Configuring AAA for VPDNs

This module describes how to configure authentication, authorization, and accounting (AAA) for Virtual Private Dialup Networks (VPDNs).

Module History

This module was first published on September 26, 2005, and last updated on November 20, 2006.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the "Feature Information for AAA for VPDNs" section on page 124.

Contents

Prerequisites for Configuring AAA for VPDNs

- Before configuring AAA for VPDNs, you should understand the concepts in the "Overview of VPDN Technology" module.
- You must identify the VPDN architecture you plan to implement.
- You must identify the tunneling protocol you will use.
- If you plan to configure remote AAA, you should understand the concepts in the "Authentication, Authorization, and Accounting (AAA)" and "Security Server Protocols" parts of the *Cisco IOS Security Configuration Guide*, Release 12.4.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- If you plan to configure L2TP Domain Screening, you must configure the L2TP access concentrator (LAC) to request authentication of a complete username before making a forwarding decision for dial-in L2TP. In other words, the LAC preauthenticates *username@domain* to find the correct L2TP tunnel for the user session.

  You can configure virtual private dialup network (VPDN) preauthentication to occur globally or per VPDN group. For global VPDN preauthentication, authentication and authorization should be done using an authentication server. For per-VPDN group-level preauthentication, authentication and authorization should be done locally.

Information About AAA for VPDNs

Before configuring AAA for VPDNs, you should understand the following concepts:

VPDN Tunnel Authorization Search Order

When a call to a network access server (NAS) is to be tunneled to a tunnel server, the NAS must identify which tunnel server to forward the call to. The router can authorize users and select the outgoing tunnel based on the domain portion of the username, the Dialed Number Identification Service (DNIS) number, the multihop hostname, or any combination of these three parameters in a specified order. The default search order for VPDN tunnel authorization is to first search by DNIS, then by domain.

The following sections contain information on VPDN tunnel lookup criteria:

VPDN Tunnel Lookup Based on Domain Name

When a NAS is configured to forward VPDN calls on the basis of the user domain name, the user must use a username of the form *username@domain*. The NAS then compares the user domain name to the domain names it is configured to search for. When the NAS finds a match, it forwards the user call to the proper tunnel server.

VPDN Tunnel Lookup Based on L2TP Domain Screening

You can modify the domain portion of the username seamlessly when you enter into a Virtual Private Network (VPN) service. The L2TP Domain Screening feature ensures that the appropriate domain has been screened before access is allowed to an L2TP tunnel for the user session.

For additional information on configuring L2TP Domain Screening tunnel authentication into a VPN, refer to the "L2TP Domain Screening" section on page 41.

VPDN Tunnel Lookup Based on DNIS Information

When a NAS is configured to forward VPDN calls on the basis of the user DNIS information, the NAS identifies the user DNIS information, which is provided on ISDN lines, and then forwards the call to the proper tunnel server.

The ability to select a tunnel on the basis of DNIS information provides additional flexibility to network service providers that offer VPDN services and to the companies that use the services. Instead of using only the domain name for tunnel selection, the NAS can use dialed number information for tunnel selection.

With this feature, a company—which might have only one domain name—can provide multiple specific phone numbers for users to dial in to the NAS at the service provider point of presence (POP). The service provider can select the tunnel to the appropriate services or portion of the company network on the basis of the dialed number.

VPDN Tunnel Lookup Based on Both Domain Name and DNIS Information

When a service provider has multiple AAA servers configured, VPDN tunnel authorization searches based on domain name can be time consuming and might cause the client session to time out.

To provide more flexibility, service providers can configure the NAS to perform tunnel authorization searches by domain name only, by DNIS only, or by both in a specified order.

VPDN Tunnel Lookup Based on the Multihop Hostname

If a device will function as a multihop tunnel switch, tunnel authorization searches may be performed based on the multihop hostname. Configuring a multihop hostname on a tunnel switch allows authorization searches to be based on the identity of the peer device that initiated the tunnel. The multihop hostname can be the hostname of the remote peer that initiated the ingress tunnel, or the tunnel ID associated with the ingress tunnel.

A multihop tunnel switch can be configured to perform authorization searches by multihop hostname only, by domain name only, by DNIS only, or by any combination of these searches in a specified order.

L2TP Domain Screening

The Layer 2 Tunnel Protocol (L2TP) Domain Screening feature provides a flexible mechanism for controlling session access to an L2TP tunnel. This feature provides the ability to modify the domain portion of the username seamlessly when a subscriber enters into a virtual private network (VPN) service. The L2TP Domain Screening feature allows per-user L2TP tunnel setup by combining the following two features:

- User preauthentication using the **vpdn authen-before-forward** command

- Modifying the domain portion of the username using the **vpn service** command to bind an incoming session to a certain L2TP tunnel

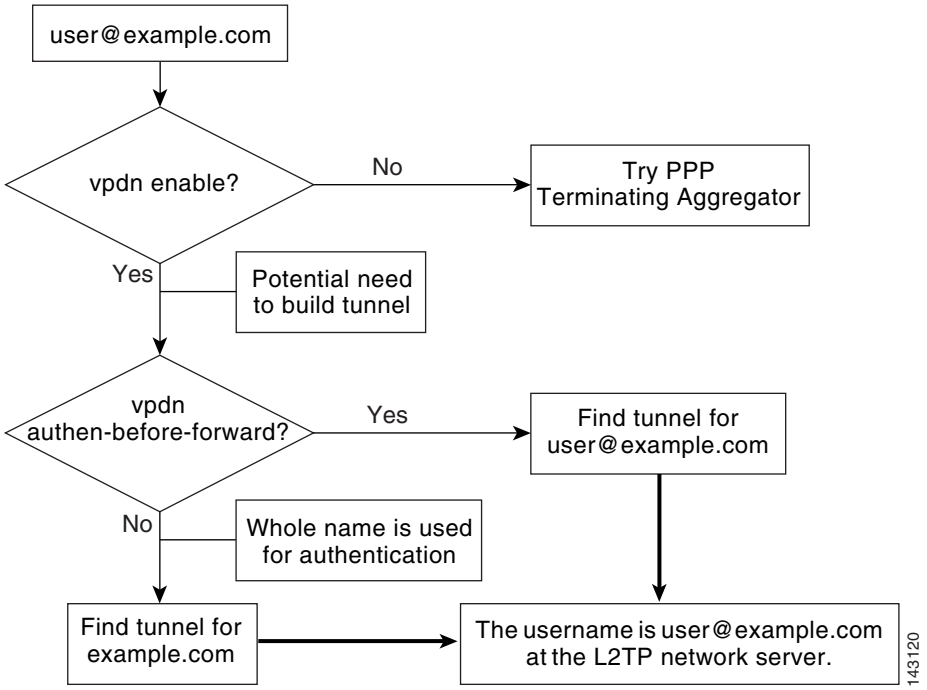
These two commands work together in the L2TP Domain Screening feature to make sure that the appropriate domain has been screened before access is allowed to an L2TP tunnel for the user session.

With Cisco Software Release 12.2(31)SB2 or higher, you can modify the domain portion of the username seamlessly when you enter into a VPN service. The L2TP Domain Screening, Rules Based feature allows per-user L2TP tunnel setup by creating customized Policy Manager match rules. For more information on the L2TP Domain Screening, Rules Based, see L2TP Domain Screening, Rules Based, page 44.

L2TP Tunnel Authentication

Figure 11 shows the general process flow for tunnel authentication. In this case, the vpdn authen-before-forward process is called if necessary to authenticate the username and domain name to find the correct L2TP tunnel for the session. If no authentication is required, the tunnel match for the domain name is found for the session. In either case, the original username with the original domain is used for session authentication at the L2TP network server.

Figure 11 Normal Tunnel Authentication Without VPN Service



In Figure 12, the same authentication flow proceeds, this time with the VPN service applied to the configuration. Just as before, if the vpdn authen-before-forward process determines that the session must be locally authenticated before being placed into the correct tunnel, authentication proceeds as normal. However, with the vpn service statement applied, the session is placed into the appropriate tunnel for the VPN domain.

