



Provisioning Dial Access to MPLS VPN Integration

This chapter describes how to provision each of the methods of dial access to MPLS (Multiprotocol Label Switching) VPN (virtual private network) integration. It covers the following subjects:

- [Provisioning Dial-In Access, page 3-1](#)
 - Provisioning L2TP dial-in
 - Provisioning direct ISDN PE dial-in



Note

Because many of the configuration tasks for these two methods are the same, they are described in a single section, with differences noted where a task applies to only one of the access methods.

- [Provisioning L2TP Dial Backup, page 3-18](#)
- [Provisioning Dial-out Access, page 3-20](#)
 - Provisioning L2TP dial-out
 - Provisioning direct ISDN dial-out

The chapter also includes a section on [Sample Configurations, page 3-24](#).

Descriptive overviews of the dial access methods and related features are covered in [Chapter 2, “Overview of Dial Access to MPLS VPN Integration”](#).

Provisioning Dial-In Access

Before You Begin

The procedures provided here are specific to provisioning remote access to an MPLS VPN and are based on two assumptions:

1. That the following setup and configuration tasks have already been carried out:
 - Setup of the MPLS core network
 - Setup of the customer VPN
 - Configuration of the links between the provider edge router (PE) and the customer edge router (CE)

- That you have a good understanding of the architecture and features you are using and that you have selected the means you will use for implementing those features (for example, which of several strategies you will use for address management or for user authentication and authorization).

See [Chapter 2, “Overview of Dial Access to MPLS VPN Integration”](#) for information that will help you understand the dial architectures and decide on your implementation approach.

Dial-In Provisioning Checklist

[Table 3-2](#) lists provisioning tasks for L2TP dial-in and for direct ISDN PE dial-in. Procedures for completing each task are described in the sections that follow. If you are viewing this document online, you can click on highlighted text to get details on the procedure.

Table 3-1 Checklist of Tasks for Dial-in Provisioning

Task	L2TP Dial-In	Direct ISDN PE Dial-In
Before you begin, read the Cisco Remote Access to MPLS VPN Integration 2.0 Release Notes at http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/ramp2/relnote/index.htm		
Do initial, one-time setup		
Task 1. Configure the PE Routers for MPLS.	On the VHG/PE	On the NAS/PE
Task 2. Configure the SP AAA RADIUS Server with Client Information.	On the SP AAA server: <ul style="list-style-type: none"> NAS/LAC client information VHG/PE client information 	On the SP AAA server: NAS/PE client information
Task 3. Configure RADIUS AAA on the Querying Device.	On the NAS/LAC On the VHG/PE	On the NAS/PE
Add new customer groups as needed		
Task 1. Configure L2TP Information for New Customers (L2TP only).	On the NAS/LAC or the SP AAA RADIUS server	—
Task 2. Configure VRF Information for the Customer Group.	On the VHG/PE	On the NAS/PE
Task 3. Configure VPDN Information for the Customer Group (L2TP only).	On the VHG/PE	—
Task 4. Configure Authentication and Authorization.	On one of the following, depending on how you are handling authentication and authorization: <ul style="list-style-type: none"> VHG/PE SP AAA RADIUS server (Proxy) SP AAA RADIUS server and customer AAA RADIUS server 	On the SP AAA server

Table 3-1 Checklist of Tasks for Dial-in Provisioning (continued)

Task	L2TP Dial-In	Direct ISDN PE Dial-In
Task 5. Configure Accounting Between the VHG/PE or NAS/PE and the Access Registrar.	On VHG/PE	On NAS/PE
Task 6. Configure Address Management.	On VHG/PE or On SP AAA server	On NAS/PE or On SP AAA server
Task 7. (If You Are Using MLP) Configure LCP Renegotiation and Enable MLP for Users in the Group.	On VHG/PE	On NAS/PE
Task 8. (If You Are Using MMP) Configure SGBP on Each Stack Group Member.	On each VHG/PE in the stack group	On each NAS/PE in the stack group

Miscellaneous Component Configurations

For miscellaneous component configuration details, refer to the documentation listed in Table 3-2.

Table 3-2 Miscellaneous component configurations

Component	Documentation Location
Cisco Access Registrar	http://www.univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm
Cisco Network Registrar	http://www.univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/index.htm
MPLS VPN PE (IOS Release 12.2x)	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt3/xcftagc.htm
MPLS VPNSC 2.1	http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vpnsc/mpls/2_1/index.htm

Initial, One-Time Setup Tasks

These tasks are done once and are not specific to a particular customer or VPN.

Task 1. Configure the PE Routers for MPLS

In L2TP dial-in, configure the VHG/PE routers. In direct ISDN PE dial-in, configure the NAS/PE routers. Perform the following steps:

-
- Step 1 Configure the loopback interface:
Router (config)# **interface loopback** [number]
 - Step 2 Configure IGP (OSPF or IS-IS).



Note For details on configuring OSPF, refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfsf.htm.

For details on configuring IS-IS, refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfisis.htm

- Step 3** On the interface connected to the MPLS core, use the following commands to configure CEF and label switching:
- Router (config)# **ip cef**
 - Router (config-if)# **tag-switching ip**
- Step 4** Use the following commands to configure a BGP peer from the VHG/PE or the NAS/PE to loop back on the remote PEs:
- Router (config)# **router bgp** [*autonomous system number of sp*]
 - Router (config-router)# **neighbor** [*ip address of the first remote pe*] **remote-as** [*same autonomous number*]
 - Router (config-router)# **neighbor** [*ip address of first remote pe*] **update-source Loopback0**
 - Repeat (b) and (c) for each remote PE.
- Step 5** Use the following commands to configure the BGP session to exchange VPN-IPV4 route prefixes for each remote PE:
- Router (config-router)# **address-family vpnv4**
 - Router (config-router-af)# **neighbor** [*ip address of first remote pe*] **activate**
 - Router (config-router-af)# **neighbor** [*ip address of first remote pe*] **send-community extended**
 - Repeat (b) and (c) for each remote PE.

Table 3-3 provides links to relevant Cisco router configuration documentation.

Table 3-3 PE Routers and Configuration Documentation

Platform	Documentation Location
Cisco 7200-NPE300/NPE400 series routers	http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:7200&s=Hardware_Info#Hardware_Installation_%26_Configuration
Cisco 7500 series routers	http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/cicg7500/cicg75bc.htm
Cisco 6400-NRP1/NRP2 series routers	http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/sw_setup/ss_nrp.htm

Task 2. Configure the SP AAA RADIUS Server with Client Information

You must perform this task if you are using a AAA RADIUS server in your network to provide address management or user authentication, authorization, and accounting.

