Provisioning Management VPN

This chapter describes how to implement the IP Solutions Center (ISC) Management VPN. It contains the following sections:

- Overview of the ISC Management Network, page 9-1
- Provisioning a Management CE in ISC, page 9-8

Overview of the ISC Management Network

This section provides the fundamental concepts and considerations for administering customer edge routers (CEs) in the context of an ISC management subnet. Before ISC can be appropriately deployed to deliver services to customers, the question of whether the CEs are to be managed by the Service Provider or not must be answered.

This section contains the following sections:

- Unmanaged Customer Edge Routers, page 9-1
- Managed Customer Edge Routers, page 9-2
- Network Management Subnets, page 9-3
- Implementation Techniques, page 9-4
- Out-of-Band Technique, page 9-7

Unmanaged Customer Edge Routers

One of the options available to the Service Provider is to not manage the customer edge routers (CEs) connected to the Service Provider network. For the Service Provider, the primary advantage of an unmanaged CE is administrative simplicity.

If the CEs are unmanaged, the provider can use IPv4 connectivity for all management traffic. ISC is not employed for provisioning or managing unmanaged CEs.

Figure 9-1 shows a basic topology with unmanaged CEs. The network management subnet has a direct link to the Service Provider MPLS core network.
Regarding unmanaged CEs, Service Providers should note the following considerations:

- Because unmanaged CEs are outside the Service Provider’s administrative domain, the Service Provider does not maintain or configure unmanaged CEs.
- The Service Provider does not administer the following elements on the unmanaged CE:
  - IP addresses
  - Host Name
  - Domain Name server
  - Fault management (and timestamp coordination by means of the Network Time Protocol)
  - Collecting, archiving, and restoring CE configurations
  - Access data such as passwords and SNMP strings on the unmanaged CE
- Prototype CE configlets are generated, but they are not automatically downloaded to the router.
- There is no configuration management.
  - With no configuration management, no configuration history is maintained and there is no configuration change management.
  - Changes to a service request (on the PE-CE link) are not deployed to the CE.
- There is no configuration auditing because there is no means to retrieve the current CE configuration.
- You can perform routing auditing.
- You can use the Service Assurance Agent (SA Agent) to measure response times between shadow routers, but you cannot use SA Agent to measure response times between CEs.

### Managed Customer Edge Routers

The alternative to unmanaged CEs is managed CEs, that is, customer edge routers managed by the Service Provider. Managed CEs can be wholly within the Service Provider’s administrative domain or co-managed between the provider and the customer, although CE co-management poses a number of ongoing administrative challenges and is not recommended.
Regarding managed CEs, Service Providers should note the following considerations:

- Managed CEs are within the Service Provider’s administrative domain. Thus, some connectivity to the CEs from the Service Provider network is required.
- The Service Provider must administer the following elements on the managed CE:
  - IP addresses
  - Host Name
  - Domain Name server
  - Access data such as passwords and SNMP strings
- The Service Provider should administer fault management (and timestamp coordination by means of the Network Time Protocol)
- The Service Provider can administer collecting, archiving, and restoring CE configurations.
- CE configlets are generated and downloaded to the managed CE.
- Changes to service requests are based on the current CE configuration and automatically downloaded.
- The CE configurations are audited.
- Customer routing and Service Provider routing must interact.
- Access from CEs to the management hosts on the network management subnet is required.
- Configuration auditing and routing auditing are both functional.
- You can use the Service Assurance Agent (SA Agent) to measure response times between CEs and between shadow routers.

The following sections discuss the concepts and issues required for administering a managed CE environment.

**Network Management Subnets**

The Network Management Subnet is required when the provider’s service offering entails the management of CEs. Once a CE is in a VPN, it is no longer accessible by means of conventional IPv4 routing unless one of the techniques described in this chapter is employed.

Figure 9-2 shows the ISC network management subnet and the devices that might be required to connect to it:
Issues Regarding Access to VPNs

The core issues with regard to gaining access to VPNs are as follows:

- How to keep provider space “clean” from unnecessary customer routes
- How to keep customer space “clean” from both the provider’s and other customer’s routes
- How to provide effective security
- How to prevent routing loops

\[\text{Note}\] ISC does not handle any of these responsibilities—doing so must be designed and implemented by the Service Provider.

- Reachability changes as a direct consequence of employing ISC.
  Before you provision a CE in the ISC, you might be able to reach the CE via IPv4 connectivity, but the moment the product deploys a service request, you cannot reach that CE any more—unless you have \textit{first} implemented the network management subnet.