Figure 12 Normal Tunnel Authentication with VPN Service Configured

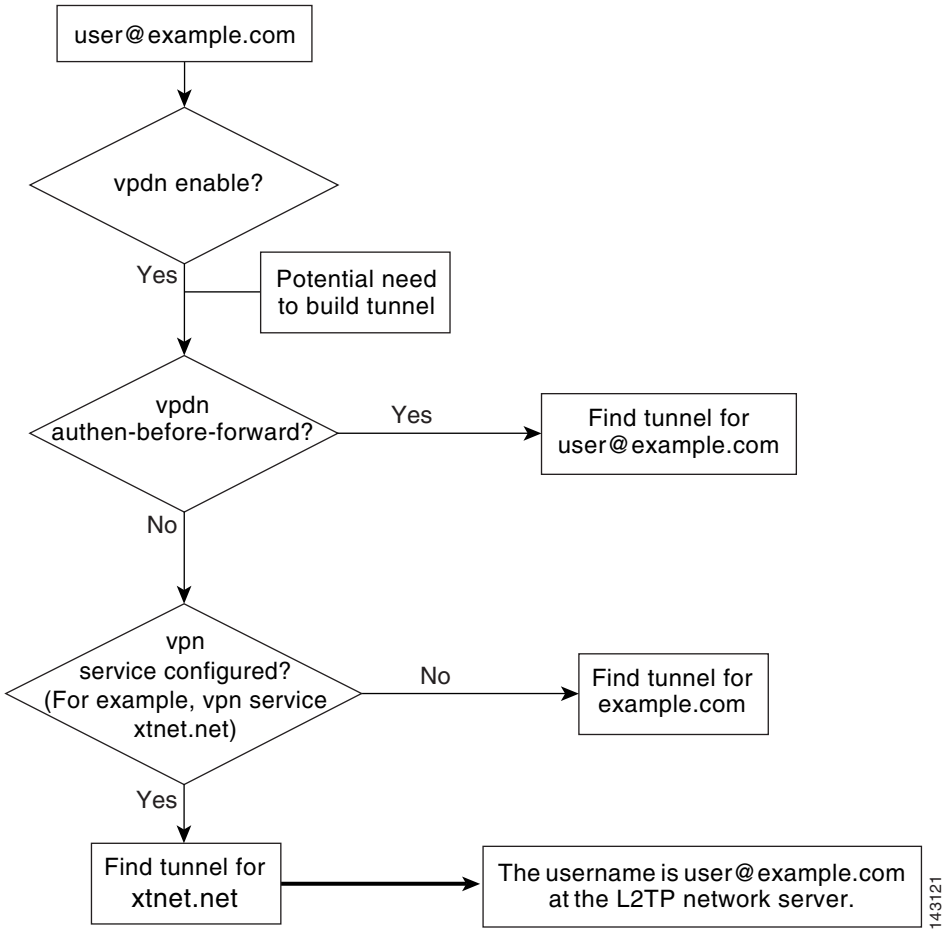


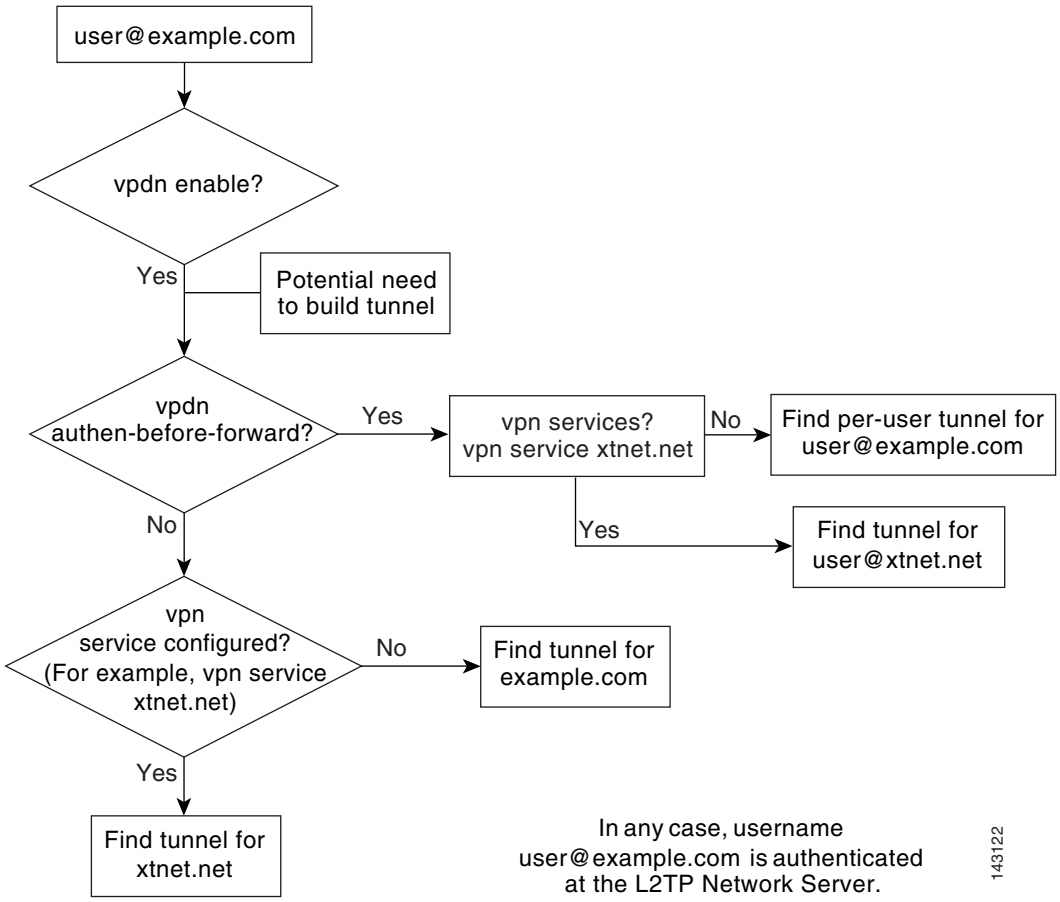
Figure 13 shows the full VPN service application flow. If local authentication at the LAC is required and a VPN service is configured, a local authentication is done with the username provided and the domain of the VPN service provider. This step returns the necessary L2TP tunnel for this VPN session. If VPN service is not configured, local authentication is provided on the username and domain name provided by the subscriber.

If the session does not require local authentication but there is a configured VPN service, the session is placed into the L2TP tunnel for the VPN service provider. Otherwise, the session will be placed into the tunnel for the specified domain name.

In any of these scenarios, the username and domain name for the subscriber session stay the same at the L2TP network server (LNS). This allows a wholesale provider to dedicate a service provider for providing all VPN services to its subscribers without the need for complex configuration for each VPN.

The **vpn service** command binds a physical incoming interface to a certain tunnel. The result is that no matter what username or domain is presented, the user is always forwarded to the specified tunnel configured by the **vpn service** command.

Figure 13 New Operation with VPN Service



L2TP Domain Screening, Rules Based

With Cisco Software Release 12.2(31)SB2 or later releases, you can modify the domain portion of the username seamlessly when you enter into a VPN service. The L2TP Domain Screening, Rules Based feature allows per-user L2TP tunnel setup by creating customized Policy Manager match rules. The L2TP Domain Screening, Rules Based feature allows you to construct rules to customize specific policy behavior. You can use the following commands to construct specific policy behavior.

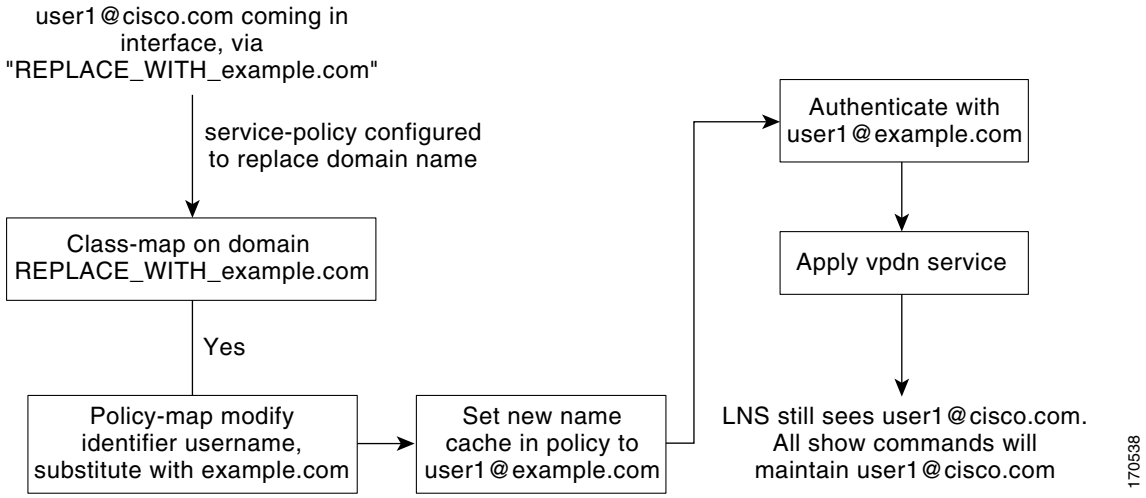
- Collect and cache the unauthenticated user name using the **set variable** command
- Replace the domain portion of the cached username using the **substitute** command and authenticate using the new altered domain name
- Authenticate the name specified using the **authenticate** command and send the authenticated name to policy manager

These commands work together in the L2TP Domain Screening, Rules Based feature to make sure that the appropriate domain has been screened before access is allowed to an L2TP tunnel for the user session.

L2TP Tunnel Authentication, Rules Based

Figure 14 shows the general process flow for tunnel authentication, rules based.

Figure 14 Normal Tunnel Authentication, Rules Based



For all users with service policy "REPLACE_WITH_abc.com, this configuration, following a policy-map session-start event, replaces the domain field of username with abc.com, with the new domain name cached in policy manager. Users authenticate based on username@abc.com, and the per-user profile is retrieved as authorization data. Finally, service abc applies to the user.

Per-User VPDN AAA

If remote AAA is used for VPDN, the NAS that receives the call from a user forwards information about that user to its remote AAA server. With basic VPDN, the NAS sends the user domain name when performing authentication based on domain name or the telephone number the user dialed in from when performing authentication based on DNIS.

When per-user VPDN is configured, the entire structured username is sent to a RADIUS AAA server the first time the router contacts the AAA server. This enables Cisco IOS software to customize tunnel attributes for individual users that use a common domain name or DNIS.

Without VPDN per-user configuration, Cisco IOS software sends only the domain name or DNIS to determine VPDN tunnel attribute information. Then, if no VPDN tunnel attributes are returned, Cisco IOS software sends the entire username string.

VPDN Authorization for Directed Request Users

Directed requests allow users logging in to a NAS to select a RADIUS server for authorization. With directed requests enabled, only the portion of the username before the "@" symbol is sent to the host specified after the "@" symbol. Using directed requests, authorization requests can be directed to any of the configured servers, and only the username is sent to the specified server.

Domain Name Prefix and Suffix Stripping

When a user connects to a NAS configured to use a remote server for AAA, the NAS forwards the username to the remote AAA server. Some RADIUS or TACACS+ servers require the username to be in a particular format, which may be different from the format of the full username. For example, the remote AAA server may require the username to be in the format user@domain.com, but the full username could be prefix/user@domain.com@suffix. Configuring domain name stripping allows the NAS to strip incompatible portions from the full username before forwarding the reformatted username to the remote AAA server.

Beginning in Cisco IOS Release 12.2(13)T, the NAS can be configured to strip generic suffixes from the full username using the suffix delimiter character @. Any portion of the full username that follows the first delimiter that is parsed will be stripped.

Beginning in Cisco IOS Release 12.3(4)T, the NAS can be configured to use a different character or set of characters as the suffix delimiter.

Beginning in Cisco IOS Release 12.4(4)T, the NAS can be configured to strip both suffixes and prefixes from the full username. The NAS can also be configured to strip only specified suffixes instead of performing generic suffix stripping.

VPDN Tunnel Authentication

VPDN tunnel authentication enables routers to authenticate the other tunnel endpoint before establishing a VPDN tunnel. VPDN tunnel authentication is required for Layer 2 Forwarding (L2F) tunnels, and optional for Layer 2 Tunneling Protocol (L2TP) tunnels.

