CHAPTER 29

Provisioning Cable Services

Using MPLS VPN technology, service providers can create scalable and efficient private networks using a shared Hybrid Fiber Coaxial (HFC) network and Internet Protocol (IP) infrastructure. The cable MPLS VPN network consists of the following two major elements:

- The Multiple Service Operator (MSO) or cable company that owns the physical infrastructure and builds VPNs for the Internet Service Providers (ISPs) to move traffic over the cable and IP backbone.
- ISPs that use the HFC network and IP infrastructure to supply Internet service to cable customers.

Benefits of Cable MPLS VPNs

Provisioning cable services with MPLS VPNs provides the following benefits:

- MPLS VPNs give cable MSOs and ISPs a manageable way of supporting multiple access to a cable plant.

  Service providers can create scalable and efficient VPNs across the core of their networks MPLS VPNs provide systems support scalability in cable transport infrastructure and management.
- Each ISP can support Internet access services from a subscriber's PC through an MSO's physical cable plant to their networks.
- MPLS VPNs allow MSOs to deliver value-added services through an ISP, and thus, deliver connectivity to a wider set of potential customers.

  MSOs can partner with ISPs to deliver multiple services from multiple ISPs and add value within the MSO's own network using VPN technology.
- Subscribers can choose combinations of services from various service providers.
- The Cisco IOS MPLS VPN cable feature sets build on Cable Modem Termination Server (CMTS) and DOCSIS 1.0 extensions to ensure services are reliably and optimally delivered over the cable plant.

  MPLS VPN provides systems support domain selection, authentication per subscriber, selection of QoS, policy-based routing, and ability to reach behind the cable modem to subscriber end-devices for QoS and billing, while preventing session-spoofing.
- MPLS VPN technology ensures both secure access across the shared cable infrastructure and service integrity.

The Cable MPLS VPN Network

As shown in Figure 29-1, each ISP moves traffic to and from a subscriber's PC, through the MSO's physical network infrastructure, to the ISP's network. MPLS VPNs, created in Layer 3, provide privacy and security by constraining the distribution of VPN routes only to the routers that belong to its network. Thus, each ISP's VPN is insulated from other ISPs that use the same MSO infrastructure.

In the MPLS-based cable scheme, a VPN is a private network built over a shared cable plant and MPLS-core backbone. The public network is the shared cable plant or backbone connection points. A cable plant can support Internet access services and carry traffic for an MSO and its subscribers, as well as for multiple Internet Service Providers (ISPs) and their subscribers.

An MPLS VPN assigns a unique VPN Routing/Forwarding (VRF) instance to each VPN. A VRF instance consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine the contents of the forwarding table.

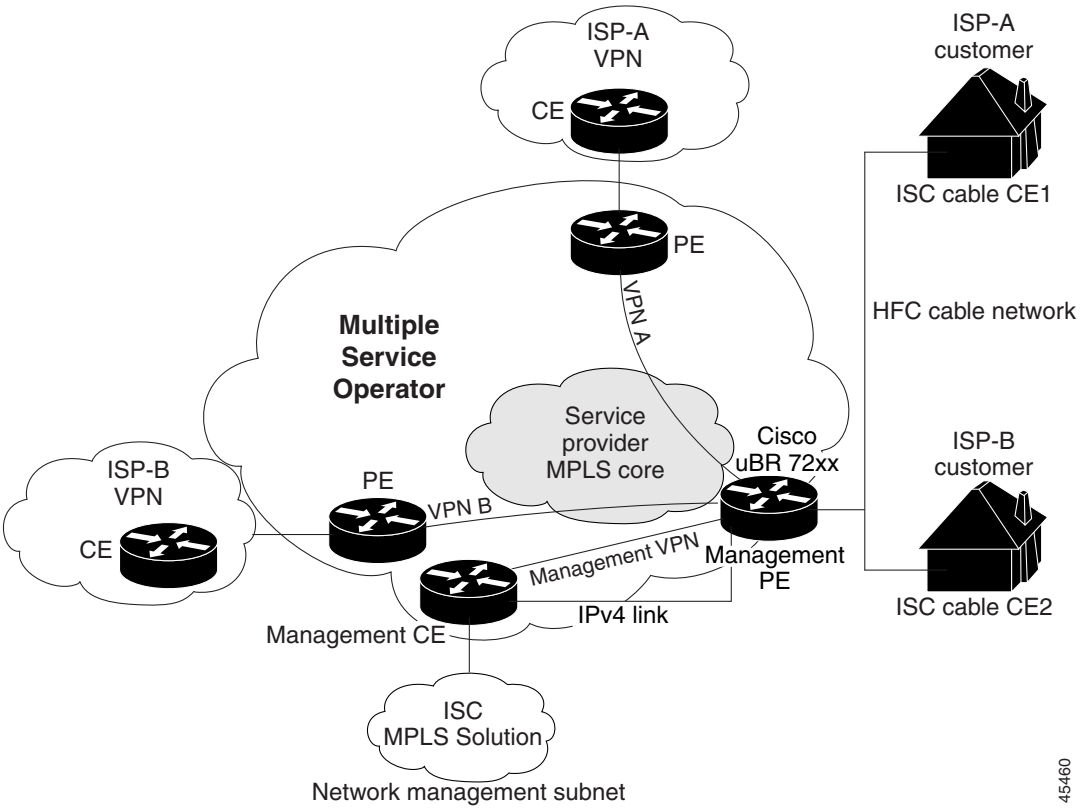
Each PE router maintains one or more VRF tables. If a packet arrives directly through an interface associated with a particular VRF, the PE looks up a packet's IP destination address in the appropriate VRF table. MPLS VPNs use a combination of BGP and IP address resolution to ensure security.