Implementation Techniques

The network management subnet must have access to a Management CE (MCE) and PEs. The network management subnet is appropriate—and necessary—when there is an intent to have managed CEs connected via an in-band connection. \textit{In-band} indicates a single link or permanent virtual circuit (PVC) that carries \textit{both} the customer’s VPN traffic, as well as the provider’s network management traffic.
Management CE (MCE)

The network management subnet is connected to the Management CE (MCE). 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 MCE is part of a management site as defined in the ISC. You configure the MCE by identifying the CE as part of the management LAN in ISC.

Management PE (MPE)

The Management PE (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 MPE needs access to the following devices:

<table>
<thead>
<tr>
<th>Device</th>
<th>Connectivity</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Customer Edge Routers (CEs)</td>
<td>Access from the network management subnet into the VPNs</td>
<td>Provision or change configuration and collect SA Agent performance data.</td>
</tr>
<tr>
<td>2. Shadow CEs</td>
<td>Access from the network management subnet into the VPNs</td>
<td>A simulated CE used to measure data travel time between two devices. A shadow CE is connected directly to a PE via Ethernet.</td>
</tr>
<tr>
<td>3. Provider Edge Routers (PEs)</td>
<td>Standard IP connectivity</td>
<td>Provision or change configuration.</td>
</tr>
</tbody>
</table>

At the current time, ISC recommends two main network management subnet implementation techniques:

- Management VPN Technique
  
  The MPE-MCE link uses a Management VPN (see Management VPN, page 9-5) to connect to managed CEs. To connect to the PEs, the MPE-MCE link uses a parallel IPv4 link.

- Out-of-Band Technique
  
  In the Out-of-Band technique, the MCE has IPv4 connectivity (that is, not MPLS VPN connectivity) to all the CEs and PEs in the network (see Out-of-Band Technique, page 9-7). In this context, *out-of-band* signifies a separate link between PEs that carries the provider’s management traffic.

The network management subnet technique the provider chooses to implement depends on many factors, which are discussed later in this chapter.

Management VPN

The Management VPN technique is the default method provisioned by ISC. A key concept for this implementation technique is that all the CEs in the network are a member of the management VPN. To connect to the PEs, the MPE-MCE link uses a parallel IPv4 link. Figure 9-3 shows a typical topology for the Management VPN technique.
When employing the Management VPN technique, the MPE-MCE link uses a management VPN to connect to managed CEs. To connect to the PEs, the MPE-MCE link employs a parallel IPv4 link. Each CE in a customer VPN is also added to the management VPN by selecting the Join the management VPN option in the service request user interface.

The function of the management route map is to allow only the routes to the specific CE into the management VPN. The Cisco IOS supports only one export route map and one import route map per VRF.

As shown in Figure 9-3, a second parallel non-MPLS VPN link is required between the MPE and MCE to reach the PEs.

**Note**

Implementation of the Management VPN technique requires Cisco IOS 12.07 or higher.

**Advantages**

The advantages involved in implementing the Management VPN technique are as follows:

- Provisioning with this method requires only one service request.
• The only routes given to the network management subnet are the routes to the CEs—that is, either the address of the CE link to the PE or the CE loopback address. General VPN routes are not given to the network management subnet.

• A CE in the Management VPN method is a spoke to the Management VPN regardless of which role the CE has within its own VPN. Therefore, CEs cannot be accidentally exposed to inappropriate routes. The only management routes the CEs can learn must come from a hub of the Management VPN.

**Out-of-Band Technique**

The Out-of-Band technique does not employ a management VPN to manage the CEs. Out-of-band connectivity is provided by IPv4 links. *Out-of-band* signifies a separate link between PEs that carries the provider’s management traffic. As shown in Figure 9-4, the MCE provides separation between the provider’s routes and the customer’s routes.

![Figure 9-4 Out-of-Band Technique](image)

The Out-of-Band technique has the advantage of being relatively simple to set up, and no management VPN is required. However, its disadvantages are that it is expensive since it requires an IPv4 connection to each CE. Also, due to the delicate staging requirements for this technique, the Out-of-Band implementation does have a high degree of complexity.
Provisioning a Management CE in ISC

The ISC network management subnet is connected to the Management CE (MCE). 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 MCE is part of a management site as defined in ISC.

This section covers the following topics:
- Defining CE as MCE, page 9-8
- Creating MCE Service Requests, page 9-10
- Adding PE-CE Links to Management VPNs, page 9-15

Defining CE as MCE

You configure the MCE by identifying the CE as part of the management LAN in ISC software. To do this, perform the following steps:

**Step 1** Choose Service Inventory > Inventory and Connection Manager > CPE Devices.

The list of CPE devices for all currently defined customers is displayed, as shown in Figure 9-5.