For additional information on configuring VPDN tunnel authentication for client-initiated VPDN tunneling deployments, refer to the "Configuring VPDN Tunnel Authentication" section.

VPDN tunnel authentication can be performed in the following ways:

- Using local AAA on both the NAS and the tunnel server
- Using a remote RADIUS AAA server on the NAS and local AAA on the tunnel server
- Using a remote TACACS+ AAA server on the NAS and local AAA on the tunnel server

For L2TP tunnels only, a remote RADIUS AAA server can be used to perform VPDN tunnel authentication on the VPDN tunnel terminator as follows:

- Using a remote RADIUS AAA server on the tunnel server for dial-in VPDNs
- Using a remote RADIUS AAA server on the NAS for dial-out VPDNs

For detailed information on configuring remote RADIUS or TACACS+ servers, refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.

RADIUS Tunnel Accounting for L2TP VPDNs

RADIUS tunnel accounting for VPDNs is supported by RFC 2867, which introduces six new RADIUS accounting types beginning in Cisco IOS 12.3(4)T. Without RADIUS tunnel accounting support, VPDN with network accounting will not report all possible attributes to the accounting record file. RADIUS tunnel accounting support allows users to determine tunnel-link status changes. Because all possible attributes can be displayed, users can better verify accounting records with their Internet service providers (ISPs).

VPDN-Specific Remote RADIUS AAA Server Configurations

The following RADIUS attributes are specific to VPDN configurations. For detailed information on configuring remote RADIUS or TACACS+ servers, refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.

VPDN-specific RADIUS attributes provide the following functionality:

- Tunnel server load balancing and failover—The NAS remote RADIUS AAA server can be configured to forward the NAS information about tunnel server priorities.
- DNS name support—The NAS AAA server can be configured to resolve Domain Name System (DNS) names and translate them into IP addresses.
- Tunnel assignments—The NAS AAA server can be configured to group users from different per-user or domain RADIUS profiles into the same active VPDN tunnel when the tunnel type and tunnel endpoint are identical.
- L2TP tunnel connection speed labeling—The NAS AAA server can be configured to perform an authentication check based on the user's connection speed.
- Authentication names for NAS-initiated tunnels—The NAS AAA server can be configured with authentication names other than the default names for the NAS and the NAS AAA server.

Shell-Based Authentication of VPDN Users

The NAS and tunnel server can be configured to perform shell-based authentication of VPDN users. Shell-based authentication of VPDN users provides terminal services (shell login or exec login) for VPDN users to support rollout of wholesale dial networks. Authentication of users occurs via shell or exec login at the NAS before PPP starts and the tunnel is established.

A character-mode login dialog is provided before PPP starts, and the login dialog supports schemes such as token-card synchronization and initialization, challenge-based password, and so on. After a user is authenticated in this way, the connection changes from character mode to PPP mode to connect the user to the desired destination. The AAA server that authenticates the login user can be selected based on the dialed DNIS or the domain-name part of the username.

VPDN profiles can be kept by a Resource Pool Manager Server (RPMS), RADIUS-based AAA server, or on the NAS.

How to Configure AAA for VPDNs

To configure AAA for VPDNs, perform the following tasks:

- Enabling VPDN on the NAS and the Tunnel Server, page 48 (required)
- Configuring the VPDN Tunnel Authorization Search Order, page 49 (optional)
- Configuring L2TP Domain Screening, page 50 (optional)
- Configuring L2TP Domain Screening, Rules Based, page 56 (optional)
- Configuring AAA on the NAS and the Tunnel Server, page 62 (optional)
- Configuring Remote AAA for VPDNs, page 63 (optional)
- Verifying and Troubleshooting Remote AAA Configurations, page 68 (optional)
- Configuring Directed Request Authorization of VPDN Users, page 76 (optional)

- Configuring Domain Name Prefix and Suffix Stripping, page 79 (optional)
- Configuring VPDN Tunnel Authentication, page 82 (optional, required for L2F tunnels)
- Configuring RADIUS Tunnel Accounting for L2TP VPDNs, page 88
- Configuring Authentication of L2TP Tunnels at the Tunnel Terminator Remote RADIUS AAA Server, page 90 (optional)
- Configuring DNS Name Support on the NAS Remote RADIUS AAA Server, page 92 (optional)
- Configuring L2TP Tunnel Server Load Balancing and Failover on the NAS Remote RADIUS AAA Server, page 93 (optional)
- Configuring Tunnel Assignments on the NAS Remote RADIUS AAA Server, page 96 (optional)
- Configuring L2TP Tunnel Connection Speed Labeling on the Remote ARS RADIUS AAA Server and the Tunnel Server, page 98 (optional)
- Configuring Secure Tunnel Authentication Names on the NAS Remote RADIUS AAA Server, page 102 (optional)
- Configuring the NAS for Shell-Based Authentication of VPDN Users, page 103 (optional)

Enabling VPDN on the NAS and the Tunnel Server

Before performing any VPDN configuration tasks, you must enable VPDN on the NAS and the tunnel server. If you are deploying a multihop VPDN tunnel switching architecture, VPDN must be enabled on the tunnel switch as well.

Perform this task on all required devices to enable VPDN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables VPDN on the router.

What to Do Next

You may perform the optional task in the "Configuring the VPDN Tunnel Authorization Search Order" section.

- You may perform the optional task in the "Configuring L2TP Domain Screening" section.
- You may perform the optional task in the "Configuring AAA on the NAS and the Tunnel Server" section.

Configuring the VPDN Tunnel Authorization Search Order

The default search order for VPDN tunnel authorization is to first search by DNIS, then by domain.

Perform this task on the NAS or the tunnel switch to configure the VPDN tunnel authorization search order if you prefer to use an order other than the default order.

Prerequisites

You must perform the task in the "Enabling VPDN on the NAS and the Tunnel Server" section.

Restrictions

- Tunnel authorization searches based on the multihop hostname are supported only for multihop tunnel switching deployments.
- Multihop tunnel switching based on DNIS numbers or multihop hostnames is supported only in Cisco IOS Release 12.2(13)T and later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn search-order** {[**dnis**] [**domain**] [**multihop-hostname**]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**vpdn search-order** {[**dnis**] [**domain**] [**multihop-hostname**]}
	
	`Example:`
	`Router(config)# vpdn search-order domain dnis`
		Specifies how the service provider NAS or tunnel switch is to perform VPDN tunnel authorization searches.
		• At least one search parameter keyword must be specified. You may specify multiple search parameter keywords in any order to define the desired order in which searches will be performed.
		Note The **multihop-hostname** keyword is used only on a device configured as a tunnel switch.

What to Do Next

- You may perform the optional task in the "Configuring L2TP Domain Screening" section.
- You may perform the optional task in the "Configuring AAA on the NAS and the Tunnel Server" section.

Configuring L2TP Domain Screening

To configure L2TP Domain Screening, enable VPN service and VPDN preauthentication on the LAC. You can enable VPDN preauthentication globally or for specific VPDN groups.

This section contains the following procedures:

- Configuring L2TP Domain Screening with Global Preauthentication, page 50 (required)
- L2TP Domain Screening with Global Preauthentication: Example, page 53 (required)
- Configuring L2TP Domain Screening with per-VPDN Group Preauthentication, page 53 (required)

Configuring L2TP Domain Screening with Global Preauthentication

To configure L2TP Domain Screening with global preauthentication, enable VPN service and enable VPDN preauthorization globally. RADIUS authentication and authorization are required for per-user tunnels.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **aaa new-model**
4. **aaa authentication ppp** {**default** | *list-name*] *method1* [*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2...*]
6. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]
7. **radius-server key** {**0** *string* | **7** *string* | *string*}
8. **vpdn enable**
9. **vpdn authen-before-forward**
10. **interface atm** *interface-number*
11. **ip address** *ip-address mask*
12. **pvc** *vpi/vci*
13. **encapsulation aal5snap**
14. **protocol pppoe**
15. **vpn service** *domain-name* [**replace-authen-domain**]
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control system.
Step 4	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp default group radius`	Specifies the use of RADIUS authentication for PPP authentication.
Step 5	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authorization network default group radius`	Specifies that authorization be run for all network-related service requests and uses **group radius** as the default method for authorization. This command is required for the AAA server to provide VPDN attributes.

	Command or Action	Purpose
Step 6	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config)# radius-server host 10.1.10.1 auth-port 1645 acct-port 1646`	Specifies the AAA server that will supply the network access server or L2TP access concentrator (LAC) with the VPDN attributes for the user.
Step 7	**radius-server key** {**0** *string* | **7** *string* | *string*} **Example:** `Router(config)# radius-server key cisco`	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
Step 8	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database or on a remote authorization server (home gateway), if one is present.
Step 9	**vpdn authen-before-forward** **Example:** `Router(config)# vpdn authen-before-forward`	Enables authentication of all dial-in L2TP sessions before the sessions are forwarded to the tunnel server (global preauthentication).
Step 10	**interface atm** *interface-number* **Example:** `Router(config)# interface atm 4/0`	Defines an ATM interface.
Step 11	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.0.0.2 255.255.0.0`	Sets the primary IP address for this interface.
Step 12	**pvc** *vpi/vci* **Example:** `Router(config-if)# pvc 1/20`	Enters ATM VC configuration mode for the interface identified by this virtual path identifier/virtual channel identifier pair.
Step 13	**encapsulation aal5snap** **Example:** `Router(config-if-atm-vc)# encapsulation aal5snap`	Configures the encapsulation type for this PVC range. The global default encapsulation option is **aal5snap**.
Step 14	**protocol pppoe** **Example:** `Router(config-if-atm-vc)# protocol pppoe`	Enables PPP over Ethernet sessions for this PVC.

	Command or Action	Purpose
Step 15	**vpn service** *domain-name* [**replace-authen-domain**] **Example:** `Router(config-if-atm-vc)# vpn service example.com replace-authen-domain`	Replaces the domain field with the domain name during preauthentication.
Step 16	**end** **Example:** `Router(config-if-atm-vc)# end`	Ends the current configuration session and returns to privileged EXEC mode.

L2TP Domain Screening with Global Preauthentication: Example

Global preauthentication for L2TP domain screening requires RADIUS authentication and authorization. Each user must have a RADIUS user profile that enables per-user L2TP tunneling.