The routers in the cable network are as follows:

- Provider (P) router—Routers in the MPLS core of the service provider network. P routers run MPLS switching, and do not attach VPN labels (MPLS labels in each route assigned by the PE router) to routed packets. VPN labels direct data packets to the correct egress router.
- Provider Edge (PE) router—A router that attaches the VPN label to incoming packets based on the interface or subinterface on which they are received. A PE router attaches directly to a CE router. In the MPLS-VPN approach, each Cisco uBR72xx series router acts as a PE router.
- Customer (C) router—A router in the ISP or enterprise network.
- Customer Edge (CE) router—Edge router on the ISP's network that connects to the PE router on the MSO's network. A CE router must interface with a PE router.
- Management CE (MCE) router—The MCE emulates the role of a customer edge router (CE), but the MCE is in provider space and serves as a network operations center gateway router. The network management subnet is connected to the Management CE (MCE). The MCE is part of a management site as defined in the Prime Fulfillment.
- Management PE (MPE) router—The MPE emulates the role of a PE in the provider core network. The MPE connects the MCE to the provider core network. An MPE can have a dual role as both a PE and the MPE.

The shared cable plant supports Internet connectivity from ISP A to its subscribers and from ISP B to its subscribers.

Figure 29-1 Example of an MPLS VPN Cable Network



Management VPN in the Cable Network

The MPLS network has a unique VPN that exclusively manages the MSOs devices called the management VPN. It contains servers and devices that other VPNs can access. The management VPN connects the Management CE (MCE) router and the management subnet to the MSO PE router (a uBr72xx router or equivalent). Prime Fulfillment and the management servers, such as Dynamic Host Configuration Protocol (DHCP), Cisco Network Registrar (CNR) Time of Day (ToD) are part of the management subnet and are within the management VPN for ISP connectivity. For an explanation of the management VPN, see Chapter 28, "Provisioning Management VPN."

As shown in Figure 29-1, the management VPN is comprised of the network management subnet (where the Prime Fulfillment workstation resides), which is directly connected to the Management CE (MCE). The management VPN is a special VPN between the MCE and the cable VPN gateway. The cable VPN gateway is usually a Cisco uBR 72xx router that functions as both a regular PE and a Management PE. Notice that there is also a parallel IPv4 link between the MCE and the MPE.

Cable VPN Configuration Overview

Cable VPN configuration involves the following:

- An MSO domain that requires a direct peering link to each enterprise network (Prime Fulfillment), provisioning servers for residential and commercial subscribers, and dynamic DNS for commercial users. The MSO manages cable interface IP addressing, Data Over Cable Service Interface Specifications (DOCSIS) provisioning, cable modem host names, routing modifications, privilege levels, and user names and passwords.
- An ISP or enterprise domain that includes the DHCP server for subscriber or telecommuter host devices, enterprise gateway within the MSO address space, and static routes back to the telecommuter subnets.

Note Cisco recommends that the MSO assign all addresses to the end user devices and gateway interfaces. The MSO can also use split management to let the ISP configure tunnels and security.

To configure MPLS VPNs for cable services, the MSO must configure the following:

- Cable Modem Termination System (CMTS). The CMTS is usually a Cisco uBR72xx series router. The MSO must configure Cisco uBR72xx series routers that serve the ISP.
- PE routers. The MSO must configure PE routers that connect to the ISP as PEs in the VPN.