On the AAA RADIUS server, perform the steps in the following section to configure the Cisco Access Registrar (AR) application with information for either of the following dial-in situations:

- L2TP dial-in, where the SP AAA RADIUS server can be queried for user information by the VHG/PE, or for L2TP information by the NAS/LAC, or both.
- Direct ISDN PE dial-in, where the AAA SP RADIUS server is queried by the NAS/PE.

Configure the SP AAA RADIUS Server for L2TP Dial-In

-
- Step 1** Use the following commands to configure the NAS/LAC client information:
- Enter CLI configuration mode of AR:
admin@sun-ar% aregcmd -s
 - Change to the client directory:
--> cd /radius/clients
 - Add the NAS/LAC router name to the client directory:
--> add [name of NAS/LAC]
 - Define the IP address and shared key of the NAS/LAC:
--> cd to the new directory
--> set ipaddress [ip address]
--> set sharedsecret [sharedsecret]
- Step 2** Repeat Step 1 to configure VHG/PE client information.
-

Configure the SP AAA RADIUS Server for Direct ISDN PE Dial-In

Use the following commands to configure the NAS/PE client:

-
- Step 1** Enter CLI configuration mode of AR:
admin@sun-ar% aregcmd -s
- Step 2** Change to the client directory:
--> cd /radius/clients
- Step 3** Add the NAS/PE router name to the client directory:
--> add [name of NAS/PE]
- Step 4** Define the IP address and shared key of the NAS/PE :
--> cd to the new directory
--> set ipaddress [ip address]
--> set sharedsecret [sharedsecret]
-

For AR configuration details, refer to <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm>

Task 3. Configure RADIUS AAA on the Querying Device

This task is required if you are using an AAA RADIUS server in your network to provide address management or user authentication, authorization, and accounting.

Perform the following steps on whichever device queries the SP AAA RADIUS server—the NAS/LAC or VHG/PE (in L2TP dial-in) or the NAS/PE (in direct ISDN PE dial-in):

Step 1 Enable the device to use the RADIUS protocol for authorization and authentication:

- a. Router (config)# **aaa new-model**
- b. Router (config)# **aaa authentication ppp default local group radius**
- c. Router (config)# **aaa authorization network default local group radius**

Step 2 Use the following command to configure the RADIUS server on the device:

Router (config)# **radius-server host** [*ip address of radius server*] **key** [*sharedsecret*]



Note The sharedsecret must match the sharedsecret defined in Step 1d of “[Task 2. Configure the SP AAA RADIUS Server with Client Information](#)” on page 3-4.

Task 4. On the RADIUS AAA Server, Configure a Per-user Static Route Using the Framed-route Attribute

To use the cisco VSA route command, enter:

```
cisco-avpair "ip:route = vrf vrf-name 10.10.100.0 255.255.255.0 [next hop ip address(opt)]"
```

To use the framed route attribute, enter:

```
framed-route = 10.10.100.0 255.255.255.0 [next hop ip address(opt)]
```

To use the framed-ip-address /framed-netmask (same function as framed route above), enter:

```
framed-route = 10.10.100.0/24 [next hop ip address(opt)]
```

Example 3-1 Example of RADIUS Access Registrar Configuration

```
[ //localhost/Radius/Profiles/827-fr/Attributes ]
cisco-avpair = "lcp:interface-config#1= ip vrf forwarding FRtest.com"
cisco-avpair = "lcp:interface-config#2= ip unnumbered FastEthernet0/0"
cisco-avpair = "lcp:interface-config#3= encapsulation ppp"
Framed-IP-Address = 10.10.8.1
Framed-IP-Netmask = 255.255.255.224
Framed-Protocol = ppp
Framed-Routing = None
Service-Type = Framed
```

Adding New Customer Groups

Perform the tasks described in the following sections for each new customer group.

Task 1. Configure L2TP Information for New Customers (L2TP only)

To configure L2TP information for new customers, do one of the following. The option you select depends on where the L2TP information is stored, on the NAS/LAC or on the AAA server.

- [Option 1. Configure L2TP Information Locally on the NAS/LAC](#)
- [Option 2. Configure L2TP Information on the AAA Server](#)

Option 1. Configure L2TP Information Locally on the NAS/LAC

Perform the following steps to configure local L2TP information on the NAS/LAC:

-
- Step 1** Enable VPDN on the access server:
- ```
Router (config)# vpdn enable
```
- Step 2** Enable the search order to look up L2TP tunnels:
- ```
Router (config)# vpdn search-order domain dnis
```
- Step 3** Define a new VPDN group for each user:
- Router (config)# **vpdn-group** *[number]*
 - Router (config-vpdn)# **request-dialin**
 - Router (config-vpdn-req-in)# **protocol l2tp**
 - Router (config-vpdn-req-in)# **domain** *[domain name]*



Note Use the domain name syntax for VPDN customers and the **dnis** *[number]* syntax for DNIS customers.

- Router (config-vpdn-req-in)# **exit**
 - Router (config-vpdn)# **initiate-to ip** *[ip address of VHG]*
- Step 4** Define a local username and password for tunnel authentication:
- ```
Router (config)# username [hostname] password [tunnel password]
```




---

**Note** By default, the host name used in the L2TP tunnel authentication is the host name of the router. You can change this by adding the following command to the VPDN group:

```
Router (config-vpdn)# local name [hostname]
```

---

### Option 2. Configure L2TP Information on the AAA Server

Perform the following steps to configure L2TP information on the AAA server:

- 
- Step 1** On the NAS/LAC, enable VPDN:
- ```
Router (config)# vpdn enable
```
- Step 2** Enable the search order to look up L2TP tunnels:
- ```
Router (config)# vpdn search-order domain dnis
```

**Step 3** On the AAA server, enable AAA to look up L2TP information. For details, see “Task 3. Configure RADIUS AAA on the Querying Device” on page 3-6.

**Step 4** On the AAA server, configure the AR to receive L2TP information:

a. Add a service to the AR:

```
--> add /Radius/Services/[service name] [service name description] local "" "" RejectAll ""
[userlist name]
--> set /Radius/DefaultAuthenticationService [service name]
--> set /Radius/DefaultAuthorizationService [service name]
```



**Note** You can also select the authentication and authorization service with scripting. For Access Registrar (AR) configuration details, refer to <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm>.

b. Add a user list to the AR:

```
--> add /Radius/Userlists/[userlist name]
```



**Note** The user list name must match the user list name defined in Step a. Add a service to the AR:

c. Add tunnel names to user lists:

```
--> add /Radius/UserLists/[userlist name]/[domain name] [domain name description] cisco TRUE
"" [attributes list]
```



**Note** The userlist name must match the userlist name defined in Step a, “Add a service to the AR:”.



**Note** All user records inside the AR database containing tunnel information must have **cisco** entered in the password field.