The following example shows a user profile for user-1@example.net; the IP address in the profile is the LNS interface connected to the LAC.

```
[ /Radius/UserLists/Default/user-1@example.net ]
    Name = user_1@xnet.net
    Description = TEST
    Password = <encrypted>
    Enabled = TRUE

cisco-avpair = vpdn:tunnel-type=l2tp
    cisco-avpair = vpdn:l2tp-tunnel-password=tunnel
    cisco-avpair = vpdn:l2tp-hello-interval=60
    cisco-avpair = vpdn:ip-addresses=10.1.1.1
    cisco-avpair = vpdn:tunnel-id=LAC1-1
    Framed-protocol = PPP
    Service-Type = Outbound
```

Configuring L2TP Domain Screening with per-VPDN Group Preauthentication

To configure L2TP Domain Screening with per-VPDN group preauthentication, enable VPN service and enable VPDN preauthentication by specific VPDN group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2...*]
6. **vpdn enable**
7. **vpdn-group** *name*
8. **request-dialin**

9. **protocol l2tp**
10. **domain** *domain-name*
11. **exit**
12. **authen-before-forward**
13. **initiate-to ip** *ip-address*
14. **end**
15. **configure terminal**
16. **interface atm** *interface-number*
17. **ip address** *ip-address mask*
18. **pvc** *vpi/vci*
19. **encapsulation aal5snap**
20. **protocol pppoe**
21. **vpn service** *domain-name* [**replace-authen-domain**]
22. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control system.
Step 4	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp default local`	Specifies the use of local authentication for PPP authentication.
Step 5	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authorization network default local`	Specifies that authorization be run for all network-related service requests and uses local authentication as the default method for authorization. This command is required for the AAA server to provide VPDN attributes.

	Command or Action	Purpose
Step 6	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database or on a remote authorization server (home gateway), if one is present.
Step 7	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group l2tp`	Creates a VPDN group and associates a name with it.
Step 8	**request-dialin** **Example:** `Router(config-vpdn)# request-dialin`	Configures the VPDN group to request an L2TP dial-in tunnel.
Step 9	**protocol l2tp** **Example:** `Router(config-vpdn-req-in)# protocol l2tp`	Specifies the tunneling protocol to be used by the VPDN group.
Step 10	**domain** *domain-name* **Example:** `Router(config-vpdn-req-in)# domain example.com`	Specifies the domain name of users that will be forwarded to the tunnel server.
Step 11	**exit** **Example:** `Router(config-vpdn-req-in)# exit`	Returns to VPDN configuration mode.
Step 12	**authen-before-forward** **Example:** `Router(config-vpdn)# authen-before-forward`	Enables authentication of dial-in L2TP sessions associated with this VPDN group before the sessions are forwarded to the tunnel server (per-VPDN group preauthentication).
Step 13	**initiate-to ip** *ip-address* **Example:** `Router(config-vpdn)# initiate-to ip 10.2.2.2`	Specifies an IP address to be used for L2TP tunneling.
Step 14	**end** **Example:** `Router(config-vpdn)# end`	Returns to privileged EXEC mode.
Step 15	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 16	**interface atm** *interface-number* **Example:** `Router(config)# interface atm 4/0`	Defines an ATM interface.

	Command or Action	Purpose
Step 17	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.0.0.2 255.255.0.0`	Sets the primary IP address for this interface.
Step 18	**pvc** *vpi/vci* **Example:** `Router(config-if)# pvc 1/20`	Enters ATM VC configuration mode for the interface identified by this virtual path identifier/virtual channel identifier pair.
Step 19	**encapsulation aal5snap** **Example:** `Router(config-if-atm-vc)# encapsulation aal5snap`	Configures the encapsulation type for this PVC range. The global default encapsulation option is **aal5snap**.
Step 20	**protocol pppoe** **Example:** `Router(config-if-atm-vc)# protocol pppoe`	Enables PPP over Ethernet sessions for this PVC.
Step 21	**vpn service** *domain-name* [**replace-authen-domain**] **Example:** `Router(config-if-atm-vc)# vpn service example.com replace-authen-domain`	Replaces the domain field with the domain name during preauthentication.
Step 22	**end** **Example:** `Router(config-if-atm-vc)# end`	Ends the current configuration session and returns to privileged EXEC mode.

Configuring L2TP Domain Screening, Rules Based

To configue domain screening, rules based, proceed with the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-policy*}] *policy-map-name*
4. **class-map** [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log class*}] [**match-all** | **match-any**] *class-map-name*
5. *action-number* **collect** [**aaa list** *list-name*] **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
6. *action-number* **set** [*variable-name*] [**identifier**] [*type*]

7. *action-number* **substitute** [*variable-name*] [*matching-pattern*] [*rewrite-pattern*]
8. *action-number* **authenticate** [**variable** *variable-name*] [**aaa list** *method-list-name*]
9. **end**

Note that if you specify the default method list for any of the control policy actions, the default list will not appear in the output of the **show running-config** command. For example, if you configure the following command:

```
Router(config-control-policymap-class-control)# 1 authenticate aaa list default
```

the following will display in the output for the **show running-config** command:

```
1 authenticate
```

Named method lists will display in the **show running-config** command output.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-policy*}] *policy-map-name* **Example:** `Router(config)# policy-map type control start-up-ppp`	Creates or modifies a control policy map, which is used to define a control policy.
Step 4	**class-map** [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log class*}] [**match-all** | **match-any**] *class-map-name* **Example:** `Router(config-control-policymap)# class type control always event session-start`	Specifies a control class for which actions may be configured. • A policy rule for which the control class is **always** will always be treated as the lowest priority rule within the control policy map.
Step 5	*action-number* **collect** [**aaa list** *list-name*] **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**} **Example:** `Router(config-control-policymap-class-control)# 1 collect identifier unauthenticated-username`	(Optional) Collects the specified subscriber identifier from the access protocol.

	Command or Action	Purpose
Step 6	*action-number* **set** [*variable-name*] [**identifier**] [*type*] **Example:** `Router(config-control-policymap-class-control)# 2 set NAME identifier unauthenticated-username`	Creates a temporary memory space to hold values received by policy manager on the identifier type.
Step 7	*action-number* **substitute** [*variable-name*] [*matching-pattern*] [*rewrite-pattern*] **Example:** `Router(config-control-policymap-class-control)# 3 substitute NEWNAME`	Matches the contents of *variable-name* using *matching-pattern* and perform the substitution defined in *rewrite-pattern.*
Step 8	*action-number* **authenticate aaa list** *list-name* **Example:** `Router(config-control-policymap-class-control)# 1 authenticate aaa list LIST1`	Initiates an authentication request using the contents of *variable-name* instead of the default unauthenticated-username.
Step 9	**exit** **Example:** `Router(config-control-policymap-class-control)# exit`	Exits the current configuration mode.

Configuring L2TP Domain Screening, Rules Based: Example

The following examples shows a policy map configuration for L2TP domain screening, rules based:

```
policy-map type control REPLACE_WITH_example.com
 class type control always event session-start
  1 collect identifier unauthenticated-username
  2 set NEWNAME identifier unauthenticated-username
  3 substitute NEWNAME "(.*@).*" "\1example.com"
  4 authenticate variable NEWNAME aaa list EXAMPLE
  5 service-policy type service name example

policy-map type service abc
 service vpdn group 1

bba-group pppoe global
 virtual-template 1
!
interface Virtual-Template1
 service-policy type control REPLACE_WITH_example.com
```

Configuring per-User VPDN on the NAS

If remote AAA is used for VPDN, the NAS that receives the call from a user forwards information about that user to its remote AAA server. With basic VPDN, the NAS sends the user domain name when performing authentication based on domain name or the telephone number the user dialed in from when performing authentication based on DNIS.

When per-user VPDN is configured, the entire structured username is sent to a RADIUS AAA server the first time the router contacts the AAA server. This enables Cisco IOS software to customize tunnel attributes for individual users that use a common domain name or DNIS.

Without VPDN per-user configuration, Cisco IOS software sends only the domain name or DNIS to determine VPDN tunnel attribute information. Then, if no VPDN tunnel attributes are returned, Cisco IOS software sends the entire username string.

Per-user VPDN can be configured globally, or for individual VPDN groups. The VPDN group configuration will take precedence over the global configuration.

Perform one of the following tasks on the NAS to configure per-user VPDN:

- Configuring Global per-User VPDN, page 59 (optional)
- Configuring per-User VPDN for a VPDN Group, page 60 (optional)

Prerequisites

The NAS remote RADIUS server must be configured for AAA. For more information on configuring remote RADIUS AAA servers refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.

Restrictions

- Per-user VPDN configuration supports only RADIUS as the AAA protocol.
- This task is compatible only with NAS-initiated dial-in VPDN scenarios.

Configuring Global per-User VPDN

Configuring per-user VPDN on a NAS causes the NAS to send the entire structured username of the user to a RADIUS AAA server the first time the NAS contacts the AAA server. Per-user VPDN can be configured globally, or for individual VPDN groups. Configuring per-user VPDN globally will apply per-user VPDN to all request-dialin VPDN groups configured on the NAS.

Perform this task on the NAS to configure global per-user VPDN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn authen-before-forward**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn authen-before-forward** **Example:** `Router(config)# vpdn authen-before-forward`	Configures a NAS to request authentication of a complete username before making a forwarding decision for all dial-in L2TP or L2F tunnels.

What to Do Next

You may perform the optional task in the "Configuring AAA on the NAS and the Tunnel Server" section.