Tip When configuring MPLS VPNs for cable services, you must configure the cable maintenance subinterface on the PE. The cable maintenance interface is the means by which the cable device retrieves its own IP address. For this reason, the maintenance subinterface must be configured before cable services provisioning can take place.

- CE routers.
- P routers.
- One VPN per ISP.
- DOCSIS servers for all cable modem customers. The MSO must attach DOCSIS servers to the management VPN and make them visible to the network.

The MSO must determine the *primary IP address range*. The primary IP address range is the MSO's address range for all cable modems that belong to the ISP subscribers.

The ISP must determine the *secondary IP address range*. The secondary IP address is the ISP's address range for its subscriber PCs.

To reduce security breaches and differentiate DHCP requests from cable modems in VPNs or under specific ISP management, MSOs can use the **cable helper-address** command in Cisco IOS software. The MSO can specify the host IP address to be accessible only in the ISP's VPN. This lets the ISP use its DHCP server to allocate IP addresses. Cable modem IP address must be accessible from the management VPN.

In Prime Fulfillment, you specify the maintenance helper address and the host helper address and the secondary addresses for the cable subinterface.

Cable VPN Interfaces and Subinterfaces

In the cable subscriber environment, several thousand subscribers share a single physical interface. Configurations with multiple logical subinterfaces are a vital part of the MPLS VPN network over cable. You can configure multiple subinterfaces and associate a specific VRF with each subinterface. You can split a single physical interface (the cable plant) into multiple subinterfaces, where each subinterface is associated with a specific VRF. Each ISP requires access on a physical interface and is given its own subinterface. The MSO administrator can define subinterfaces on a cable physical interface and assign Layer 3 configurations to each subinterface.

The MPLS VPN approach of creating VPNs for individual ISPs or customers requires subinterfaces to be configured on the cable interface. One subinterface is required for each ISP. The subinterfaces are tied to the VPN Routing/Forwarding (VRF) tables for their respective ISPs.

You must create the maintenance subinterface on the cable interface and tie it to the management VPN. The maintenance interface is for the ISP's use, and it is used for VPN connectivity, as well as the management VPN using an extranet between the ISP and the management VPN.

Prime Fulfillment automatically selects the subinterface number based on the VRF. If a subinterface that is associated with the current VRF does not yet exist, Prime Fulfillment creates a subinterface and assigns it to the correct VRF. The subinterface number is incremented to 1 greater than the largest subinterface currently assigned for the selected cable interface.

The network management subnet (which includes the CNR, ToD, and Prime Fulfillment) can reply to the cable modem because the management VPN allows connectivity for one filtered route from the ISP's VPN to the Management CE (MCE). Similarly, in order to forward the management requests (such as DHCP renewal to CNR), the ISP VPN must import a route to the MCE in the management VPN.

Cisco uBR7200 series software supports the definition of logical network layer interfaces over a cable physical interface. The system supports subinterface creation on a physical cable interface.

Subinterfaces allow traffic to be differentiated on a single physical interface and associated with multiple VPNs. Each ISP requires access on a physical interface and is given its own subinterface. Using each subinterface associated with a specific VPN (and therefore, ISP) subscribers connect to a logical subinterface, which reflects the ISP that provides their subscribed services. Once properly configured, subscriber traffic enters the appropriate subinterface and VPN.

Provisioning Cable Services in Prime Fulfillment

The tasks you must complete to provision cable services in Prime Fulfillment are as follows:

- Add the PE that has cable interfaces to the appropriate Region.
- Generate a service request to provision the cable maintenance interface on the PE.
- Generate a second service request to provision the MPLS-based cable service. You must generate this cable service request for each VPN.

When using the Prime Fulfillment to provision cable services, there are no CEs in the same sense there are when provisioning a standard MPLS VPN. Thus, you must use a PE-only policy or create a cable policy with no CE.

Creating the Service Requests

This section contains the following subsections:

Creating a Cable Subinterface Service Request

The cable maintenance subinterface on the PE is the means by which the cable device retrieves its own IP address. For this reason, the maintenance subinterface must be configured before provisioning cable services. To create a cable subinterface service request, perform the following steps.

Step 1 Choose **Operate > Service Requests > MPLS**.

The MPLS Policy Selection dialog box appears. This dialog box displays the list of all the MPLS service policies that have been defined in Prime Fulfillment.

Step 2 Choose the PE-Only policy (**cable** in the example above) policy, and then click **OK**.

The MPLS Service Request Editor appears.

Step 3 Click **Add Link**.