The command for adding a DNIS user is:

```
--> add /Radius/UserLists/[userlist name]/dnis:[dnis number] [dnis description] cisco TRUE ""
[attributes list]
```

d. Add tunnel attributes:

```
--> add /Radius/Profiles/[attributes list]
--> cd /Radius/Profiles/[attributes list]/Attributes
--> set tunnel-medium-type_tag1 1
--> set tunnel-password_tag1 [tunnel password]
--> set tunnel-server-endpoint_tag1 [vhg ip address]
--> set tunnel-type_tag1 3
```



**Note** If you are using AR 1.6 Revision 1 or higher, the syntax for the following commands changes from what is given above:

```
--> set tunnel-medium-type_tag1 ipv4
--> set tunnel-type_tag1 l2tp
```

## Task 2. Configure VRF Information for the Customer Group

To configure the customer virtual routing/forwarding instance (VRF), which is information associated with a specific VPN, perform the following steps on the VHG/PE or NAS/PE.



**Note** Before you begin, make sure you have performed the initial BGP configuration in [“Task 1. Configure the PE Routers for MPLS”](#) on page 3-3.

- Step 1** Define the VRF:
- Router (config)# **ip vrf** [*vpn name*]
  - Router (config-vrf)# **rd** [*route descriptor value*]
  - Router (config-vrf)# **route-target import** [*route target value*]
  - Router (config-vrf)# **route-target export** [*route target value*]
- Step 2** Configure the loopback interface:
- Router (config)# **interface loopback** [*number*]
  - Router (config-if)# **ip vrf forwarding** [*vpn name*]



**Note** The vpn name must match that defined in Step 1a above.

- Router (config-if)# **ip address** [*ip address*] [*netmask*]
- Step 3** Configure the BGP session to transport VRF information:
- Router (config)# **router bgp** [*autonomous system number*]



**Note** The autonomous system number must match that defined in Step 4a of [“Task 1. Configure the PE Routers for MPLS”](#) on page 3-3.

- Router (config-router)# **address-family ipv4 vrf** [*vpn name*]
- Router (config-router-af)# **redistribute connected metric 1**

## Task 3. Configure VPDN Information for the Customer Group (L2TP only)

To configure VPDN information for the customer group, perform the following steps:

---

**Step 1** Enable VPDN on the VHG/PE:

Router (config)# **vpdn enable**

**Step 2** Define a new VPDN group for each user:




---

**Note** VPDN on a home gateway is stored locally on the VHG/PE.

---

- a. Router (config)# **vpdn-group** *[number]*
- b. Router (config-vpdn)# **accept-dialin**
- c. Router (config-vpdn-acc-in)# **protocol l2tp**
- d. Router (config-vpdn-acc-in)# **virtual-template** *[virtual template number]*
- e. Router (config-vpdn-acc-in)# **exit**
- f. Router (config-vpdn)# **terminate-from hostname** *[hostname]*




---

**Note** The host name must match the host name defined in Step 4 of “[Task 1. Configure L2TP Information for New Customers \(L2TP only\)](#)” on page 3-7.

---

**Step 3** Define a local username and password for tunnel authentication:

Router (config)# **username** *[hostname]* **password** *[tunnel password]*

---

## Task 4. Configure Authentication and Authorization

To configure components where user authentication and authorization take place, use one of the following options. (The choice you make depends on your strategy for authentication and authorization.)

- [Option 1. Configure Local Authentication on the VHG/PE \(L2TP Only\)](#).
- [Option 2. Configure Authorization and Authentication on the SP AAA RADIUS Server](#).
- [Option 3. Configure Proxy AAA \(L2TP Only\)](#). Here the SP AAA RADIUS server queries the customer AAA RADIUS server.
- [Task 4. On the RADIUS AAA Server, Configure a Per-user Static Route Using the Framed-route Attribute](#).

### Option 1. Configure Local Authentication on the VHG/PE (L2TP Only)




---

**Note** Local authentication is not used with direct ISDN PE dial-in.

---

To configure user authentication and authorization on the VHG/PE, perform the following steps:

---

**Step 1** Create a virtual template:

- a. Router (config)# **interface virtual-template** *[number]*



**Note** The virtual template number must match the virtual template number defined in Step 2d of “[Task 2. Configure VRF Information for the Customer Group](#)” on page 3-9.

b. Router (config-if)# **ip vrf forwarding** [vpn name]



**Note** The vpn name must match the vpn name in Step 1a of “[Task 2. Configure VRF Information for the Customer Group](#)” on page 3-9.

c. Router (config-if)# **ip unnumbered loopback** [loopback number]



**Note** The loopback number must match the loopback number in Step 2a of “[Task 2. Configure VRF Information for the Customer Group](#)” on page 3-9.

d. Router (config-if)# **ppp authentication chap callin**

**Step 2** For each user in the customer group, use the following command to configure a username and password:

Router (config)# **username** [username@domain] **password** [user password]

## Option 2. Configure Authorization and Authentication on the SP AAA RADIUS Server

To configure user authentication and authorization on the SP AAA RADIUS server, perform the following steps:

**Step 1** Configure the VHG/PE or NAS/PE with information on the MPLS group:

- a. Router (config)# **aaa new-model**
- b. Router (config)# **aaa authentication ppp default local group radius**
- c. Router (config)# **aaa authorization ppp default local group radius**
- d. Router (config)# **virtual-profile aaa**
- e. Router (config)# **interface virtual-template** [number]



**Note** The virtual template number must match the virtual template number in Step 2d of “[Task 2. Configure VRF Information for the Customer Group](#)” on page 3-9.

f. Router (config-if)# **ppp authentication chap callin**

g. Router (config-if)# **exit**

h. Router (config)# **radius-server host** [radius server ip address] **key** [sharedsecret]

**Step 2** Configure the AR with VHG/PE or NAS/PE client information:

- a. Add the VHG/PE or NAS/PE as a client:

```
--> add /Radius/Clients/[vhg name] [vhg description] [vhg ip address] [sharedsecret] NAS ""
[script]
```



**Note** The script indicates which service needs to be selected for VPDN user authorization and authentication.

- b. Add the service:

```
--> add /Radius/Services/[vpdn name] {vpdn description} local "" "" RejectAll "" [vpdn userlist name]
```



**Note** The VPDN name is derived from the username that is sent by the VHG within the RADIUS access request packet. This information is provided by the script in Step 2a. For scripting procedures, refer to <http://www.univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm>.