Configuring per-User VPDN for a VPDN Group

Configuring per-user VPDN on a NAS causes the NAS to send the entire structured username of the user to a RADIUS AAA server the first time the NAS contacts the AAA server. Per-user VPDN can be configured globally, or for individual VPDN groups. Configuring per-user VPDN at the VPDN group level will apply per-user VPDN only to calls associated with that specific VPDN group

Perform this task on the NAS to configure per-user VPDN for a specific VPDN group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **request-dialin**
5. **protocol** {**l2f** | **l2tp** | **any**}
6. **exit**
7. **authen-before-forward**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**request-dialin** **Example:** `Router(config-vpdn)# request-dialin`	Configure a NAS to request the establishment of an L2F or L2TP tunnel to a tunnel server, creates a request-dialin VPDN subgroup, and enters VPDN request dial-in subgroup configuration mode.
Step 5	**protocol** {**l2f** | **l2tp** | **any**} **Example:** `Router(config-vpdn-req-in)# protocol l2tp`	Specifies the Layer 2 protocol that the VPDN group will use. • L2TP and L2F are the only valid tunneling protocols for dial-in VPDNs. The **any** keyword can be used to specify that both L2TP and L2F tunnels can be established.
Step 6	**exit** **Example:** `Router(config-vpdn-req-in)# exit`	Exits to VPDN group configuration mode.
Step 7	**authen-before-forward** **Example:** `Router(config-vpdn)# authen-before-forward`	Configures a NAS to request authentication of a complete username before making a forwarding decision for dial-in L2TP or L2F tunnels belonging to a VPDN group.

What to Do Next

- You may configure per-user VPDN for another VPDN group.
- You may perform the optional task in the "Configuring AAA on the NAS and the Tunnel Server" section.

Configuring AAA on the NAS and the Tunnel Server

For NAS-initiated dial-in VPDN tunneling and L2TP dial-out tunneling deployments, perform this task on the NAS and the tunnel server.

For client-initiated dial-in VPDN tunneling, perform this task on the tunnel server.

Prerequisites

You must perform the task in the "Enabling VPDN on the NAS and the Tunnel Server" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} *method1* [*method2*...]
5. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2*...]
6. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2*...]]
7. **vpdn aaa attribute** {**nas-ip-address vpdn-nas** | **nas-port** {**vpdn-nas** | **physical-channel-id**}}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new model`	Enables the AAA access control model.
Step 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication login default local`	Sets AAA authentication at login.

	Command or Action	Purpose
Step 5	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp default radius`	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP. **Note** This command must be configured with the **if-needed** option for the *method1* argument if you are configuring shell-based authentication for VPDNs. This configures PPP to bypass user authentication if the user has been authenticated at the login prompt.
Step 6	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]] **Example:** `Router(config)# aaa authorization network default radius`	Sets parameters that restrict user access to a network.
Step 7	**vpdn aaa attribute** {**nas-ip-address vpdn-nas** | **nas-port** {**vpdn-nas** | **physical-channel-id**}} **Example:** `Router(config)# vpdn aaa attribute nas-ip-address vpdn-nas`	(Optional) Enables AAA attributes related to a VPDN that will be reported to the AAA server in accounting records. **Note** Configure this command only on the tunnel server when remote AAA accounting will be enabled on the NAS.

What to Do Next

- You may perform the optional task in the "Configuring Remote AAA for VPDNs" section.
- You must perform the process in the "Configuring VPDN Tunnel Authentication" section.

Configuring Remote AAA for VPDNs

A remote RADIUS or TACACS+ AAA server can be used for tunnel authentication. For detailed information on configuring remote RADIUS or TACACS+ servers, refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.

Remote AAA authentication can be configured on the NAS or the tunnel server in the following ways:

Dial-In Configurations

- The NAS can be configured to use a remote AAA server.
- The tunnel server, functioning as the tunnel terminator, can be configured to use a remote AAA server for L2TP tunnels only.

Dial-Out Configurations

- The NAS, functioning as the tunnel terminator, can be configured to use a remote AAA server for L2TP tunnels only.

Perform one of the following tasks to configure remote AAA for VPDNs:

- Configuring the NAS for Remote AAA for Dial-In VPDNs, page 64
- Configuring the Tunnel Terminator for Remote RADIUS AAA for L2TP Tunnels, page 66

Configuring the NAS for Remote AAA for Dial-In VPDNs

Perform this task to configure the NAS to use a remote RADIUS or TACACS+ server for tunnel authentication. This task applies only to dial-in VPDN configurations.

Prerequisites

- The remote RADIUS or TACACS+ AAA server must be configured. For more information on configuring remote RADIUS or TACACS+ AAA servers, refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.
- AAA must be enabled. To enable AAA, perform the task in the "Configuring AAA on the NAS and the Tunnel Server" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]
   or
   tacacs-server host {*host-name* | *host-ip-address*} [**key** *string*] [**nat**] [**port** [*integer*]] [**single-connection**] [**timeout** [*integer*]]
4. **aaa group server radius** *group-name*
   or
   aaa group server tacacs+ *group-name*
5. **server ip-address** [**auth-port** *port-number*] [**acct-port** *port-number*]
   or
   server *ip-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]
	or
	tacacs-server host {*host-name* | *host-ip-address*} [**key** *string*] [**nat**] [**port** [*integer*]] [**single-connection**] [**timeout** [*integer*]]
	Example:
	`Router(config)# radius-server host 10.1.1.1`
	or
	Example:
	`Router(config)# tacacs-server host 10.2.2.2`
		Specifies a RADIUS server host.
		Note This command is required if you will be performing the task in the "Configuring the NAS for Shell-Based Authentication of VPDN Users" section.
		or
		Specifies a TACACS+ host.

Step 4	**aaa group server radius** *group-name*
	or
	aaa group server tacacs+ *group-name*
	Example:
	`Router(config)# aaa group server radius group1`
	or
	`Router(config)# aaa group server tacacs+ group7`
		(Optional) Groups different RADIUS server hosts into distinct lists and distinct methods and enters RADIUS server group configuration mode.
		or
		(Optional) Groups different TACACS+ server hosts into distinct lists and distinct methods and enters RADIUS server group configuration mode.

Step 5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
	or
	server *ip-address*
	Example:
	`Router(config-sg-radius)# server 10.1.1.1 auth-port 1000 acct-port 1646`
	or
	`Router(config-sg-radius)# server 10.2.2.2`
		(Optional) Configures the IP address of the RADIUS server for the group server.
		or
		(Optional) Configures the IP address of the TACACS+ server for the group server.
		Note Perform this step multiple times to configure multiple RADIUS or TACACS+ servers as part of the server group.

What to Do Next

- You can choose to verify your configuration by performing the tasks in the "Verifying and Troubleshooting Remote AAA Configurations" section.
- You must perform the process in the "Configuring VPDN Tunnel Authentication" section.

Configuring the Tunnel Terminator for Remote RADIUS AAA for L2TP Tunnels

You may configure the device that terminates the L2TP VPDN tunnel to perform remote RADIUS AAA. Without this functionality, the tunnel terminator can only perform L2TP authentication locally. Local authentication requires that data about the corresponding tunnel endpoint be configured within a VPDN group. This mechanism does not scale well because the information stored in the VPDN groups on each device must be updated independently.

Remote RADIUS authentication allows users to store configurations on the RADIUS server, avoiding the need to store information locally. New information can be added to the RADIUS server as needed, and a group of tunnel terminators can access a common database on the RADIUS server.

Perform this task to configure remote RADIUS AAA for L2TP tunnels on the tunnel terminator. This task can be performed on the tunnel server for dial-in VPDN tunnels, or on the NAS for dial-out VPDN tunnels.

Prerequisites

- The remote RADIUS AAA server must be configured. For more information on configuring remote RADIUS AAA servers refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.
- AAA must be enabled. To enable AAA, perform the task in the "Configuring AAA on the NAS and the Tunnel Server" section.
- You must be running Cisco IOS Release 12.3(4)T or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]
4. **aaa group server radius** *group-name*
5. **server ip-address** [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **exit**
7. **vpdn tunnel authorization network** {*list-name* | **default**}
8. **vpdn tunnel authorization virtual-template** *vtemplate-number*
9. **vpdn tunnel authorization password** *password*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] **Example:** `Router(config)# radius-server host 10.1.1.1`	Specifies a RADIUS server host.
Step 4	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius group1`	Groups different RADIUS server hosts into distinct lists and distinct methods and enters RADIUS server group configuration mode.
Step 5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config-sg-radius)# server 10.1.1.1 auth-port 1000 acct-port 1646`	Configures the IP address of the RADIUS server for the group server. **Note** Perform this step multiple times to configure multiple RADIUS or TACACS+ servers as part of the server group.
Step 6	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits RADIUS server group configuration mode.
Step 7	**vpdn tunnel authorization network** {*list-name* | **default**} **Example:** `Router(config)# vpdn tunnel authorization network default`	Specifies the AAA authorization method list that will be used for remote tunnel hostname-based authorization. • If the *list-name* argument was specified in the **aaa authorization** command, you must use that list name. • If the default keyword was specified in the **aaa authorization** command, you must use that keyword.
Step 8	**vpdn tunnel authorization virtual-template** *vtemplate-number* **Example:** `Router(config)# vpdn tunnel authorization virtual-template 3`	(Optional) Selects the default virtual template from which to clone virtual access interfaces.
Step 9	**vpdn tunnel authorization password** *password* **Example:** `Router(config)# vpdn tunnel authorization password my-secret`	(Optional) Configures a false password for the RADIUS authorization request to retrieve the tunnel configuration that is based on the remote tunnel hostname. **Note** If this command is not enabled, the password will always be "cisco."

What to Do Next

- You may verify your configuration by performing the tasks in the "Verifying and Troubleshooting Remote AAA Configurations" section.
- You must perform the process in the "Configuring VPDN Tunnel Authentication" section.
- You must perform the task in the "Configuring Authentication of L2TP Tunnels at the Tunnel Terminator Remote RADIUS AAA Server" section.

Verifying and Troubleshooting Remote AAA Configurations

Perform the tasks in this section to verify remote RADIUS AAA configurations.

Verifying that the VPDN Tunnel Is Up

Perform this task to verify that the VPDN tunnel is up.

SUMMARY STEPS

1. **enable**
2. **show vpdn tunnel**

DETAILED STEPS

Step 1 **enable**

Enter this command to enable privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 2 **show vpdn tunnel**

Enter this command to display information about active VPDN tunnels. At least one tunnel and one session must be set up.

```
Router# show vpdn tunnel

L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions VPDN Group
4571  61568 csidtw13 est    10.0.195.4      1701  1        ?

LocID RemID TunID Intf          Username               State  Last Chg
4     11    4571  Vi4.1         csidtw9@cisco.com       est    00:02:29

%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels
```

Verifying the Remote RADIUS AAA Server Configuration

Perform this task to verify that the remote AAA authorization server is configured on the tunnel endpoint and that the tunnel endpoint can receive attributes 90 and 69 from the RADIUS server.

