet** *router_name*	Telnet to the router you want to configure.
Step 2	`Router>` **enable** `Router>` *enable_password*	Enter enable mode, then enter the enable password.
Step 3	`Router#` **configure terminal**	Enter global configuration mode.
Step 4	`Router(config)#` **rtr responder**	Enable SA Agent on the SLA probe's target router.
Step 5	`Router(config)#` **Ctrl+Z**	Return to Privileged Exec mode.
Step 6	`Router#` **copy running startup**	Save the configuration changes to NVRAM.

Enabling Telnet Sessions for Terminal Server Ports

You must enable at least as many Telnet sessions on the terminal server as there are terminal server ports. Otherwise, concurrent access to all the routers via the terminal server may fail.

To enable the appropriate number of Telnet sessions for terminal server access, follow these steps:

	Command	Description
Step 1	> **telnet** *terminal_server_name*	Telnet to the terminal server.
Step 2	`Terminalserver>` **enable** `Terminalserver>` *enable_password*	Enter enable mode, then enter the enable password.
Step 3	`Terminalserver#` **configure terminal**	Enter global configuration mode.
Step 4	`Terminalserver(config)#` **`line vty 0 31`**	Set the number of Telnet sessions to the number of available ports on the terminal server. This example sets 32 Telnet sessions.
Step 5	`Terminalserver(config)#` **`Ctrl+Z`**	Return to Privileged Exec mode.
Step 6	`Terminalserver#` **`copy running startup`**	Save the configuration changes to NVRAM.

Time Zone Support in ISC

ISC supports only the time zones that are in the */usr/share/lib/zoneinfo* directory of the Solaris workstation on which the ISC software is installed. The contents of this directory could change with each version of Solaris.

ISC cannot change the manner in which these time zones are configured, most notably the variations in Daylight Savings Time.

Note ISC does not support custom time zones.

Setting Up the ISC Workstation

This section describes the elements or components you should set up on the Cisco ISC workstation.

Enabling TFTP in Cisco ISC

The Cisco ISC software in MPLS mode is set by default to use Telnet as the mechanism to transport configuration files to and from routers. To set Cisco ISC software to use the Trivial File Transfer Protocol (TFTP) instead, edit the Hosts Configuration GTL device-config-access protocol property as described in this section. ISC properties are defined in the Dynamic Component Properties Library (DCPL).

Changing this value sets the default upload and download mechanism for all the devices configured to use the default for the Terminal Session Protocol and the Configuration Access Protocol.

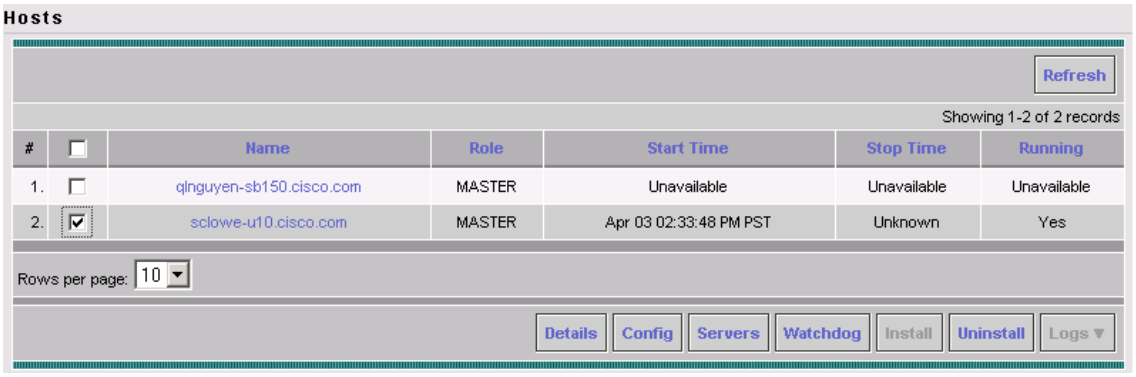
Step 1 Log into Cisco ISC.

Step 2 From the Welcome to ISC window, choose **Administration**.

Step 3 From the Administration window, choose **Control Center**.

The Hosts window appears (see Figure A-2).