- c. Add the user list:

```
--> add /Radius/Userlists/[vpdn userlist name]
```

- d. Add individual VPDN users for the user list:

```
--> add /Radius/UserLists/[vpdn userlist name]/[vpdn username] [vpdn user description] [vpdn user password] TRUE "" [vpdn user attributes]
```

- e. Define attributes for selecting the VPN service:

```
--> add /Radius/Profiles/[vpdn user attributes]
```

```
--> cd /Radius/Profiles/[vpdn user attributes]/Attributes
```

```
--> set service-type framed
```

```
--> set framed-protocol ppp
```

```
--> set cisco-avpair "lcp:interface-config=ip vrf forwarding [vpn name]\\n ip unnumbered Loopback [number]"
```



**Note** If you are configuring dial backup, see “Option 1. Configure Static Routing” on page 3-18.



**Note** The vpn name must match the vpn name in Step 1a of “Task 2. Configure VRF Information for the Customer Group” on page 3-9.



**Note** The loopback number must match the loopback number in Step 2a of “Task 2. Configure VRF Information for the Customer Group” on page 3-9.

### Option 3. Configure Proxy AAA (L2TP Only)

To configure proxy AAA, perform the following steps:

- Step 1** Configure the VHG/PE:

- a. Router (config)# **aaa new-model**

- b. Router (config)# **aaa authentication ppp default local group radius**
- c. Router (config)# **aaa authorization ppp default local group radius**
- d. Router (config)# **virtual-profile aaa**
- e. Router (config)# **interface virtual-template** *[number]*



**Note** The virtual template number must match the virtual template number defined in Step 2d of “Task 2. Configure VRF Information for the Customer Group” on page 3-9.

- f. Router (config-if)# **ppp authentication chap callin**
- g. Router (config-if)# **exit**
- h. Router (config)# **radius-server host** *[radius server ip address]* **key** *[sharedsecret]*

**Step 2** Configure the SP AAA RADIUS server:

- a. Add the VHG as a client:

```
--> add /Radius/Clients/[vhg name] [vhg description] [vhg ip address] [sharedsecret] NAS ""
[script]
```



**Note** The script indicates which service needs to be selected for VPDN user authorization and authentication.

- b. Add remote AA servers to which you proxy AA information:

```
--> add /Radius/RemoteServers/[remote server host name] [remote server description] radius
[remote server ip address] 1645 300000 [sharedsecret]
```



**Note** The remote server IP address cannot be reached from the SP AAA server because the MPLS service provider cloud does not have VPN customer routing information. To provide the SP AAA server with routing information, use route leaking or a management VPN. For information on VPN management refer to <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vpnsc/mpls/index.htm>.

- c. Add a service:

```
--> add /Radius/Services/[vpdn name] [vpdn description] radius
--> cd /Radius/Services/[vpdn name] RemoteServers
--> set 1 [remote server host name]
```



**Note** The VPDN name is derived from the username that is sent by the VHG/PE in the RADIUS access request packet. This information is provided by the script in Step 2a. For scripting procedures, refer to <http://www.univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm>.

## Task 5. Configure Accounting Between the VHG/PE or NAS/PE and the Access Registrar

To configure accounting between the VHG/PE or NAS/PE and the AR, perform the following steps:

**Note**

Make sure you have performed the configuration of the user authentication and authorization on your AAA server, described in “[Task 4. Configure Authentication and Authorization](#)” on page 3-10.

**Step 1** Configure the VHG/PE.

- a. Router (config)# **aaa accounting network default start-stop group radius**

**Step 2** Configure the AR.

```
--> add /radius/services/[accounting service name]
--> cd /radius/services/[accounting service name]
--> set type file
```

**Note**

The accounting service name is derived from the username that is sent by the VHG/PE in the RADIUS accounting request packet. This information is provided by the script in Step 2a. For scripting procedures, refer to <http://www.univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm>.

## Task 6. Configure Address Management

Configure address management using one of the following procedures. The procedure you select depends on the address management strategy you are using.

- [Option 1. Configure Local Overlapping Address Pools on the VHG/PE or NAS/PE](#)
- [Option 2. Configure Address Management on the SP AAA RADIUS Server](#)
- [Option 3. Configure ODAP on the VHG/PE or NAS/PE](#)
- [Option 4. Configure the RADIUS AR for ODAP](#)

### Option 1. Configure Local Overlapping Address Pools on the VHG/PE or NAS/PE

To configure address management using local overlapping address pools, perform the following steps on the VHG/PE or NAS/PE:

**Step 1** Create an address pool on the VHG/PE:

```
Router (config)# ip local pool [vpn customer address pool] [start ip address] [end ip address]
```

**Step 2** Perform one of the following steps. The step you select depends on how you configured user authentication and authorization in “[Task 4. Configure Authentication and Authorization](#)” on page 3-10.

- If you configured user authentication and authorization on the VHG/PE, add the following command to the virtual template configuration:

```
Router (config-if)# peer default ip address pool [vpn customer address pool]
```

- If you configured user authentication and authorization on the AAA server, add the following command to the attributes for selecting VPN service:

```
--> set cisco-avpair "lcp:interface-config=ip vrf forwarding [vpn name]\\n ip unnumbered Loopback[number]\\n peer default ip address pool [vpn customer address pool]"
```

## Option 2. Configure Address Management on the SP AAA RADIUS Server

To configure address management on the SP AAA RADIUS server, perform the following steps.



**Note** Make sure you have performed the accounting configuration in “[Task 5. Configure Accounting Between the VHG/PE or NAS/PE and the Access Registrar](#)” on page 3-13. Accounting is mandatory for address management on a RADIUS server.

- Step 1** Define the resource manager:
- a. --> **add /Radius/ResourceManagers/[resource manager for vpn customer]**
  - b. --> **cd /Radius/ResourceManagers/[resource manager for vpn customer]**
  - c. --> **set type ip-dynamic**
  - d. --> **set netmask 255.255.255.255**
  - e. --> **cd IPAddresses**
  - f. --> **add [ip address range for address pool]**
- Step 2** Define the session manager:
- a. --> **add /Radius/SessionManagers/[session manager name ]**
  - b. --> **cd /Radius/SessionManagers/[session manager name]/ResourceManagers**
  - c. --> **add 1 [resource manager for vpn customer]**



**Note** The session manager name is derived from the domain name that is sent by the VHG/PE in the RADIUS access request packet. This information is provided by the script in Step 2a. For scripting procedures, refer to <http://www.univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm>.

## Option 3. Configure ODAP on the VHG/PE or NAS/PE

If you are implementing ODAP, perform the following steps on VHG/PE or NAS/PE.