In this example the steps are performed on the tunnel server, which is performing remote RADIUS AAA as a tunnel terminator. These steps can also be performed on the NAS when remote RADIUS AAA is being performed on the NAS as a tunnel initiator for dial-in VPDNs or as a tunnel terminator for dial-out VPDNs.

SUMMARY STEPS

1. **enable**
2. **debug radius**
3. **show logging**

DETAILED STEPS

Step 1 **enable**

Enter this command to enable privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 2 **debug radius**

Enter this command on the tunnel server to display RADIUS debugging messages.

Step 3 **show logging**

Enter this command on the tunnel server to display the contents of the standard system logging message buffer. Ensure that “access-accept” is in the output and that attributes 90 and 69 can be seen in the RADIUS reply, as shown in bold.

```
Router# show logging

00:32:56: RADIUS: Received from id 21645/5 172.19.192.50:1645, Access-Accept, len 81
00:32:56: RADIUS:  authenticator 73 2B 1B C2 33 71 93 19 - 62 AC 3E BE 0D 13 14 85
00:32:56: RADIUS:  Service-Type        [6]   6   Outbound                  [5]
00:32:56: RADIUS:  Tunnel-Type         [64]  6   00:L2TP                   [3]
00:32:56: RADIUS:  Tunnel-Medium-Type  [65]  6   00:IPv4                   [1]
00:32:56: RADIUS:  Tunnel-Client-Auth-I[90]  6   00:"csidtw13"
00:32:56: RADIUS:  Tunnel-Password     [69]  8   *
00:32:56: RADIUS:  Vendor, Cisco       [26]  29
00:32:56: RADIUS:   Cisco AVpair       [1]   23  "vpdn:vpdn-vtemplate=1"
```

Verifying the Remote TACACS+ AAA Server Configuration on the NAS

Perform this task on the NAS to verify that the remote TACACS+ AAA server is properly configured.

Prerequisites

Enable the following debug commands before performing this task:

- **debug aaa accounting**—Displays information on accountable events as they occur.
- **debug aaa authentication**—Displays information on AAA TACACS+ authentication.
- **debug aaa authorization**—Displays information on AAA TACACS+ authorization.
- **debug tacacs**—Displays information associated with TACACS+.
- **debug vpdn error**—Displays information about Layer 2 protocol-independent errors that occur.
- **debug vpdn events**—Displays information about Layer 2 protocol-independent events that are part of normal tunnel establishment or shutdown.
- **debug vpdn l2x-errors**—Displays information about Layer 2 protocol-specific errors that are part of normal PPP tunnel establishment or shutdown.
- **debug vpdn l2x-events**—Displays information about Layer 2 protocol-specific events that are part of normal PPP tunnel establishment or shutdown.
- **debug vpdn l2x-packets**—Displays information about Layer 2 protocol-specific
- **debug vtemplate**—Displays cloning information for a virtual access interface from the time it is cloned from a virtual template to the time the virtual access interface comes down when the call ends.

SUMMARY STEPS

1. **enable**
2. **show debugging**
3. Examine debug output.

DETAILED STEPS

Step 1 **enable**

Enter this command to enable privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 2 **show debugging**

Enter this command to display information about the types of debugging that are enabled for your router.

```
Router# show debugging

General OS:
AAA Authentication debugging is on
AAA Authorization debugging is on
AAA Accounting debugging is on
VPN:
L2X protocol events debugging is on
L2X protocol errors debugging is on
VPDN events debugging is on
VPDN errors debugging is on
```

```
VTEMPLATE:
Virtual Template debugging is on
!
```

Step 3 Examine debug output.

The following example shows complete debug output from the NAS for successful VPDN tunnel establishment using remote TACACS+ AAA authentication at the NAS:

```
Jan 30 12:17:09: As1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
20:03:18: %LINK-3-UPDOWN: Interface Async1, changed state to up
Jan 30 12:17:09: As1 VPDN: Looking for tunnel -- rtp.cisco.com --
Jan 30 12:17:09: AAA: parse name=Async1 idb type=10 tty=1
Jan 30 12:17:09: AAA: name=Async1 flags=0x11 type=4 shelf=0 slot=0 adapter=0
port=1 channel=0
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x278B90) user='rtp.cisco.com'
ruser=''
port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0
Jan 30 12:17:09: AAA/AUTHOR/VPDN (898425447): Port='Async1' list='default'
service=NET
Jan 30 12:17:09: AAA/AUTHOR/VPDN: (898425447) user='rtp.cisco.com'
Jan 30 12:17:09: AAA/AUTHOR/VPDN: (898425447) send AV service=ppp
Jan 30 12:17:09: AAA/AUTHOR/VPDN: (898425447) send AV protocol=vpdn
Jan 30 12:17:09: AAA/AUTHOR/VPDN (898425447) found list "default"
Jan 30 12:17:09: AAA/AUTHOR/VPDN: (898425447) Method=TACACS+
Jan 30 12:17:09: AAA/AUTHOR/TAC+: (898425447): user=rtp.cisco.com
Jan 30 12:17:09: AAA/AUTHOR/TAC+: (898425447): send AV service=ppp
Jan 30 12:17:09: AAA/AUTHOR/TAC+: (898425447): send AV protocol=vpdn
Jan 30 12:17:09: TAC+: (898425447): received author response status = PASS_ADD
Jan 30 12:17:09: AAA/AUTHOR (898425447): Post authorization status = PASS_ADD
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV service=ppp
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV protocol=vpdn
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV tunnel-id=rtp_tunnel
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV ip-addresses=10.31.1.56
Jan 30 12:17:09: As1 VPDN: Get tunnel info for rtp.cisco.com with NAS
rtp_tunnel, IP 10.31.1.56
Jan 30 12:17:09: AAA/AUTHEN: free_user (0x278B90) user='rtp.cisco.com' ruser=''
port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0
Jan 30 12:17:09: As1 VPDN: Forward to address 10.31.1.56
Jan 30 12:17:09: As1 VPDN: Forwarding...
Jan 30 12:17:09: AAA: parse name=Async1 idb type=10 tty=1
Jan 30 12:17:09: AAA: name=Async1 flags=0x11 type=4 shelf=0 slot=0 adapter=0
port=1 channel=0
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x22CDEC) user='user1@rtp.cisco.com'
ruser='' port='Async1' rem_addr='async' authen_type=CHAP
service=PPP priv=1
Jan 30 12:17:09: As1 VPDN: Bind interface direction=1
Jan 30 12:17:09: Tnl/Cl 74/1 L2TP: Session FS enabled
Jan 30 12:17:09: Tnl/Cl 74/1 L2TP: Session state change from idle to
wait-for-tunnel
Jan 30 12:17:09: As1 74/1 L2TP: Create session
Jan 30 12:17:09: Tnl 74 L2TP: SM State idle
Jan 30 12:17:09: Tnl 74 L2TP: O SCCRQ
Jan 30 12:17:09: Tnl 74 L2TP: Tunnel state change from idle to wait-ctl-reply
Jan 30 12:17:09: Tnl 74 L2TP: SM State wait-ctl-reply
Jan 30 12:17:09: As1 VPDN: user1@rtp.cisco.com is forwarded
Jan 30 12:17:10: Tnl 74 L2TP: I SCCRP from ABCDE
Jan 30 12:17:10: Tnl 74 L2TP: Got a challenge from remote peer, ABCDE
Jan 30 12:17:10: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:10: AAA/AUTHEN: create_user (0x23232C) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN/START (1598999635): port='' list='default'
action=SENDAUTH service=PPP
```

```
Jan 30 12:17:10: AAA/AUTHEN/START (1598999635): found list default
Jan 30 12:17:10: AAA/AUTHEN (1598999635): status = UNKNOWN
Jan 30 12:17:10: AAA/AUTHEN/START (1598999635): Method=TACACS+
Jan 30 12:17:10: TAC+: send AUTHEN/START packet ver=193 id=1598999635
Jan 30 12:17:10: TAC+: ver=192 id=1598999635 received AUTHEN status = ERROR
Jan 30 12:17:10: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:10: AAA/AUTHEN: create_user (0x232470) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: TAC+: ver=192 id=3400389836 received AUTHEN status = PASS
Jan 30 12:17:10: AAA/AUTHEN: free_user (0x232470) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN (1598999635): status = PASS
Jan 30 12:17:10: AAA/AUTHEN: free_user (0x23232C) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: Tnl 74 L2TP: Got a response from remote peer, ABCDE
Jan 30 12:17:10: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:10: AAA/AUTHEN: create_user (0x22FBA4) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN/START (2964849625): port='' list='default'
action=SENDAUTH service=PPP
Jan 30 12:17:10: AAA/AUTHEN/START (2964849625): found list default
Jan 30 12:17:10: AAA/AUTHEN (2964849625): status = UNKNOWN
Jan 30 12:17:10: AAA/AUTHEN/START (2964849625): Method=TACACS+
Jan 30 12:17:10: TAC+: send AUTHEN/START packet ver=193 id=2964849625
20:03:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1,
changed state to up
Jan 30 12:17:11: TAC+: ver=192 id=2964849625 received AUTHEN status = ERROR
Jan 30 12:17:11: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:11: AAA/AUTHEN: create_user (0x22FC8C) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: As1 74/1 L2TP: Discarding data packet because tunnel
is not open
Jan 30 12:17:11: As1 74/1 L2TP: Discarding data packet because tunnel
is not open
Jan 30 12:17:11: TAC+: ver=192 id=1474818051 received AUTHEN status = PASS
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x22FC8C) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN (2964849625): status = PASS
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x22FBA4) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: Tnl 74 L2TP: Tunnel Authentication success
Jan 30 12:17:11: Tnl 74 L2TP: Tunnel state change from wait-ctl-reply to
established
Jan 30 12:17:11: Tnl 74 L2TP: O SCCCN to ABCDE tnlid 56
Jan 30 12:17:11: Tnl 74 L2TP: SM State established
Jan 30 12:17:11: As1 74/1 L2TP: O ICRQ to ABCDE 56/0
Jan 30 12:17:11: As1 74/1 L2TP: Session state change from wait-for-tunnel
to wait-reply
Jan 30 12:17:11: Tnl 74 L2TP: Dropping old CM, Ns 0, expected 1
Jan 30 12:17:11: As1 74/1 L2TP: O ICCN to ABCDE 56/1
Jan 30 12:17:11: As1 74/1 L2TP: Session state change from wait-reply to
established
```

Verifying the Remote TACACS+ AAA Server Configuration on the Tunnel Server

Perform this task on the tunnel server to verify that the remote TACACS+ AAA server is properly configured.