Figure A-2 Selecting the ISC Host



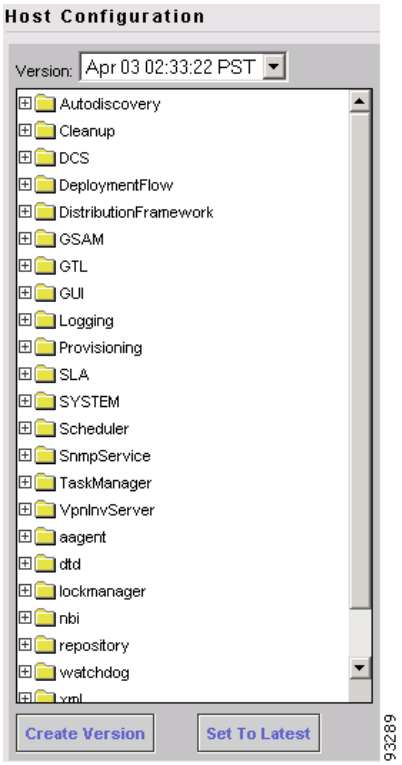
The Hosts window lists the hosts and servers that are managed by ISC.

Step 4 In the check box next to the host name, select the name of the ISC workstation.

Step 5 Click **Config**.

The Hosts Configuration window appears (see Figure A-3).

Figure A-3 Hosts Configuration Window



Step 6 Locate the **GTL** (Generic Transport Layer) folder, then click to expand it.

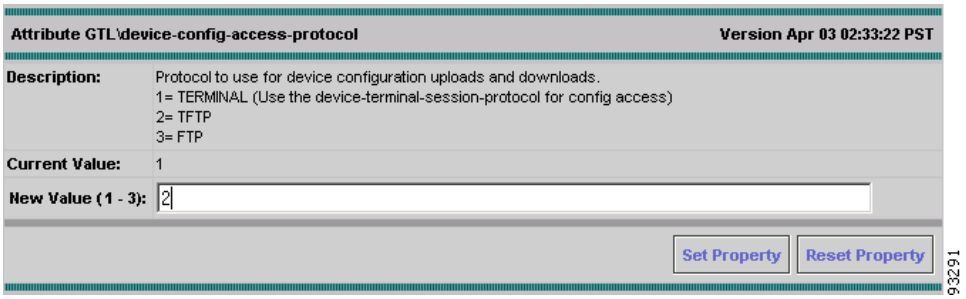
Figure A-4 shows the expanded GTL folder displaying the list of GTL options.

Figure A-4 GTL Options

Step 7 Select **device-config-access-protocol**.

The GTL Attributes dialog box for the device access protocol appears (see Figure A-5).

Figure A-5 Specifying the Device Access Protocol



As you can see from the Description area, the numeral **2** corresponds to **TFTP**.

Step 8 In the *New Value* field, enter the numeral **2**.

Step 9 Click **Set Property**.

Proceed to the next section to define the ISC workstation as a TFTP server.

Setting the ISC Host as a TFTP Server

This section describes how to set up a local Solaris host as a TFTP server. If the ISC Network Management Subnet includes one or more Collection or Processing servers, you must set up the Cisco ISC workstation as a TFTP host.

To set up the ISC workstation as a TFTP server:

Step 1 From the Welcome to ISC window, choose **Administration**.

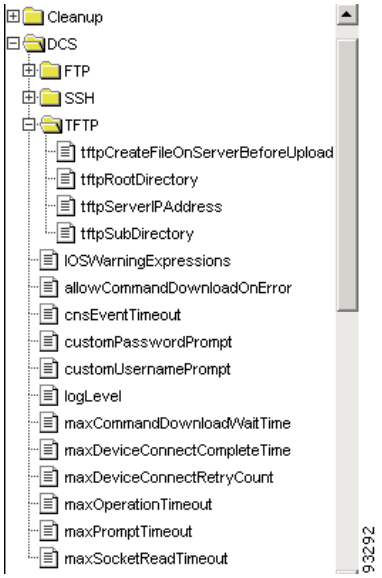
Step 2 From the Administration window, choose **Control Center**.

The Hosts window appears (see Figure A-2 on page A-9).

Step 3 Locate the **DCS** (Device Configuration Service) folder, then click the folder to expand it.

Figure A-6 shows the expanded DCS folder displaying the list of TFTP options.