- Step 1** Configure a DHCP address pool on a Cisco IOS DHCP server.
- ```
Router(config)# ip dhcp pool address pool name
```
- Step 2** Tie the pool to a particular VPN.
- a. Router(config-dhcp)# **vpn type 1 vrf name**
 - b. Router(config-dhcp)# **origin aaa autogrow size**
- Step 3** Configure the network access server to recognize and use vendor-specific attributes.
- a. Router(config)# **radius-server host ip address**
 - b. Router(config)# **radius-server key string**
 - c. Router(config)# **radius-server vsa send accounting**
 - d. Router(config)# **radius-server vsa send authentication**
- Step 4** Enable an address pooling mechanism used to supply IP addresses.

```
Router(config)# ip address-pool dhcp-pool
```

Step 5 Create a virtual template interface.

```
Router(config)# interface virtual-template number
```

Step 6 Specify an address from the DHCP mechanism to be returned to a remote peer connecting to this virtual-template interface.

```
Router(config-if)# peer default ip address dhcp-pool
```



Note

Since the user name might be the same as the VPDN domain name, either use scripts on the RADIUS AR to differentiate between requests for subnets and VPDN information, or make the VRF name different from the domain name.

Example 3-2 ODAP Configuration Example

```
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius (to release subnets accounting
needed)
ip dhcp pool odap-test vrf <vrf-name> (part of access-request username)
origin aaa subnet size initial /27 autogrow /27
radius-server host 10.10.100.3 radius-server key wwradius-server vsa send accounting (VSA
attributes in accounting packet)
radius-server vsa send authentication (VSA attributes in access-request packet)
ip address-pool dhcp-pool (global command - use local DHCP VRF pools)
int virtual-template X
peer default ip address dhcp-pool
```

Option 4. Configure the RADIUS AR for ODAP

To configure the RADIUS AR for ODAP, use a script that accomplishes the following:

- Selects a service with its name *<vrf name>-odap* and a session manager with the same name as the service
- Configures the resource manager for ODAP

Cisco AR 1.7 R1 has been enhanced to make ODAP functionality more accessible and to enable ODAP requests and normal user authentication to occur on the same Cisco AR server. To achieve this functionality, a new Cisco vendor script **CiscoWithODAPIncomingScript** was written to direct ODAP requests to particular services and session managers. **CiscoWithODAPIncomingScript** also provides the same functionality as the previous **CiscoIncomingScript**.

Additionally, Cisco AR 1.7 R1 has a new vendor type, **CiscoWithODAP** which references **CiscoWithODAPIncomingScript** as its IncomingScript and references the existing script, **CiscoOutgoingScript**, as its Outgoing Script.

For Cisco AR configuration details, see

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/users/odap.htm#xtocid1.

Task 7. (If You Are Using MLP) Configure LCP Renegotiation and Enable MLP for Users in the Group

If you are implementing MLP, perform the following steps on the VHG/PE or NAS/PE:

Step 1 (L2TP only) On the VHG/PE, configure LCP renegotiation so that requests from the LAC are not rejected. For each customer group, enter these commands on the VPDN group:

a. Router (config)# **vpdn-group** *[number]*



Note The vpdn-group number is the number defined for this group in “Task 3. Configure VPDN Information for the Customer Group (L2TP only)” on page 3-9.

b. Router (config)# **lcp renegotiation always**



Note Without LCP renegotiation, the NAS/LAC might reject MLP requests during initial LCP negotiation between the dial-in user and the NAS/LAC.

Step 2 Use the following command on the virtual template (in L2TP dial-in) or the physical interface or rotary dialer group (in direct ISDN PE dial-in) to enable MLP for users in the group:

Router (config)# **enable mlppp**



Note Enabling MLP is exactly the same in this context as in a non-MPLS environment. For more information, refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/fnsprt9/dcdppp.htm.

Task 8. (If You Are Using MMP) Configure SGBP on Each Stack Group Member



Note To use MMP, you must also implement MLP. See [Task 7. \(If You Are Using MLP\) Configure LCP Renegotiation and Enable MLP for Users in the Group](#), page 3-16.

If you are implementing MMP, perform the following steps to configure SGBP on each stack group member (VHG/PE or NAS/PE). Do not define more than one stack group on the same router. In this example, you are configuring stack group member C.

Step 1 Define a stack group:

Router (config)# **sgbp group** *<stack-group-name>*

Where *<stack-group-name>* is the name of the stack group. A stack group name is a unique name used for all members of the group.

Step 2 Define the username and the password for stack group member authentication between members of the group:

Router (config)# **user** *<stack-group-name>* **password** *<password>*



Note The username and password must be the same for all members of the group.

- Step 3** Specify the host name and IP address of each stack group peer of this router. For each peer (but not for the local system), enter the following command:

```
Router (config)# sgbp member <peer-name> <peer-ip-address>
```

Provisioning L2TP Dial Backup

You provision L2TP dial backup in the same way as L2TP dial-in (see “[Dial-In Provisioning Checklist](#)” on page 2), with the following differences:

- The same remote CE is used for the primary and the backup link.
- Because dial backup ordinarily connects remote sites, not remote users, to a customer VPN, address assignment is not needed.
- Backup links are typically MLP links, and an IGP routing protocol can be configured on the backup link.
- Static or dynamic routing must be provisioned. Authentication of the remote CE is similar to remote user authentication in L2TP dial-in. If you are managing the CE, the SP AAA server can authenticate the remote CE; proxy authentication is not needed.
- Accounting records, including MLP information, are maintained for the duration of the backup session. As with L2TP dial-in, accounting can be implemented through use of the SP AAA server or AAA proxy.

For more information on dial backup technology, refer to “Dial Backup Configuration” in the *Cisco IOS Dial Technologies Configuration Guide, Release 12.2* at

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/fnsprt6/dcdbakdp.htm.

Configuring Routing on a Backup CE-PE Link

In dial backup, either static or dynamic routing can be used, depending on whether dynamic routing is enabled on the primary link.

If dynamic routing is not enabled on the primary link between the CE and the VHG/PE, you must configure static VRF routes for the backup link on the VHG/PE. When the primary link goes down because of lack of connectivity, the primary static route is withdrawn.

For the backup PPP session, the static route is downloaded from the RADIUS AAA server as part of the virtual profile, and the route is inserted into the appropriate VRF when the backup virtual interface is brought up. When the primary link is restored, the primary static VRF route is also restored, and the CE terminates the backup connection. The PE then deletes the backup static VRF route.

If dynamic routing is enabled on the primary CE-PE link, you should configure dynamic routing for the backup link also.

