Getting Started with L2VPN

This chapter provides a road map to help you get started using the L2VPN component in ISC 4.1. It contains the following sections:

Overview

Before you can use the L2VPN component to provision Layer 2 services (L2VPN or VPLS), you must complete several installation and configuration steps, as outlined in this chapter. In addition, you should be familiar with basic concepts for ISC and L2VPN (or VPLS) services. The following sections provide a summary of the key tasks you must accomplish to be able to provision L2VPN or VPLS services using ISC. You can use the information provided below as a checklist. Where appropriate, references to other sections in this manual or to other manuals in the ISC documentation set are provided. See the referenced documentation for more detailed information. After the basic installation and configuration steps are completed for both ISC and the L2VPN component, you can refer to the subsequent chapters of this manual to create and provision L2VPN or VPLS services.

Installing ISC and Configuring the Network

Before you can use the L2VPN module in ISC to provision L2VPN or VPLS services, you must first install ISC and do the basic network configuration required to support ISC. Details on these steps are provided in *Cisco IP Solution Center Installation Guide, 4.1*. Refer to that manual for information about ISC installation and general network configuration requirements.

Note To use the L2VPN component within ISC, you must purchase and activate the L2VPN license.

Configuring the Network to Support Layer 2 Services

In additional to basic network configuration required for ISC, you must perform the following network configuration steps to support Layer 2 services. Information on doing these steps is not provided in the ISC documentation. See the documentation for your devices for information on how to perform these steps.

Step 1 Enable MPLS on the core-facing interfaces of the N-PE devices attached to the provider core.

Step 2 Set up /32 loopback addresses on N-PE devices. These loopback addresses should be the termination of the LDP connection(s).

Step 3 Set all L2 devices (switches) to VTP transparent mode. This is so that none of the switches will operate as VLAN servers. This will prevent VLAN information from automatically propagating through the network.

Setting Up Basic ISC Services

After the basic network configuration tasks are completed to support ISC and L2 services, you use ISC to define elements in the ISC repository, such as providers and regions, customers and sites, devices, VLAN and VC pools, NPCs, and other resources that are necessary to provision L2 services. Detailed steps to perform general ISC tasks are covered in *Cisco IP Solution Center Infrastructure Reference, 4.1*. You can also find a summary of some important ISC set up tasks in this manual in Chapter 3, "Setting Up the ISC Service." The information below is a checklist of basic ISC services you must set up before provisioning L2 services.

Setting Up Providers, Customers, and Devices

Perform the following steps to set up providers, customers and devices in the ISC repository. These are global resources that can be used by all ISC services.

Step 1 **Set up service providers and regions.** The region is important because a single provider could have multiple networks. The region is used as a further level of differentiation to allow for such circumstances. To create a provider and a region, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Defining a Service Provider and Its Regions, page 3-3.

Step 2 **Set up customers and customer sites.** A customer is a requestor of a VPN service from an ISP. Each customer can own many customer sites. Each customer site belongs to one and only one Customer and can own many CEs. For detailed steps to create customers and sites, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Defining Customers and Their Sites, page 3-4.

Step 3 **Import or add raw devices.** Every network element that ISC manages must be defined as a device in the ISC repository. An element is any device from which ISC can collect information. In most cases, devices are Cisco IOS routers and switches. You can set up devices in ISC manually, through autodiscovery, or through importing device configuration files. For detailed steps to importing and adding devices, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Chapter 10, "Using Autodiscovery for L2 Services."

Step 4 **Assign devices roles as PE or CE.** After devices are created in ISC, must define them as customer (CE) or provider (PE) devices. You do this by editing the device attributes on individual devices or in batch editing through the ISC inventory manager. To set device attributes, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Setting Up the N-PE Loopback Address

Within ISC, you must set the loopback address on the N-PE device(s). For details about this procedure, see Setting the Loopback Address, page 3-2.

Setting Up ISC Resources for L2VPN and VPLS Services

Some ISC resources, such as access domains, VLAN pools and VC pools are set up to support ISC L2VPN and VPLS services only. Perform the following steps to set up these resources.

Step 1 **Create access domain(s).** For L2VPN and VPLS, you create an access domain if you provision an Ethernet-based service and want ISC to automatically assign a VLAN for the link from the VLAN pool. For each Layer 2 access domain, you need a corresponding access domain object in ISC. During creation, you select all the N-PE devices that are associated with this domain. Later, one VLAN pool can be created for an access domain. For detailed steps to create access domains, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Creating Access Domains, page 3-5.

Step 2 **Create a VLAN pool(s).** A VLAN pool is created for each access domain. For L2VPN and VPLS, you create a VLAN pool so that ISC can assign a VLAN to the links. VLAN ID pools are defined with a starting value and a size. For detailed steps to create VLAN pools, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Creating VLAN Pools, page 3-6.

Step 3 **Create VC pool(s).**VCID pools are defined with a starting value and a size of the VC ID pool. A given VC ID pool is not attached to any inventory object (a provider or customer). Create one VC ID pool per network. For detailed steps to create VC pools, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Creating a VC ID Pool, page 3-9.

Setting Up NPCs

Before creating an L2VPN or VPLS service request, you must predefine the physical links between CEs and PEs or between U-PEs and N-PEs. The Named Physical Circuit (NPC) represents a link going through a group of physical ports. Thus, more than one logical link can be provisioned on the same NPC. Therefore, the NPC is defined once but used by several L2VPN or VPLS service requests. For detailed steps to create NPCs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Creating Named Physical Circuits, page 3-11.

Setting Up VPNs

You must define VPNs before provisioning L2VPN or VPLS services. In L2VPN, one VPN can be shared by different service types. In VPLS, one VPN is required for each VPLS instance. To define VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Defining VPNs, page 3-4.

Working with L2VPN and VPLS Policies and Service Requests

After you have set up providers, customers, devices and resources in ISC, you are ready to create L2VPN or VPLS policies, provision service requests (SRs), and deploy the services. After the service requests are deployed you can monitor, audit and run reports on them. All of these tasks are covered in the *Cisco IP Solution Center L2VPN User Guide, 4.1* (this manual). Perform the following steps to accomplish these tasks.

Step 1 **Review overview information about L2 services concepts.** See Chapter 2, "ISC L2VPN and VPLS Concepts."

Step 2 **Set up a L2VPN or VPLS policy.** See the appropriate chapter, depending on the type of policy you want to create:

- Chapter 4, "Creating an L2VPN Policy."
- Chapter 6, "Creating an L2TPv3 Policy."
- Chapter 8, "Creating a VPLS Policy."

Step 3 **Provision the L2VPN or VPLS service request.** See the appropriate chapter, depending on the type service request you want to provision:

- Chapter 5, "Managing an L2VPN Service Request."
- Chapter 7, "Managing an L2TPv3 Service Request."
- Chapter 9, "Managing a VPLS Service Request."

Step 4 **Deploy the service request.** See Chapter 12, "Deploying, Monitoring and Auditing Service Requests."

Step 5 **Check the status of deployed services.** You can use one or more of the following methods:

- Monitor service requests. See to Chapter 12, "Deploying, Monitoring and Auditing Service Requests."
- Audit service requests. See to Chapter 12, "Deploying, Monitoring and Auditing Service Requests."
- Run L2 and VPLS reports. See to Chapter 11, "Generating L2 and VPLS Reports."