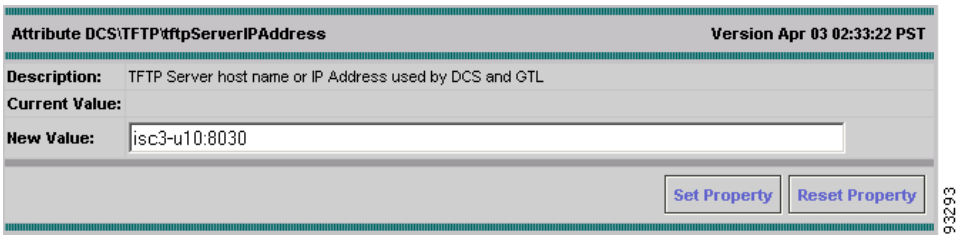
Figure A-6 TFTP Options



Step 4 Select **tfpServerIPAddress**.

The TFTP Server IP Address Attributes dialog box appears (see Figure A-7).

Figure A-7 Specifying the Host as a TFTP Server



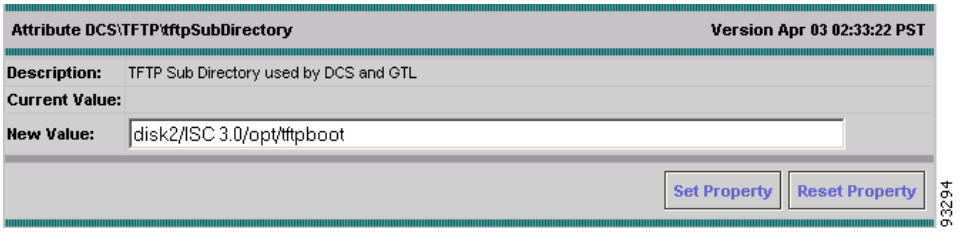
Step 5 In the *New Value* field, enter the host name or the IP address of the ISC workstation.

Step 6 Click **Set Property**.

Step 7 From the list of TFTP options, select **tftpSubDirectory**.

The TFTP Subdirectory dialog box appears (see Figure A-8).

Figure A-8 Specifying the Directory for the TFTP Server



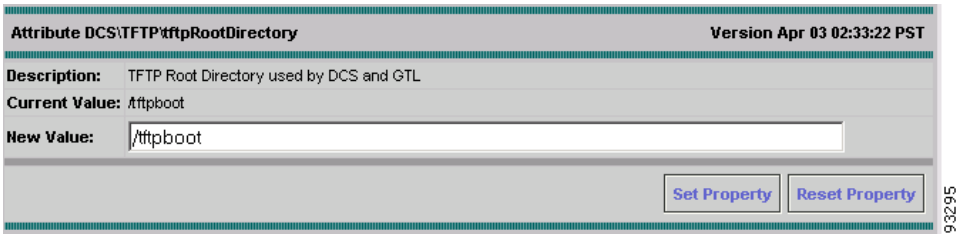
Step 8 In the *New Value* field, enter the location of the directory for TFTP server.

Step 9 Click **Set Property**.

Step 10 From the list of TFTP options, select **tftpRootDirectory**.

The TFTP Root Directory dialog box appears (see Figure A-9).

Figure A-9 Specifying the TFTP Root Directory



Step 11 In the *New Value* field, enter the location of the TFTP root directory.

Step 12 Click **Set Property**.

Step 13 From the ISC workstation, at the command line, stop the WatchDog by typing **stopwd -y**.

Step 14 To enable these changes, restart the WatchDog (**startwd**).

Step 15 Restart ISC.

Defining Collection Zones and Assigning Devices to Zones

ISC is designed to provision a large number of devices through its distributed architecture. If the Master server (equivalent to the ISC workstation) cannot keep up with the number of devices, Collection servers can be added to off load the work of the Master server.

Since Collection servers communicate a great deal with the network devices (for example, uploading and downloading configuration files to Cisco routers is handled through a Collection server), it makes sense to place Collection servers in a LAN near the routers, instead of placing the Collection server in the ISC network management subnet of the Master server.

Network devices are associated with collection servers by means of *collection zones*. A collection zone is a geographical grouping of devices that are served by a single Collection server. Each collection zone is associated with exactly one Collection server that collects data from each device. However, a Collection server can service multiple collection zones. For example, you may initially create several collection zones and have all of them serviced by the Master server. As the number of devices in each zone grows you can install additional Collection servers and assign some of the zones to them.

For information on installing a Collection server in ISC, see “Installing ISC” in Chapter 2, “Installing and Logging Into ISC” in the *Cisco IP Solution Center Installation Guide*.