The MPLS Service Request Editor now displays a set of fields. Notice that the Select PE field is enabled. Specifying the PE for the link is the first task required to define the link for this service.

Step 4 **PE:** Click **Select PE**.

The Select PE Device dialog box appears.

Step 5 In the Select column, choose the name of the PE for the MPLS link, then click **Select**.

You return to the Service Request Editor window, where the name of the selected PE is now displayed in the PE column.

Step 6 **PE Interface:** Choose the PE interface from the drop-down list.

Only the major interface names are available for you to select. Prime Fulfillment assigns the appropriate subinterface number for each VPN.

The Link Attribute **Add** option is now enabled.

Step 7 In the Link Attribute column, click **Add**.

The MPLS Link Attribute Editor is displayed, showing the fields for the interface parameters, as shown in Figure 29-2.

Figure 29-2 Specifying the MPLS Link Interface Attributes

Step 8 Enter a subinterface name in the Interface Description field.

Step 9 Check the check box for the Cable Maintenance Interface, then click **Edit beside Cable Helper Addresses**.

The Cable Helper Addresses window appears.

Step 10 Click **Add**.

The Cable Helper Addresses window appears.

Step 11 Enter an **IP address** in the IP Address field and choose **Both** for IP Type.

Cable Modems and their attached CPE devices (hosts) will broadcast DHCP packets to the destination IP address, and this destination IP address is the configured cable helper address. So, from configured cable helper address, cable modems and their attached CPE (hosts) will receive their (CM and CPE) IP address.

IP Type can have the following values:

- Host—When selected, only UDP broadcasts from hosts (CPE devices) are forwarded to that particular destination IP address. (For example, only hosts will receive IP addresses from the mentioned helper address.)
- Modem—When selected, only UDP broadcasts from cable modems are forwarded to that particular destination IP address. (For example, only cable modems will receive IP addresses from the mentioned helper address.)
- Both—When selected, UDP broadcasts from hosts (CPE devices) and cable modems are forwarded to that particular destination IP address. (For example, both cable modems and hosts will receive IP addresses from the mentioned helper address.)

Step 12 Click **OK**.

The MPLS Link Attribute Editor reappears.

Step 13 Click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme appears.

Step 14 Edit any IP address scheme values that must be modified for this particular link, then click **Next**. The MPLS Link Attribute Editor for Routing Information appears.

The following routing protocol options are supported:

- STATIC
- RIP
- OSPF
- EIGRP
- None

Because the service policy used for this service specified the routing protocol as editable, you can change the routing protocol for this service request as needed.

Step 15 Edit any routing protocol values that must be modified for this particular link, then click **Next**.

Note For information about protocol types, see Chapter 24, "Specifying the Routing Protocol for a Service".

The MPLS Link Attribute Editor for the VRF and VPN attributes appears. The field values displayed in this dialog box reflect the values specified in the service policy associated with this service.

Note If you want to set the VRF and VPN attributes via a previously defined VRF object, check the **Use VRF Object** check box. For more information on this feature, see Chapter 22, "Independent VRF Management." That chapter describes how to use independent VRF objects in MPLS VPN service policies and service requests.

Note For more information on setting the VRF and VPN attributes in MPLS VPN service requests, see Chapter 25, "Defining VRF and VPN Attributes in an MPLS Service Request".

Step 16 Check the check box for **Join the Management VPN**.

Step 17 Edit any VRF and VPN values that must be modified for this particular link.

Step 18 Click the **Next** button to associate templates or data files to the service request.

Note This step assumes the policy on which the service request is based has template association enabled. If not, there will be no **Next** button visible in the GUI. In that case, click **Finish** and return to the MPLS Service Request Editor window and proceed with Step 34, below.

The MPLS Link Attribute Editor - Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see Chapter 49, "Using Templates and Data Files with Policies and Service Requests"

Step 19 When you have completed setting up templates and data files for any device(s), click **Finish** in the Template Association window to close it and return to the MPLS Service Request Editor window.

Note You can define multiple links in this service request.

Step 20 To save your work on this service request, click **Save**.

The MPLS Service Requests window reappears showing that the service request is in the Requested state and ready to deploy.

Creating Cable Link Service Requests

To create a cable link service request, perform the following steps.

Step 1 Choose **Operate > Service Requests > MPLS**.

The MPLS Policy Selection dialog box appears. This dialog box displays the list of all the MPLS service policies that have been defined in Prime Fulfillment.

Step 2 Choose the policy of choice, then click **OK**.

The MPLS Service Request Editor appears.