**Figure 9-5   List of All CPEs for All Customers**

<table>
<thead>
<tr>
<th>CPE Devices</th>
<th>Show CPEs with Device Name matching</th>
<th>Find</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Device Name</th>
<th>Customer Name</th>
<th>Site Name</th>
<th>Management Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>mke1.cisco.com</td>
<td>AcmeInc</td>
<td>Acme_NY</td>
<td>Managed - No SA Agent</td>
</tr>
<tr>
<td>2</td>
<td>mke2.cisco.com</td>
<td>AcmeInc</td>
<td>Acme_NY</td>
<td>Managed - No SA Agent</td>
</tr>
<tr>
<td>3</td>
<td>mke3.cisco.com</td>
<td>AcmeInc</td>
<td>Acme_SF</td>
<td>Managed - No SA Agent</td>
</tr>
<tr>
<td>4</td>
<td>mke4.cisco.com</td>
<td>AcmeInc</td>
<td>Acme_SF</td>
<td>Managed - No SA Agent</td>
</tr>
<tr>
<td>5</td>
<td>mke5.cisco.com</td>
<td>AcmeInc</td>
<td>Acme_SF</td>
<td>Managed - No SA Agent</td>
</tr>
<tr>
<td>6</td>
<td>mke6.cisco.com</td>
<td>AcmeInc</td>
<td>Acme_TX</td>
<td>Managed - No SA Agent</td>
</tr>
<tr>
<td>7</td>
<td>mke7.cisco.com</td>
<td>AcmeInc</td>
<td>Acme_TX</td>
<td>Managed - No SA Agent</td>
</tr>
<tr>
<td>8</td>
<td>mke8.cisco.com</td>
<td>Widget Inc</td>
<td>Widget_SF</td>
<td>Managed - No SA Agent</td>
</tr>
<tr>
<td>9</td>
<td>mke9.cisco.com</td>
<td>Widget Inc</td>
<td>Widget_SF</td>
<td>Managed - No SA Agent</td>
</tr>
<tr>
<td>10</td>
<td>mke10.cisco.com</td>
<td>Widget Inc</td>
<td>Widget_SF</td>
<td>Managed - No SA Agent</td>
</tr>
</tbody>
</table>

**Step 2** Choose the CE that will function as the MCE in the management VPN, then click Edit.

The Edit CPE Device dialog box appears, displaying the pertinent information for the selected CPE, as shown in Figure 9-6.
Step 3  Management Type: From the drop-down list, set the management type to Managed—Management LAN.

Step 4  Click Save.

You return to the list of CPE devices, where the new management type for the selected CE (in our example, 3. mlce8.cisco.com) is now displayed, as shown in Figure 9-7.

Figure 9-7  Selected CE Defined as a Management CE

<table>
<thead>
<tr>
<th>#</th>
<th>Device Name</th>
<th>Customer Name</th>
<th>Site Name</th>
<th>Management Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>mlce8.cisco.com</td>
<td>AcmeInc</td>
<td>Acme_NV</td>
<td>Managed - No SA Agent</td>
</tr>
<tr>
<td>2</td>
<td>mlce2.cisco.com</td>
<td>AcmeInc</td>
<td>Acme_NV</td>
<td>Managed - No SA Agent</td>
</tr>
<tr>
<td>3</td>
<td>mlce8.cisco.com</td>
<td>AcmeInc</td>
<td>Acme_SF</td>
<td>Managed - Management LAN</td>
</tr>
<tr>
<td>4</td>
<td>mlce8.cisco.com</td>
<td>AcmeInc</td>
<td>Acme_SF</td>
<td>Managed - No SA Agent</td>
</tr>
<tr>
<td>5</td>
<td>mlce3.cisco.com</td>
<td>AcmeInc</td>
<td>Acme_SF</td>
<td>Multi-VRF - No SA Agent</td>
</tr>
</tbody>
</table>
Creating MCE Service Requests

To create an MCE service request, perform the following steps:

**Step 1**  Choose **Service Inventory > Inventory and Connection Manager > Service Requests.**
The Service Requests dialog box appears.

**Step 2**  To start the process to create a new service, click **Create.**
A drop-down list is displayed, showing the types of service requests you can create.

**Step 3**  Choose **MPLS VPN.**
The Select MPLS Policy dialog box appears, as shown in Figure 9-8.

![Figure 9-8 Selecting the MPLS Policy for This Service](image)

This dialog box displays the list of all the MPLS service policies that have been defined in ISC.

**Step 4**  Choose the policy of choice, then click **OK.**
The MPLS Service Request Editor appears, as shown in Figure 9-9.