The recommended sequence for setting up collection zones in ISC is as follows:

1. Examine your network to determine the optional set of collection zones.
2. Create the collection zones that are optimal for your network.
3. Create the network devices in ISC.
4. Assign each network device to the appropriate collection zone.

Defining Collection Zones

To define collection zones in ISC, follow these steps:

Step 1 Log into Cisco ISC.

Step 2 From the Welcome to ISC window, choose **Administration**.

Step 3 From the Administration window, choose **Control Center**.

The Hosts dialog box appears, along with the Hosts table of contents (TOC), as shown in Figure A-10.

Figure A-10 Collection Zones Option in Hosts TOC

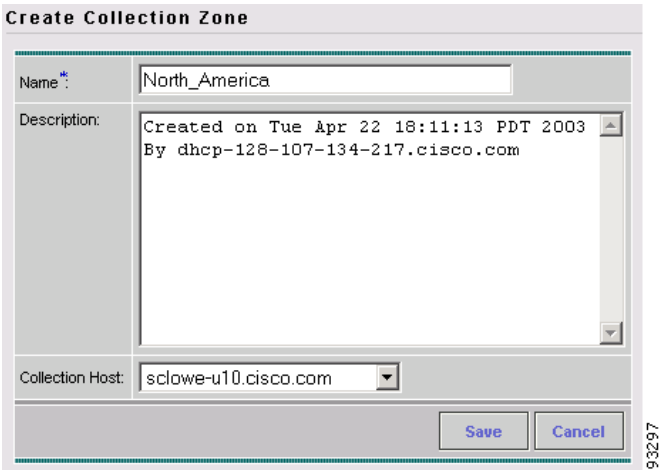
Step 4 From the Hosts TOC, choose **Collection Zones**.

The Collection Zones dialog box is displayed.

Step 5 Click **Create**.

The Create Collection Zone dialog box appears (see Figure A-11).

Figure A-11 Creating a Collection Zone

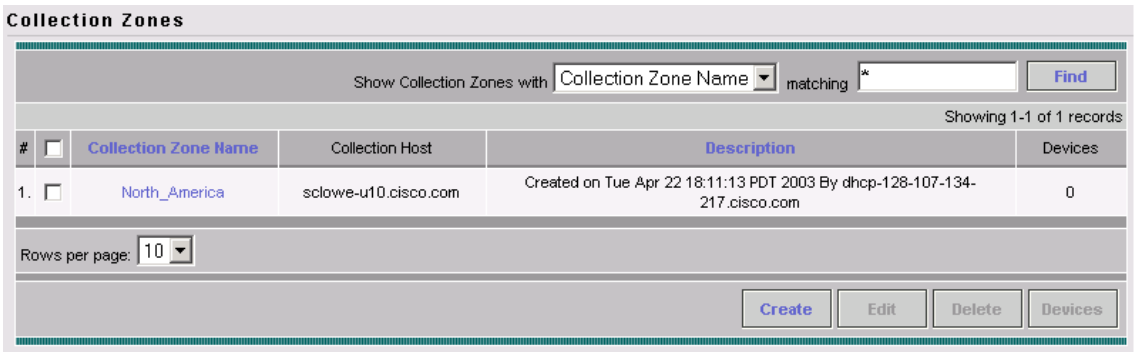


Step 6 Enter the name of the collection zone.

Step 7 From the *Collection Host* drop-down list, select the name of the Collection server, then click **Save**.

You return to the Collection Zones dialog box, where the new collection zone name and its attributes are displayed (see Figure A-12).

Figure A-12 Collection Zone Created



Step 8 Repeat this procedure for any additional collection zones you need to define for your network.

Assigning Devices to a Collection Zone

After you have defined all the collection zones that are necessary for your network, you must assign the set of geographically related network devices to the appropriate collection zone.