Prerequisites

Enable the following debug commands before performing this task:

- **debug aaa authentication**—Displays information on AAA authentication.
- **debug aaa authorization**—Displays information on AAA authorization.
- **debug aaa accounting**—Displays information on accountable events as they occur. The information displayed by this command is independent of the accounting protocol used to transfer the accounting information to a server.
- **debug tacacs+**—Displays detailed debugging information associated with TACACS+.
- **debug vtemplate**—Displays cloning information for a virtual access interface from the time it is cloned from a virtual template to the time the virtual access interface comes down when the call ends.
- **debug vpdn error—**Displays errors that prevent a PPP tunnel from being established or errors that cause an established tunnel to be closed.
- **debug vpdn events**—Displays messages about events that are part of normal PPP tunnel establishment or shutdown.
- **debug vpdn l2x-errors**—Displays messages about events that are part of normal PPP tunnel establishment or shutdown.
- **debug vpdn l2x-events—**Displays messages about events that are part of normal PPP tunnel establishment or shutdown for Layer 2.

SUMMARY STEPS

1. **enable**
2. **show debugging**
3. Examine debug output.

DETAILED STEPS

Step 1 **enable**

Enter this command to enable privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 2 **show debugging**

Enter this command to display information about the types of debugging that are enabled for your router.

```
Router# show debugging
General OS:
AAA Authentication debugging is on
AAA Authorization debugging is on
AAA Accounting debugging is on
VPN:
L2X protocol events debugging is on
L2X protocol errors debugging is on
```

```
VPDN events debugging is on
VPDN errors debugging is on
VTEMPLATE:
Virtual Template debugging is on
```

Step 3 Examine debug output.

The following example shows complete debug output from the tunnel server for successful VPDN tunnel establishment using remote TACACS+ AAA authentication at the NAS:

```
Jan 30 12:17:09: L2TP: I SCCRQ from rtp_tunnel tnl 74
Jan 30 12:17:09: Tnl 56 L2TP: New tunnel created for remote
rtp_tunnel, address 10.31.1.144
Jan 30 12:17:09: Tnl 56 L2TP: Got a challenge in SCCRQ, rtp_tunnel
Jan 30 12:17:09: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x21F6D0) user='ABCDE'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: AAA/AUTHEN/START (3194595626): port='' list='default'
action=SENDAUTH service=PPP
Jan 30 12:17:09: AAA/AUTHEN/START (3194595626): found list default
Jan 30 12:17:09: AAA/AUTHEN (3194595626): status = UNKNOWN
Jan 30 12:17:09: AAA/AUTHEN/START (3194595626): Method=TACACS+
Jan 30 12:17:09: TAC+: send AUTHEN/START packet ver=193 id=3194595626
Jan 30 12:17:09: TAC+: ver=192 id=3194595626 received AUTHEN status = ERROR
Jan 30 12:17:09: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x2281AC) user='ABCDE'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: TAC+: ver=192 id=3639011179 received AUTHEN status = PASS
Jan 30 12:17:09: AAA/AUTHEN: free_user (0x2281AC) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: AAA/AUTHEN (3194595626): status = PASS
Jan 30 12:17:09: AAA/AUTHEN: free_user (0x21F6D0) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: Tnl 56 L2TP: O SCCRP to rtp_tunnel tnlid 74
Jan 30 12:17:09: Tnl 56 L2TP: Tunnel state change from idle to
wait-ctl-reply
Jan 30 12:17:10: Tnl 56 L2TP: O Resend SCCRP, flg TLF, ver 2, len 152,
tnl 74, cl 0, ns 0, nr 1
Jan 30 12:17:10: Tnl 56 L2TP: I SCCCN from rtp_tunnel tnl 74
Jan 30 12:17:10: Tnl 56 L2TP: Got a Challenge Response in SCCCN from rtp_tunnel
Jan 30 12:17:10: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:10: AAA/AUTHEN: create_user (0x227F3C) user='ABCDE'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN/STARTTranslating "rtp.cisco.com"
(4117701992): port='' list='default' action=SENDAUTH service=PPP
Jan 30 12:17:10: AAA/AUTHEN/START (4117701992): found list default
Jan 30 12:17:10: AAA/AUTHEN (4117701992): status = UNKNOWN
Jan 30 12:17:10: AAA/AUTHEN/START (4117701992): Method=TACACS+
Jan 30 12:17:10: TAC+: send AUTHEN/START packet ver=193 id=4117701992
Jan 30 12:17:11: TAC+: ver=192 id=4117701992 received AUTHEN status = ERROR
Jan 30 12:17:11: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:11: AAA/AUTHEN: create_user (0x228E68) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: TAC+: ver=192 id=2827432721 received AUTHEN status = PASS
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x228E68) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN (4117701992): status = PASS
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: Tnl 56 L2TP: Tunnel Authentication success
Jan 30 12:17:11: Tnl 56 L2TP: Tunnel state change from wait-ctl-reply
```

```
to established
Jan 30 12:17:11: Tnl 56 L2TP: SM State established
Jan 30 12:17:11: Tnl 56 L2TP: I ICRQ from rtp_tunnel tnl 74
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: Session FS enabled
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: Session state change from idle to
wait-for-tunnel
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: New session created
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: O ICRP to rtp_tunnel 74/1
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: Session state change from wait-for-tunnel
to wait-connect
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: I ICCN from rtp_tunnel tnl 74, cl 1
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: Session state change from wait-connect
to established
Jan 30 12:17:11: Vi1 VTEMPLATE: Reuse Vi1, recycle queue size 0
Jan 30 12:17:11: Vi1 VTEMPLATE: Hardware address 00e0.1e68.942c
Jan 30 12:17:11: Vi1 VPDN: Virtual interface created for user1@rtp.cisco.com
Jan 30 12:17:11: Vi1 VPDN: Set to Async interface
Jan 30 12:17:11: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
Jan 30 12:17:11: Vi1 VTEMPLATE: Has a new cloneblk vtemplate, now it has vtemplate
Jan 30 12:17:11: Vi1 VTEMPLATE: ************ CLONE VACCESS1 *****************
Jan 30 12:17:11: Vi1 VTEMPLATE: Clone from Virtual-Template1
```

Verifying L2TP Tunnel Establishment, PPP Negotiations, and Authentication with the Remote Client

Perform this task to verify that the L2TP tunnel has been established and that the tunnel server can perform PPP negotiation and authentication with the remote client.

In this example the steps are performed on the tunnel server, which is performing remote AAA as a tunnel terminator. These steps can also be performed on the NAS when remote AAA is being performed on the NAS as a tunnel initiator for dial-in VPDNs or as a tunnel terminator for dial-out VPDNs.

SUMMARY STEPS

1. **enable**
2. **debug ppp negotiation**
3. **debug ppp authentication**
4. **show logging**

DETAILED STEPS

Step 1 **enable**

Enter this command to enable privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 2 **debug ppp negotiation**

Enter this command on the tunnel server to display PPP negotiation debugging messages.

Step 3 **debug ppp authentication**

Enter this command on the tunnel server to display PPP authentication debugging messages.

Step 4 **show logging**

Enter this command on the tunnel server to display the contents of the standard system logging message buffer. Observe that the tunnel server receives a PPP Challenge Handshake Authentication Protocol (CHAP) challenge and then sends a PPP CHAP "SUCCESS" to the client.

```
00:38:50: ppp3 PPP: Received LOGIN Response from AAA = PASS
00:38:50: ppp3 PPP: Phase is FORWARDING, Attempting Forward
00:38:50: Vi4.1  Tnl/Sn4571/4 L2TP: Session state change from wait-for-service-selection
to established
00:38:50: Vi4.1 PPP: Phase is AUTHENTICATING, Authenticated User
00:38:50: Vi4.1 CHAP: O SUCCESS id 1 len 4
```

After PPP authentication is successful, observe from the debug output that PPP negotiation has started, that the tunnel server has received Link Control Protocol (LCP) IP Control Protocol (IPCP) packets, and that negotiation is successful.

```
00:38:50: Vi4.1 IPCP: State is Open
00:38:50: Vi4.1 IPCP: Install route to 10.1.1.4
```

Configuring Directed Request Authorization of VPDN Users

Directed requests allow users logging in to a NAS to select a remote AAA server for authentication. With directed requests enabled, only the portion of the username before the "@" symbol is sent to the host specified after the "@" symbol. Using directed requests, you can direct an authentication request to any of the configured remote AAA servers, and only the username is sent to the specified server.

Directed request authorization of VPDN users can be configured on the NAS or on the tunnel server. The directed request configuration is performed on the device that ultimately performs the authentication. Directed requests are most commonly configured on the tunnel server.

Perform one of the following tasks to enable directed request authorization of VPDN users.

- Configuring Directed Request Authorization of VPDN Users on the Tunnel Server, page 76
- Configuring Directed Request Authorization of VPDN Users on the NAS, page 78

Configuring Directed Request Authorization of VPDN Users on the Tunnel Server

Perform this task on the tunnel server to configure directed request authorization of VPDN users when the tunnel server performs authentication.

Prerequisites

- You must perform the task in the "Configuring AAA on the NAS and the Tunnel Server" section.
- The remote RADIUS or TACACS+ AAA server must be configured. For more information on configuring remote RADIUS or TACACS+ AAA servers, refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.
- You must perform the task in the "Configuring Remote AAA for VPDNs" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **ip host** {*name* | **t***modem-telephone-number*} [*tcp-port-number*] *address1* [*address2...address8*]
4. **radius-server directed-request** [**restricted**]
   or
   tacacs-server directed-request [**restricted**] [**no-truncate**]
5. **vpdn authorize directed-request**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip host** {*name* | **t***modem-telephone-number*} [*tcp-port-number*] *address1* [*address2...address8*] **Example:** `Router(config)# ip host website.com 10.3.3.3`	Specifies or modifies the hostname for the network server. **Note** The IP address specified with the **ip host** command must match the IP address you configured with the **radius-server host** or **tacacs-server host** command when performing the task in the "Configuring Remote AAA for VPDNs" section.