Step 3 Click **Add Link**.

The MPLS Service Request Editor now displays a set of fields. Note that in the PE column, the **Select PE** option is now enabled.

Step 4 **PE:** Click **Select PE**.

The Select PE Device dialog box is displayed.

Step 5 In the Select column, choose the name of the PE for the MPLS link, then click **Select**.

You return to the Service Request Editor window, where the name of the selected PE is now displayed in the PE column.

Step 6 **PE Interface:** Choose the PE interface from the drop-down list.

Note that the Link Attribute **Add** option is now enabled.

Step 7 In the Link Attribute column, click **Add**.

The MPLS Link Attribute Editor is displayed, showing the fields for the interface parameters.

Note Do not check the box for Cable Maintenance Interface.

Step 8 Edit any interface values that must be modified for this particular link, then click **Edit** beside Cable Helper Addresses.

The Cable Helper Addresses window appears.

Step 9 Click **Add**.

The Cable Helper Addresses window appears.

Step 10 Enter an **IP address** in the IP Address field and choose **Both**, **Modem,** or **Host** for IP Type.

Cable Modems and their attached CPE devices (hosts) will broadcast DHCP packets to the destination IP address, and this destination IP address is the configured cable helper address. So, from configured cable helper address, cable modems and their attached CPE (hosts) will receive their (CM and CPE) IP address.

IP Type can have the following values:

- Host—When selected, only UDP broadcasts from hosts (CPE devices) are forwarded to that particular destination IP address. (For example, only hosts will receive IP addresses from the mentioned helper address.)
- Modem—When selected, only UDP broadcasts from cable modems are forwarded to that particular destination IP address. (For example, only cable modems will receive IP addresses from the mentioned helper address.)
- Both—When selected, UDP broadcasts from hosts (CPE devices) and cable modems are forwarded to that particular destination IP address. (For example, both cable modems and hosts will receive IP addresses from the mentioned helper address.)

Step 11 Click **OK**.

The MPLS Link Attribute Editor reappears.

Step 12 Click **Edit** beside Secondary Addresses.

The Cable Secondary Addresses window appears. The secondary IP address enables CPE devices (hosts) attached to cable modem to talk to CMTS. (Usually this is a public IP address so that PCs can go to internet.)

Step 13 Enter an IP address in the IP address/Mask field and click **OK**.

The MPLS Link Attribute Editor reappears.

Step 14 Click **Next**.

Step 15 The MPLS Link Attribute Editor for the IP Address Scheme appears.

Step 16 Edit any IP address scheme values that must be modified for this particular link, then click **Next**.

The MPLS Link Attribute Editor for Routing Information appears.

Note For information about protocol types, see Chapter 24, "Specifying the Routing Protocol for a Service".

Step 17 Edit any routing protocol values that must be modified for this particular link, then click **Next**.

The MPLS Link Attribute Editor for the VRF and VPN attributes appears. The field values displayed in this dialog box reflect the values specified in the service policy associated with this service.

Note If you want to set the VRF and VPN attributes via a previously defined VRF object, check the **Use VRF Object** check box. For more information on this feature, see Chapter 22, "Independent VRF Management." That chapter describes how to use independent VRF objects in MPLS VPN service policies and service requests.

Note For more information on setting the VRF and VPN attributes in MPLS VPN service requests, see Chapter 25, "Defining VRF and VPN Attributes in an MPLS Service Request".

Step 18 Check the check box for Join the Management VPN.

Step 19 Edit any VRF and VPN values that must be modified for this particular link, then click **Add**.

The Select CERCs/VPN dialog box appears.

Step 20 Choose the customer name and VPN.

Step 21 Click **Join as Spoke**, then click **Done**.

The MPLS Link Attribute Editor for the VRF and VPN attributes appears.

Step 22 Edit any VRF and VPN values that must be modified for this particular link.

Step 23 Click the **Next** button to associate templates or data files to the service request.

Note This step assumes the policy on which the service request is based has template association enabled. If not, there will be no **Next** button visible in the GUI. In that case, click **Finish** and return to the MPLS Service Request Editor window and proceed with Step 27, below.

The MPLS Link Attribute Editor - Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see Chapter 49, "Using Templates and Data Files with Policies and Service Requests"

Step 24 When you have completed setting up templates and data files for any device(s), click **Finish** in the Template Association window to close it and return to the MPLS Service Request Editor window.

Note You can define multiple links in this service request.

Step 25 To save your work on this service request, click **Save**.

The MPLS Service Requests window reappears showing that the service request is in the Requested state and ready to deploy.