Option 1. Configure Static Routing

Where static routing is used for the backup link, the static route is configured on the SP RADIUS AAA server as part of the virtual profile and downloaded to the VHG/PE. The route is inserted into the appropriate VRF when the backup virtual interface is brought up.

To configure static routing, perform the following steps:

-
- Step 1** On the AAA RADIUS server, modify the Cisco vendor-specific attribute route command. Change:
- > **cisco-avpair "ip:route = <nexthop IP address netmask>"** (the next hop IP address is optional)
- to
- > **cisco-avpair "ip:route = vrf [vrf-name] <nexthop IP address netmask>"**
- Defining the next hop IP address configures static routing. When the CE requests an IP address for the PPP link, the next hop will be set to this address. (If the next hop is not defined, routing is dynamic.)
- Step 2** Download the above information to the VHG/PE.
-

Option 2. Configure Dynamic Routing

Where you have configured dynamic routing on the primary CE-PE link, also configure dynamic routing on the backup VHG/PE.

To configure dynamic routing, perform the following steps on the VHG/PE:

-
- Step 1** Configure a loopback interface to forward traffic to the appropriate VRF:
- Router (config-if)# **interface loopback 1**
 - Router (config-if)# **ip vrf forwarding [vrf-name]**
- Step 2** Assign an address in a.b.c.d format (an IP address on the VHG/PE) to the loopback interface:
- Router (config-if)# **ip address [a.b.c.d] 255.255.255.255**
- Step 3** Configure the IGP instance (such as RIP, in this example) for this VRF:
- Router (config-if)# **router rip**
 - Router (config-if)# **address-family ipv4 vrf [vrf-name]**
- Step 4** Make network a.b.c.d part of the IGP:
- Router (config-router-at)# **network a.0.0.0**
- For example, if the IP address in Step 2 is 10.10.33.241, enter **network 10.0.0.0**.
- Step 5** Use a virtual template to download virtual access interface-specific settings from the SP AAA RADIUS server.
- Add the service:

--> **add /Radius/Services/[vpdn name] {vpdn description} local "" "" RejectAll "" [vpdn userlist name]**



Note The VPDN name is derived from the PPP session username that is sent by the VHG/PE in the RADIUS access request packet. This information is provided by the script in Task 4, Configure Authentication and Authorization, [Option 2. Configure Authorization and Authentication on the SP AAA RADIUS Server](#). For scripting procedures, refer to <http://www.univercd/cc/td/doc/product/rtrmgmt/cnsar/index.htm>.

- Add the user list:

```
--> add /Radius/Userlists/[vpdn userlist name]
```

- c. Add individual VPDN users for the user list:

```
--> add /Radius/UserLists/[vpdn userlist name]/[vpdn username] [vpdn user description] [vpdn user password] TRUE "" [vpdn user attributes]
```

- d. Define attributes for selecting the VPN service:

```
--> add /Radius/Profiles/[vpdn user attributes]
```

```
--> cd /Radius/Profiles/[vpdn user attributes]/Attributes
```

```
--> set service-type framed
```

```
--> set framed-protocol ppp
```

```
--> set cisco-avpair "lcp:interface-config=ip vrf forwarding [vpn name]\\n ip unnumbered Loopback [number]
```



Note The vpn name must match the vpn name in Step 1a of “[Task 2. Configure VRF Information for the Customer Group](#)” on page 3-9. The loopback number must match the loopback number in Step 2a of “[Task 2. Configure VRF Information for the Customer Group](#)” on page 3-9. The virtual interface should be unnumbered to the loopback interface.



Note If you are using a third-party RADIUS server, use the PPP session username to select the RADIUS record. The RADIUS record should contain the attributes in the **set cisco-avpair** command above.

Provisioning Dial-out Access

Provisioning dial-out access is similar to provisioning dial-in access, with these exceptions:

- For users to be able to place dial-out calls, you must configure dialer profiles on the VHG/PE (in L2TP dial-out) or on the NAS/PE (in direct ISDN PE dial-out).
- No AAA RADIUS configuration is needed, because user information is directly implemented on the dialer profile interface configured on the dial-out router.

Before You Begin

The procedures provided here are specific to provisioning remote access to an MPLS VPN and are based on two assumptions:

1. That the following setup and configuration tasks have already been carried out:
 - Setup of the MPLS core network
 - Setup of the customer VPN
 - Configuration of the links between the PE and the CE

- That you have a good understanding of the architecture and features you are using and that you have selected the means you will use for implementing those features (for example, which of several strategies you will use for address management or for user authentication and authorization).

See [Chapter 2, “Overview of Dial Access to MPLS VPN Integration”](#) for information that will help you understand the dial architectures and decide on your implementation approach.

Dial-Out Provisioning Checklist

[Table 3-4](#) lists tasks for dial-out provisioning. Procedures for completing each task are described in the sections that follow. If you are viewing this document online, you can click on highlighted text to get details on the procedure.

Table 3-4 Checklist of Tasks for Dial-out Provisioning

Task	L2TP Dial-Out	Direct ISDN PE Dial-Out
Before you begin, read the Cisco Remote Access to MPLS VPN Integration 2.0 Release Notes at http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/rampls2/relnote/index.htm		
Task 1. Configure the Dialer Profile.	On the VHG/PE	On the NAS/PE
Task 2. Configure the VPDN Group (L2TP Only).	On the VHG/PE	—
Task 3. Configure a Static Route in the Customer VRF.	On the VHG/PE and On the NAS	On the NAS/PE
Task 4. Configure VPDN on the NAS (L2TP only).	On the NAS	—

Miscellaneous Component Configurations

For miscellaneous component configuration details, see [Table 3-2](#).

Task 1. Configure the Dialer Profile

In this task, you configure a dialer profile (on the VHG/PE or NAS/PE) to be part of the customer VRF. In L2TP dial-out, you also configure the dialer profile to use a VPDN group.

-
- Step 1** On the VHG/PE or NAS/PE, include the following command in the dialer profile:
- ```
Router (config-if)# ip vrf forwarding [vpn name]
```
- Step 2** (L2TP only) On the VHG/PE, include the **dialer vpdn** command in the dialer profile to configure the dialer profile for L2TP:
- ```
Router (config-if)# dialer vpdn
```
-

In [Example 3-3](#), the commands listed above are in bold. The dialer profile defined is Dialer50. The vpn name is V1.17.com. The dialer pool number, 4, is referenced in the configuration of the VPDN group in [Task 2](#).