![Figure 9-9 MPLS Service Request Editor](image)

**Step 5**  Click **Add Link.**
The MPLS Service Request Editor now displays a set of fields, as shown in Figure 9-10. Notice that the Select CE field is enabled. Specifying the CE for the link is the first task required to define the link for this service.
Step 6  
CE: Click Select CE.

The Select CPE Device dialog box is displayed, as shown in Figure 9-11.

Figure 9-11 Selecting the MCE for the MPLS Link

a. From the “Show CPEs with” drop-down list, you can display CEs by Customer Name, by Site, or by Device Name.
b. You can use the Find button to either search for a specific CE, or to refresh the display.
c. You can set the “Rows per page” to 5, 10, 20, 30, 40, or All.
d. This dialog box displays the first page of the list of currently defined CE devices. The number of pages of information is displayed in the lower right corner of the dialog box.

To go to the another page of CE devices, click the number of the page you want to go to.

Step 7  
In the Select column, choose the name of the MCE for the MPLS link, then click Select.

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

Step 8  
CE Interface: Choose the CE interface from the drop-down list, as shown in Figure 9-12.
Step 9  PE: Click Select PE.

The Select PE Device dialog box is displayed, as shown in Figure 9-13.

Step 10  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 11  PE Interface: Choose the PE interface from the drop-down list, as shown in Figure 9-14.
Figure 9-14 PE and PE Interface Fields Defined

<table>
<thead>
<tr>
<th>#</th>
<th>LINK ID</th>
<th>CE</th>
<th>CE Interface</th>
<th>PE</th>
<th>PE Interface</th>
<th>Link Attribute</th>
<th>Logical Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>mbe0</td>
<td>FastEthernet/0</td>
<td>mbe1</td>
<td>FastEthernet/0</td>
<td>Add</td>
<td>NA</td>
</tr>
</tbody>
</table>

The Link Attribute Add option is now enabled.

**Step 12**
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 9-15.

**Figure 9-15 Specifying the MPLS Link Interface Attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PE Information</td>
<td></td>
</tr>
<tr>
<td>PE</td>
<td>mbe1</td>
</tr>
<tr>
<td>Interface Name</td>
<td>FastEthernet/0</td>
</tr>
<tr>
<td>Interface Description</td>
<td></td>
</tr>
<tr>
<td>Shutdown Interface</td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>DOT1Q</td>
</tr>
<tr>
<td>Auto-Pick VLAN ID</td>
<td></td>
</tr>
<tr>
<td>CE Information</td>
<td></td>
</tr>
<tr>
<td>CE</td>
<td>mbe0</td>
</tr>
<tr>
<td>Interface Name</td>
<td>FastEthernet/0</td>
</tr>
<tr>
<td>Interface Description</td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>DOT1Q</td>
</tr>
</tbody>
</table>

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on each of the PE and CE interface fields, see **Specifying PE and CE Interface Parameters, page 5-4**.

**Note** The VLAN ID is shared between the PE and CE, so there is one VLAN ID for both.

**Step 13**
Edit any interface values that need to be modified for this particular link, then click **Next**.

The MPLS Link Attribute Editor for the IP Address Scheme appears, as shown in Figure 9-16.
Step 14  Edit any IP address scheme values that need to be modified for this particular link, then click Next.

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the IP address scheme fields, see Specifying the IP Address Scheme, page 5-8.

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

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the routing information for the PE and CE, see Specifying the Routing Protocol for a Service, page 5-11.

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 16  Edit any VRF values that need to be modified for this particular link, then click Finish.
You return to the MPLS Service Request Editor.

Step 17  To save your work on this first link in the service request, click Save.
You return to the Service Requests dialog box, where the information for the link you just defined is now displayed, as shown in Figure 9-18.

Figure 9-18  Service Request for an MPLS Link Completed

You can add additional links to this service request by choosing Add Link and specifying the attributes of the next link in the service. As you can see, the service request is in the Requested state. When all the links for this service have been defined, you must deploy the service.

Adding PE-CE Links to Management VPNs

When you have created the Management VPN, then you can proceed to add service for the PE-CE links you want to participate in the Management VPN. To do this, perform the following steps:

Step 1  Navigate to the MPLS Link Attribute Editor - VRF and VPN window for the selected CE.
Step 2  Check the Join the management VPN option.
When you join the CE with the Management VPN in this step, ISC generates the appropriate route-map statements in the PE configlet. The function of the management route map is to allow only the routes to the specific CE into the management VPN. Cisco IOS supports only one export route map and one import route map per VRF (and therefore, per VPN).
Step 3  Complete the service request user interface.