Administering Customer Edge Routers

This chapter provides the fundamental concepts and considerations, as well as our recommendations, for administering customer edge routers (CEs) in a Service Provider environment. Before VPN Solutions Center software 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.

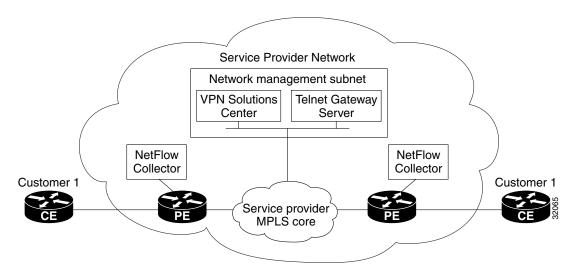
Unmanaged CE Considerations

One of the options available to the Service Provider is to not manage the CEs connected to the Service Provider network. For the Service Provider, the primary advantage of unmanaged CEs is administrative simplicity.

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

Figure 6-1 shows a basic topology with unmanaged CEs. Note that the network management subnet has a direct link to the Service Provider MPLS core network.





6

HAPTE

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 CE Considerations

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.

For information on how you define a CE as a managed CE, refer to the "Adding the Customer Edge Routers to a Site" section on page 3-4.

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.
- NetFlow Collector devices are operational.

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

What Is the Network Management Subnet?

The VPN Solutions Center Network Management Subnet consists of the VPN Solutions Center workstation and one or more Telnet Gateway Server workstations connected on a LAN or subnet.

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 6-2 shows the VPN Solutions Center network management subnet and the devices that may be required to connect to it:

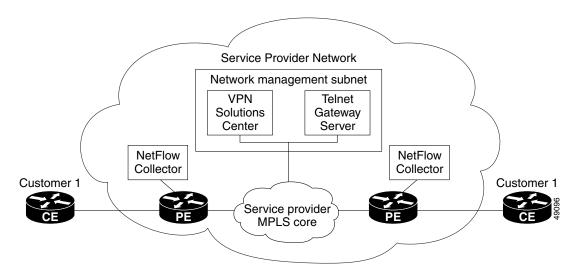


Figure 6-2 The VPN Solutions Center Network Management Subnet

Access to VPN Issues

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

VPN Solutions Center 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 VPN Solutions Center.

Before you provision a CE in the VPN Solutions Center software, you might be able to reach the CE via IPv4 connectivity, but the moment the product deploys a task, you cannot reach that CE any more—unless you have *first* implemented the network management subnet.

The Network Management Subnet Implementation Techniques

The network management subnet must have access to Management CEs (MCEs), PEs, and the NetFlow Collector devices.

The network management subnet is appropriate—and necessary—only if there is an intent to have managed CEs connected via an in-band connection. *In-band* indicates a single link or permanent virtual circuit (PVC) that carries *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 VPN Solutions Center software.

You configure the MCE by identifying the CE as part of the management LAN in the VPNSC software. For details on how to define a CE as an MCE within VPN Solutions Center software, see the "Implementing the Management VPN Technique" section on page 3-23.

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:

Device		Connectivity	Function
1.	Customer Edge Routers (CEs)	Access from the network management subnet into the VPNs	Provision or change configuration and collect SA Agent performance data
2.	Shadow routers	Access from the network management subnet into the VPNs	A simulated CE used to measure data travel time between two devices
3.	Provider Edge Routers (PEs)	standard IP connectivity	Provision or change configuration
4.	NetFlow Collector	standard IP connectivity	Collect data

At the current time, VPN Solutions Center recommends three main network management subnet implementation techniques:

• Management VPN Technique

The MPE-MCE link uses a Management VPN (see the "Management VPN Technique" section on page 6-5) to connect to managed CEs. To connect to the PEs and NetFlow Connector, the MPE-MCE link uses a parallel IPv4 link.

• Extranet Multiple VPN Technique

The MPE-MCE link uses the Extranet Multiple VPN *technique* (see the "Extranet Multiple VPN Technique" section on page 6-7) to connect to managed CEs. To connect to the PEs and NetFlow Connector, 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 the "Out-of-Band Technique" section on page 6-8). 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 Technique

The Management VPN technique is the default method provisioned by VPN Solutions Center. 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 and NetFlow Collector, the MPE-MCE link uses a parallel IPv4 link. Figure 6-3 shows a typical topology for the Management VPN technique.