Example 3-3 VHG/PE Dialer Profile Configuration (L2TP dial-out)

```

interface Dialer50
  ip vrf forwarding V1.17.com
  ip unnumbered Loopback172
  encapsulation ppp
  no keepalive
  dialer pool 4
  dialer remote-name U0001N1P4V1.17@V1.17.com
  dialer idle-timeout 200000
  dialer string 11710
  dialer load-threshold 5 either
  dialer vpdn
  dialer-group 1
  peer default ip address 42.1.17.10
  no cdp enable
  ppp authentication chap callin
  ppp chap hostname dialout
  ppp chap password 7 071836
  ppp multilink
  multilink load-threshold 5 outbound
end

```

**Note**

The **dialer-group** command specifies which dialer list to use. In the example, dialer-group 1 is linked to **dialer-list 1 protocol ip permit**, a global command that, like an access list, tells the router which traffic (in this case, all IP traffic) will trigger the dialer profile and thus the call. Alternatively, you can use an access list to filter out routing updates or allow only HTTP traffic (URL requests) to trigger a call.

For more information on configuring dialer profiles, see

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/fnsprt5/dcdiprof.htm.

Task 2. Configure the VPDN Group (L2TP Only)

This task applies to L2TP dial-out only. In this task, you configure the VPDN group as a pool member of the dialer pool defined in the dialer profile in Task 1.

On the VHG/PE, use the following command to configure the VPDN group as a pool member:

```
Router (config-vpdn-group)# pool-member [pool number]
```

In [Example 3-4](#), the pool-member corresponds to the pool number in the dialer profile configured in Task 1.

Example 3-4 VHG/PE VPDN Group Configuration

```

vpdn-group V1.17
  request-dialout
  protocol l2tp
  pool-member 4
  initiate-to ip 10.10.104.36
  local name c72d2-2-V1.17
  source-ip 10.10.104.12
  l2tp tunnel password <password>

```

The **l2tp tunnel password** command overrides the default password in the local user database. You can also define a username for the local name in the global configuration. To do so, use this command:

```
Router (config)# username c72d2-2-V1.17 password <password>
```

Task 3. Configure a Static Route in the Customer VRF

In this task, you configure the customer VRF (on the VHG/PE or NAS/PE) with a static route for this dial-out user. This will attract traffic to the appropriate remote CE.

On the VHG/PE, in the customer VRF use this command to configure a static route for this dial-out user:

```
Router (vrf)# ip route vrf [vpnname][CE ip address] 255.255.255.255 Dialer50 permanent
```

Task 4. Configure VPDN on the NAS (L2TP only)

Perform the following steps to configure VPDN for dial-out on the NAS. See [Example 3-5](#) for a configuration example.

Step 1 Enable VPDN:

```
Router (config)# vpdn enable
```

Step 2 Configure the VPDN group to accept dial-out (when the VHG/PE requests a tunnel and attempts to trigger a session):

- a. Router (config)# **vpdn-group** [number]
- b. Router (config-vpdn)# **accept-dialout**
- c. Router (config-vpdn-acc-out)# **protocol l2tp**

```
Router (config-vpdn-group-acc-out)# dialer 1
```



Note dialer 1 specifies the dialer that is used to dial out to the client.

- d. Router (config-vpdn-acc-out)# **exit**
- e. Router (config-vpdn)# **terminate-from hostname** [hostname]



Note L2TP tunnels that have this hostname will be accepted.

Step 3 Configure the tunnel secret to be used for VPN tunnel authentication for this VPDN group:

```
Router (config)# l2tp tunnel password [tunnel password]
```



Note The secret must match that used in the VPDN group on the VHG/PE or the entry in the local user password database.

Step 4 On the dialer interface, enable dial-on-demand routing:

```
Router (config-if)# dialer aaa
```



Note This enables the dialer to use the AAA server to locate the profiles to use for dialing information. When the VHG/PE sends dialer string attributes, the rotary group will trigger the call.

Step 5 On the physical dialer interface, use this command to reference the rotary group dialer 1:

```
Router (config)# interface serial [physical dialer interface]
```

Router (config-ip)# **dialer rotary-group 1**

Example 3-5 NAS VPDN Group Configuration

```

vpdn enable

vpdn-group V1.17
  accept-dialout
  protocol l2tp
  dialer 1

/*Specifies the dialer that is used to dial out to the client. */

terminate-from hostname c72d9-1-V1.4

/*Accepts L2TP tunnels that have this host name configured as a local name. */

l2tp tunnel password 7 <password>

/*Configures the tunnel secret that will be used for VPN tunnel authentication for this
VPN group. This password must match that configured in Task 2 in the VPDN group on the
VHG/PE or the entry in the local user password database.*/

source-ip 10.10.104.22
!
interface Dialer1
  ip unnumbered Loopback0
  encapsulation ppp
  no keepalive
  dialer in-band

/*Enables DDR on Dialer */

dialer aaa

/* Enables the dialer to use the AAA server to locate profiles for dialing information. */

dialer-group 1
no cdp enable
ppp authentication chap callin
!
```

Sample Configurations

This section includes sample configurations. The examples are presented as illustrations only; your configuration specifics depend on how you are implementing remote access to MPLS VPN and will vary from what is presented here. The relevant commands for remote access to MPLS VPN are in bold and are described in italicized comments.

Sample Configurations for L2TP Dial-In

Sample NAS Configuration

On the NAS, you configure the VPDN group that will bring up the L2TP tunnel to the VHG/PE.

**Note**

All MPLS VPN-relevant commands are configured on the VHG/PE, not the NAS.

Example 3-6 NAS Sample Configuration

```

Router# show run
version 12.2
no service pad
service tcp-keepalives-in
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
!
hostname c54d2-1
!
enable secret <password>.
enable password <password>
!
username c54d2-1-V1.1 password 0 ww
resource-pool disable
call rsvp-sync
dial-tdm-clock priority 1 6/0
!
!
! - VPDN configuration:
vpdn enable
vpdn search-order domain dnis
! - Look up VPDN by domain and then by DNIS
!
! - Configuration for a VPDN group (in this example, V1.1):
vpdn-group V1.1
    request-dialin
        protocol l2tp
        domain V1.1.com
initiate-to ip 10.10.104.12
local name c54d2-1-V1.1
! - Name used on this NAS, used on VHG in terminate-from hostname c54d2-1-V1.1
source-ip 10.10.104.36
! - Loopback interface
!
controller E1 6/0
pri-group timeslots 1-31
!
interface Loopback0
ip address 10.10.104.36 255.255.255.255
!
interface FastEthernet0/0
ip address 10.10.145.3 255.255.255.0
!
interface Serial6/0:15
no ip address
encapsulation ppp
dialer rotary-group 1
isdn switch-type primary-net5
ppp authentication chap callin
!
interface Dialer1
ip unnumbered Loopback0
encapsulation ppp
no ip route-cache
no ip mroute-cache

```

```

dialer in-band
ppp authentication chap callin
!
router ospf 100
log-adjacency-changes
network 10.10.0.0 0.0.255.255 area 0
!
ip classless
no ip http server
ip pim bidir-enable
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
logging synchronous
line vty 0 4
exec-timeout 0 0
login
!
end

```

Sample VHG/PE Configuration

In this example, the VHG/PE is configured to terminate L2TP sessions received from the NAS and query the RADIUS server for dial options authorized for a given dial-in user.