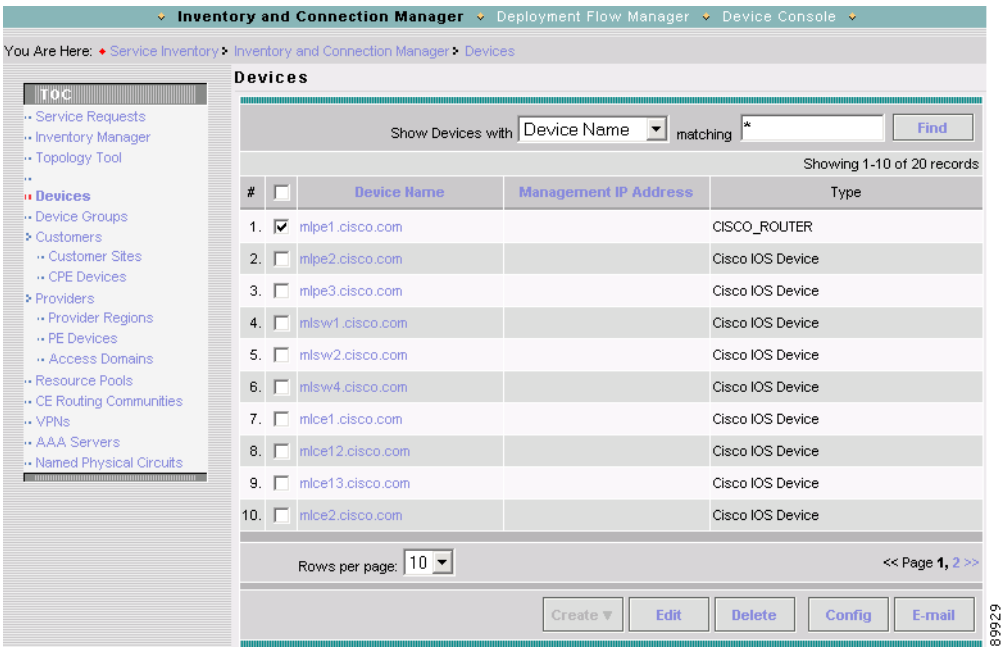
To assign devices to a collection zone:

Step 1 Choose **Service Inventory**, then choose **Inventory and Connection Manager**.

Step 2 From the Inventory and Connection Manager window, choose **Devices**.

The Devices dialog box appears (see Figure A-13).

Figure A-13 List of Devices Recognized by ISC



Step 3 Click the name of the device that you want to assign to a collection zone.

The Edit Cisco IOS Devices dialog box appears (see Figure A-14).

Figure A-14 Specifying the Collection Zone for a Device

Step 4 From the *Collection Zone* drop-down list, specify the appropriate collection zone for the selected device, then click **Save**.

Step 5 Repeat this procedure for each device to be assigned to a collection zone.

Seeing the Devices Assigned to a Collection Zone

To see the list of network devices assigned to a specific collection zone:

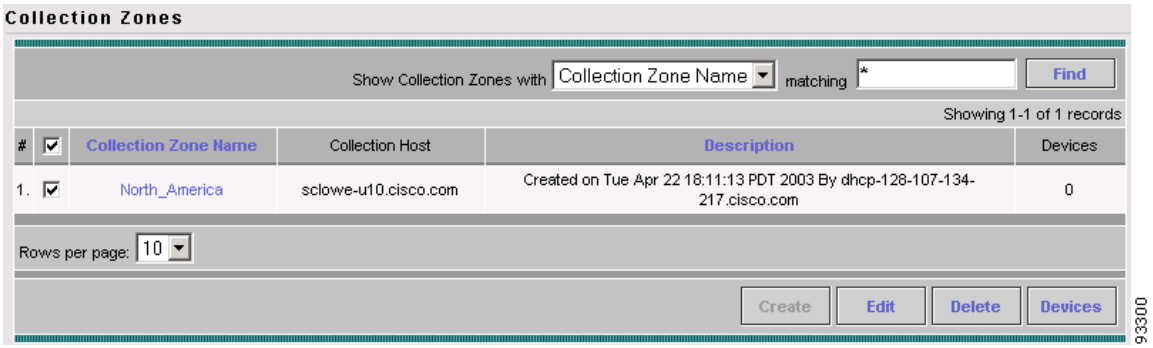
Step 1 Choose **Administration**, then choose **Control Center**.

The Hosts dialog box appears, along with the Hosts table of contents (TOC), as shown in Figure A-10.

Step 2 From the Hosts TOC, choose **Collection Zones**.

The Collection Zones dialog box is displayed (Figure A-15).

Figure A-15 Selecting the Collection Zone



Step 3 Click **Devices**.

ISC displays the list of devices assigned to the specified collection zone (see Figure A-16).

Figure A-16 List of Devices in a Collection Zone