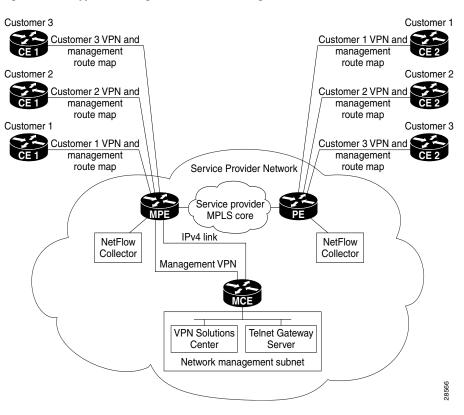


Figure 6-3 Typical Configuration for a Management VPN Network

When employing the Management VPN technique, the MPE-MCE link uses a *management VPN* to connect to managed CEs. To connect to the PEs and NetFlow Connector, 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 wizard (see the "About Provisioning PE-CE Links in the Management VPN" section on page 3-31). 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 (and therefore, per VPN).

As shown in Figure 6-3, a second parallel non-MPLS VPN link is required between the MPE and MCE to reach the PEs and the NetFlow Collector host.

For information on how to provision a Management VPN in VPN Solutions Center software, see the "Implementing the Management VPN Technique" section on page 3-23.

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.

Extranet Multiple VPN Technique

A key concept for this network management subnet technique is that the MPE-MCE pair are part of *all* the customer's VPNs. When you a add new VPN to the Extranet Multiple VPN, you must create a service request each time a VPN is defined to add that VPN to the MPE-MCE pair, and thus to the network management subnet. To connect to the PEs and NetFlow Connector, the MPE-MCE link uses a parallel IPv4 link. Figure 6-4 shows a typical topology for the Extranet Multiple VPN.

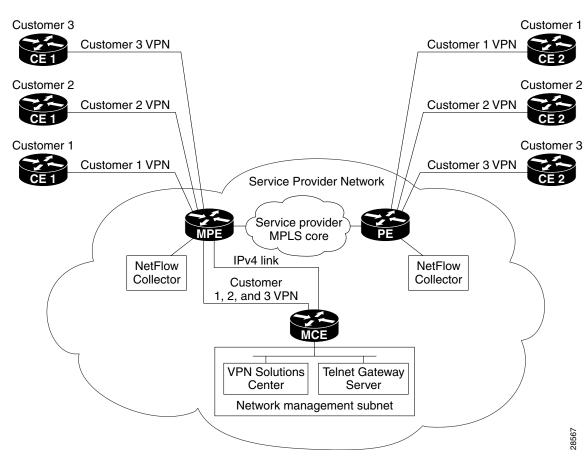


Figure 6-4 Extranet Multiple VPN

In the Extranet Multiple VPN (sometimes referred to as the *rainbow VPN*), several security and access list considerations exist, but these considerations are centralized at the MPE and MCE devices.

The MPE includes the BGP routes to *all* customer routes. This should be constrained such that only the CE subnet routes are imported to the interior gateway protocol.

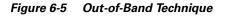
Advantages

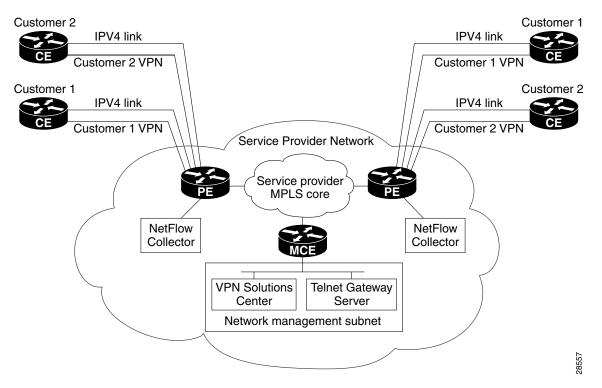
The advantages in implementing the Extranet Multiple VPN technique are as follows:

- Only the MPE has routes for all the VPNs—the PEs do not have the VPN routes; that is, all the customer routes are only in the MPE's VRF route tables.
- You must apply access lists on the MPE-MCE link only.
- It is easy to create another MPE-MCE pair if necessary.