Example 3-7 VHG/PE Sample Configuration

```

Router# sh run
version 12.2
service tcp-keepalives-in
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
hostname c72d2-2
! - RADIUS request:
aaa new-model
aaa authentication login default none
aaa authentication ppp default local group radius
! - Look for user name in local database, if not found, look on RADIUS
aaa authorization network default local group radius
! - Similarly for network authorization
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius
aaa session-id common
enable secret <password>
enable password <password>
!
! - Authenticate user and L2TP tunnel locally:
username c72d2-2 password 0 ww
( since no local name defined on vpdn group in this example the VHG/PE will use its
hostname as the username in the L2TP authentication process for the tunnel)
ip subnet-zero
!
!
ip vrf V1.1.com
rd 1:1
route-target export 1:1

```

```

route-target import 1:1
!
vpdn enable
vpdn search-order domain dnis
!
! - Bind the user coming from NAS c54d2-1-V1.1 to this profile (V1.1.) and use virtual
template 1:
vpdn-group V1.1
    accept-dialin
        protocol l2tp
        virtual-template 1
terminate-from hostname c54d2-1-V1.1
lcp renegotiation always
source-ip 10.10.104.12
! - Note that the VHG/PE clones a virtual access interface (a set of generic IOS commands)
from the specified virtual template. If per-user configuration is also used (through the
virtual-profile aaa command), the VHG/PE queries the RADIUS server to authenticate the PPP
user with a username and password.
!
tag-switching tdp router-id Loopback0
!
interface Loopback0
ip address 10.10.104.12 255.255.255.255
!
interface Loopback1
ip vrf forwarding V1.1.com
ip address 42.1.1.241 255.255.255.255
!
interface FastEthernet0/0
ip address 10.10.145.1 255.255.255.0
!
interface POS5/0
ip address 10.10.103.33 255.255.255.252
tag-switching ip
!
! - Configuration from the template; multilink is enabled
interface Virtual-Templatel
no peer default ip address
ppp authentication chap callin
ppp multilink
!
router ospf 100
log-adjacency-changes
network 10.10.0.0 0.0.255.255 area 0
!
router bgp 100
no synchronization
bgp log-neighbor-changes
neighbor 10.10.104.31 remote-as 100
neighbor 10.10.104.31 update-source Loopback0
neighbor 10.10.104.31 soft-reconfiguration inbound
neighbor 10.10.104.35 remote-as 100
neighbor 10.10.104.35 update-source Loopback0
no auto-summary
!
address-family ipv4 vrf V1.1.com
redistribute connected metric 1
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.10.104.31 activate
neighbor 10.10.104.31 send-community extended

```

```

neighbor 10.10.104.35 activate
neighbor 10.10.104.35 send-community extended
no auto-summary
exit-address-family
!
ip local pool V1.1-pool 42.1.1.10 42.1.1.19 group V1.1-group

ip classless
!
ip radius source-interface Loopback0
! - The IP source is changed to the loopback interface
!
radius-server host 10.10.100.6 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key ww
call rsvp-sync
mgcp profile default
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
!
end

```

Sample SP AAA Server Configuration

In this example, the SP AAA server is configured to:

- Add the VHG/PE as a RADIUS client
- Add a RADIUS service specifying that the list of users is found in a local database
- Add a user list and users to populate the database
- Add attributes for those users, to be provided (in the access-accept packet) upon request from the VHG/PE. Attributes can also come from the customer AAA server

In the example, you are assumed to be logged in to the RADIUS host and to have accessed the Access Registrar application.



Note

Be sure that you save and reload after changing the Access Registrar configuration.

Example 3-8 SP AAA Sample Configuration

```

--> cd      c72d2-2
[ //localhost/Radius/Clients/c72d2-2 ]
  Name = c72d2-2
  Description = c72d2-2
  IPAddress = 10.10.104.12
  SharedSecret = ww
  Type = NAS
  Vendor =
  IncomingScript~ = ParseAARealm
  OutgoingScript~ =
  UseDNIS = FALSE
  DeviceName =
  DevicePassword =

```

```

--> cd /radius/scripts/ParseAAAREalm

[ //localhost/Radius/Scripts/ParseAAAREalm ]
  Name = ParseAAAREalm
  Description = "Parse out the @<realm> from the User-Name and use it as the name of the
  AAA Service that should handle this request"
  Language = Rex
  Filename = librexscript.so
  EntryPoint = ParseAAAREalm
  InitEntryPoint =
  InitEntryPointArgs =

--> cd /radius/services/V1.1.com

[ //localhost/Radius/Services/V1.1.com ]
  Name = V1.1.com
  Description = V1.1.com
  Type = local
  IncomingScript~ =
  OutgoingScript~ =
  OutagePolicy~ = RejectAll
  OutageScript~ =
  UserList = V1.1.com

--> cd /radius/userlists/V1.1.com

[ //localhost/Radius/UserLists/V1.1.com ]
  Entries 1 to 4 from 4 total entries
  Current filter: <all>

  Name = V1.1.com
  Description =
  U0001N1P4V1.1/

--> cd U0001N1P4V1.1

[ //localhost/Radius/UserLists/V1.1.com/U0001N1P4V1.1 ]
  Name = U0001N1P4V1.1
  Description = U0001N1PV1.1@V1.1.com
  Password = <encrypted>
  AllowNullPassword = FALSE
  Enabled = TRUE
  Group~ =
  BaseProfile~ = V1.1.com-attrib
  AuthenticationScript~ =
  AuthorizationScript~ =
  UserDefined1 =

--> cd /radius/profiles/V1.1.com-attrib

[ //localhost/Radius/Profiles/V1.1.com-attrib ]
  Name = V1.1.com-attrib
  Description =
  Attributes/

--> cd attributes

[ //localhost/Radius/Profiles/V1.1.com-attrib/Attributes ]
  cisco-avpair = "lcp:interface-config=ip vrf forwarding V1.1.com \n ip unnumbered
  Loopback1 \n peer default ip address pool V1.1-pool"
  framed-protocol = ppp
  service-type = framed

```