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 6-5, the MCE provides separation between the provider's routes and the customer's routes.





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.

Securing the Management Network

If you use VPN Solutions Center for IP allocation, you know the set of legal IP addresses for management access to CEs. Therefore, you can deny all packets that do not originate from an VPN Solutions Center IP address pool. (If the network employs non-auto-picked IP addressing, augment the notion of "pool" to cover all legal IP addresses for a CE interface to a PE.) You can also limit access precisely to those hosts on the network management subnet that need it.

The CE access lists between IP pool addresses and the network management subnet hosts should also specify the required ports for access (using Telnet). It is important to limit the port numbers. Those three ports are the only permissible ones. Access to the Orbix process running on the VPN Solutions Center host should particularly be denied.

Cisco recommends the following access rules of type:

- Permit from {VPNSC host} to anything in the "pool."
- Deny all others.

Apply these access rules outbound on the CE on its interface up to the PE so that only VPN Solutions Center can send packets, and then only to management addresses. Additional rules of type are as follows:

- Permit from "pool" to {VPNSC host} for TCP established.
- Deny all others.

These rules should apply on the CE as an input list on its link from the PE. Thus, only responses are allowed in—general CEs cannot start a session to the management machines—and then only from legal IP addresses.

Given these rules of type, only the CE can send packets into the network management subnet, and even those must be in response to a network management subnet query. Spoofing could be an issue, but for that Cisco recommends anti-spoofing access lists as part of the basic configuration of CEs at customer sites—deny all packets coming from within a site marked with a management address.) The CEs do not need the CE-PE link when returning management packets.

Another option is to suppress the network management subnet; that is, you can set up static addresses with /32 subnet masks on the PE—one for each host on the network management subnet needing to receive packets from CEs. At a minimum, that would be the VPN Solutions Center workstation. No other routes need to be allowed into the VRF supporting the network management subnet.

Build the local entries in the VRF like this:

IP route VRF Management VPNSC_host/32 CE_address
IP route VRF Management CIPM_host/32 CE_address

The term "VRF Management" is for illustration purposes only; VPN Solutions Center builds all this and picks a name for the VRF.

To prevent injections of inappropriate routes, it is helpful to add this command:

```
IP route VRF Management 0.0.0.0/0 Null0
```

That is all you want to put in the local VRF table. From there, it dynamically learns all the routes to the other CEs.

However, you cannot prevent it also knowing a directly connected route for the link between this PE and the Management CE. You must protect against customer attempts to gain access to the Management CE. The access lists described above control only *transit* traffic across that CE.

Therefore, Cisco recommends that the PE have an access list applied outbound on the link to the CE in the following form:

permit packets to {VPNSC Host, CIPM Host}
deny everything else

This is simple and it prevents customers from gaining access to the Management CE.

Cisco recommends the following:

1. In the PE configuration file, enter the following commands:

```
ip route vrf management VPNSC_host ip/32 <mce
ip route vrf management CIPM_host ip/32 <mce</pre>
```

To dump unknowns, add this command:

ip route vrf management 0.0.0.0/0 Null0

2. Whenever possible, use statics on the Management CE too—use a static or set of statics covering legal management addresses, as discussed above.

If dynamic routing is absolutely required (meaning it is not known which addresses might be used for CE-PE links, which is not recommended), then you can use RIP. However, Cisco recommends doing so one way only: redistribute BGP into RIP on the PE, but do not redistribute back. VPN Solutions Center makes two-way redistributions in such cases, so add the RIP configuration manually when setting this up. Route maps could apply here, but as noted, running dynamic routing is generally undesirable.

3. The most important access lists are output and input lists on the Management CE.

The output access list: On the Management CE, connected to Link B (with access to the VPNs), make an output access list as follows:

```
permit {VPNSC host, CIPM host} to <pool
deny all</pre>
```

The input access list is as follows:

```
permit <pool to {VPNSC host, CIPM host} with tcp-established
deny all</pre>
```

4. To protect the Management CE, create an output access list on the PE's link B interface:

permit to {VPNSC host, CIPM host}
deny all

5. If desired, also place an access list to protect the IPv4 link, depending on the Service Provider's own access needs to the network management subnet.