Step 4	**radius-server directed-request** [**restricted**]
	or
	tacacs-server directed-request [**restricted**] [**no-truncate**]
	
	Example:
	`Router(config)# radius-server directed-request`
	or
	`Router(config)# tacacs-server directed-request`
		Allows users logging in to a NAS to select a RADIUS server for authentication.
		or
		Allows users logging in to a NAS to select a TACACS+ server for authentication.

Step 5	**vpdn authorize directed-request** **Example:** `Router(config)# vpdn authorize directed-request`	Enables VPDN authorization for directed request users.

What to Do Next

You must perform the process in the "Configuring VPDN Tunnel Authentication" section.

Configuring Directed Request Authorization of VPDN Users on the NAS

Perform this task on the NAS to configure directed request authorization of VPDN users when the NAS performs authentication.

Prerequisites

- You must perform the task in the "Configuring L2TP Domain Screening" section.
- You must perform the task in the "Configuring AAA on the NAS and the Tunnel Server" section.
- The remote RADIUS or TACACS+ AAA server must be configured. For more information on configuring remote RADIUS or TACACS+ AAA servers refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.

You must perform the task in the "Configuring Remote AAA for VPDNs" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip host** {*name* | **t***modem-telephone-number*} [*tcp-port-number*] *address1* [*address2...address8*]
4. **radius-server directed-request** [**restricted**]
   or
   tacacs-server directed-request [**restricted**] [**no-truncate**]
5. **vpdn authorize directed-request**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip host** {*name* | **t***modem-telephone-number*} [*tcp-port-number*] *address1* [*address2...address8*] **Example:** `Router(config)# ip host website.com 10.3.3.3`	Specifies or modifies the hostname for the network server. **Note** The IP address specified with the **ip host** command must match the IP address you configured with the **radius-server host** or **tacacs-server host** command when performing the task in the "Configuring Remote AAA for VPDNs" section.

	Command or Action	Purpose

Step 4	**radius-server directed-request** [**restricted**]
	or
	tacacs-server directed-request [**restricted**] [**no-truncate**]
	Example:
	`Router(config)# radius-server directed-request`
	or
	`Router(config)# tacacs-server directed-request`
		Allows users logging in to a NAS to select a RADIUS server for authentication.
		or
		Allows users logging in to a NAS to select a TACACS+ server for authentication.

Step 5	**vpdn authorize directed-request** **Example:** `Router(config)# vpdn authorize directed-request`	Enables VPDN authorization for directed request users.

What to Do Next

You must perform the process in the "Configuring VPDN Tunnel Authentication" section.

Configuring Domain Name Prefix and Suffix Stripping

When a user connects to a NAS configured to use a remote server for AAA, the NAS forwards the username to the remote AAA server. Some RADIUS or TACACS+ servers require the username to be in a particular format, which may be different from the format of the full username. For example, the remote AAA server may require the username to be in the format user@example.com, but the full username could be prefix/user@example.com@suffix. Configuring domain name stripping allows the NAS to strip incompatible portions from the full username before forwarding the reformatted username to the remote AAA server.

A single set of stripping rules can be configured globally. An independent set of stripping rules can be configured for each Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Global stripping rules are applied to all usernames, and per-VRF rules are applied only to usernames associated with the specified VRF. If a per-VRF rule is configured, it will take precedence over the global rule for usernames associated with that VRF.

The interactions between the different types of domain stripping configurations are as follows:

- You may configure only one instance of the **radius-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] command.
- You may configure multiple instances of the **radius-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*] command with unique values for **vrf** *vrf-name*.
- You may configure multiple instances of the **radius-server domain-stripping strip-suffix** *suffix* [**vrf** *per-vrf*] command to specify multiple suffixes to be stripped as part of a global or per-VRF ruleset.

- Issuing any version of the **radius-server domain-stripping** command automatically enables suffix stripping using the default delimiter character @ for that ruleset, unless a different delimiter or set of delimiters is specified.
- Configuring a per-suffix stripping rule disables generic suffix stripping for that ruleset. Only suffixes that match the configured suffix or suffixes will be stripped from usernames.

For detailed examples of the interactions between different types of domain stripping configurations, see the "Configuring Domain Name Prefix and Suffix Stripping: Examples" section.

Perform this task on the NAS to configure a set of global or per-VRF stripping rules.

Prerequisites

- You must be running Cisco IOS 12.2(13)T or a later release to configure generic suffix stripping using the suffix delimiter @ for usernames forwarded to a remote RADIUS AAA server.
- You must be running Cisco IOS 12.3(4)T or a later release to configure a suffix delimiter or a set of suffix delimiters for usernames forwarded to a remote RADIUS AAA server.
- You must be running Cisco IOS 12.4(4)T or a later release to configure suffix stripping for usernames forwarded to a remote TACACS+ AAA server.
- You must be running Cisco IOS 12.4(4)T or a later release to configure prefix stripping or per-suffix stripping.
- AAA must be enabled on the NAS. Perform the task in the "Configuring AAA on the NAS and the Tunnel Server" section to enable AAA.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*]
   or
   tacacs-server domain-stripping [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*]
4. **radius-server domain-stripping strip-suffix** *suffix* [**vrf** *vrf-name*]

   or

   tacacs-server domain-stripping strip-suffix *suffix* [**vrf** *vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Command or Action	Purpose

Step 3 **radius-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*]
 	
or
 	
tacacs-server domain-stripping [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*]
 	
Example:
`Router(config)# radius-server domain-stripping prefix-delimiter #%&\\ delimiter @/`
 	
or
 	
Example:
`Router(config)# tacacs-server domain-stripping prefix-delimiter %\$ vrf myvrf`
	(Optional) Configures a router to strip suffixes, or both suffixes and prefixes, from the username before forwarding the username to the RADIUS server.
	
	or
	
	(Optional) Configures a router to strip suffixes, or both suffixes and prefixes, from the username before forwarding the username to the TACACS+ server.
	
	• **right-to-left**—Configures the router to parse the username for a delimiter from right to left, rather than in the default direction of left to right. The prefix or suffix will be stripped at the first valid delimiter character detected by the router. Changing the direction that the router parses the username will control the portion of the username that is stripped if multiple valid delimiters are present.
	
	Note Only one parse direction can be configured per set of global or per-VRF rules. The router cannot be configured to parse for prefixes in one direction, and parse for suffixes in the other direction.
	
	• **prefix-delimiter** *character* [*character2...character7*]—Enables prefix stripping and specifies the character or characters that will be recognized as a prefix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\.
	
	Note Enabling prefix stripping will automatically enable suffix stripping using the default suffix delimiter @, unless a different suffix delimiter is configured using the **delimiter** *character* keyword and argument.
	
	• **delimiter** *character* [*character2...character7*]—Specifies the character or characters that will be recognized as a suffix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\.
	
	• **vrf** *vrf-name*—Restricts the stripping configuration to a VRF instance. The *vrf-name* argument specifies the name of a configured VRF.

	Command or Action	Purpose

Step 4	**radius-server domain-stripping strip-suffix** *suffix* [**vrf** *vrf-name*]
	
	or
	
	tacacs-server domain-stripping strip-suffix *suffix* [**vrf** *vrf-name*]
	
	Example:
	`Router(config)# radius-server domain-stripping strip-suffix cisco.com`
	
	or
	
	Example:
	`Router(config)# tacacs-server domain-stripping strip-suffix cisco.net vrf myvrf`
		(Optional) Configures a router to strip a specific suffix from the username before forwarding the username to the RADIUS server.
		
		or
		
		(Optional) Configures a router to strip a specific suffix from the username before forwarding the username to the TACACS+ server.
		
		• **strip-suffix** *suffix*—Enables per-suffix suffix stripping and specifies the string that must be matched for the suffix to be stripped.
		
		Note Both the suffix delimiter and the suffix must match for the suffix to be stripped from the full username. The default suffix delimiter of @ will be used if you do not specify a different suffix delimiter or set of suffix delimiters in Step 3.
		
		• **vrf** *vrf-name*—Restricts the per-suffix stripping configuration to a VRF instance. The *vrf-name* argument specifies the name of a VRF.
		
		Note You may configure a single ruleset to strip multiple specific suffixes by performing this step multiple times.

What to Do Next

For detailed examples of the interactions between different types of domain stripping configurations, see the "Configuring Domain Name Prefix and Suffix Stripping: Examples" section.

You must perform the task in the "Configuring VPDN Tunnel Authentication" section.

Configuring VPDN Tunnel Authentication

VPDN tunnel authentication enables routers to authenticate the other tunnel endpoint before establishing a VPDN tunnel. VPDN tunnel authentication is required for L2F tunnels; it is optional but highly recommended for L2TP, L2TPv3, and PPTP tunnels.

By default, the router will use the hostname as the tunnel name in VPDN tunnel authentication. If a local name is configured under a VPDN group, the router will use the local name when negotiating authentication for tunnels belonging to that VPDN group.

For NAS-initiated VPDN deployments and dial-out VPDN deployments, tunnel authentication requires that a single shared secret be configured on both the NAS and the tunnel server. The password can be configured using the hostname or local name for L2F tunnels. For L2TP tunnels, the password can be configured using the hostname, the local name, or the L2TP tunnel password.

For client-initiated VPDN tunneling deployments, tunnel authentication requires that a single shared secret be configured on both the client and the tunnel server. The available authentication configuration options depend on the tunneling protocol being used.

For L2TPv3 client-initiated VPDN tunnels, the shared secret can be configured on the local peer router and the tunnel server in either of the following ways:

- In an L2TP class configuration. Perform the task "Configuring L2TP Control Channel Authentication Parameters" in the "Configuring Client-Initiated Dial-In VPDN Tunneling" module instead of the process documented in this section.
- Using the hostname of the router as described in the process documented in this section.

For L2TP client-initiated VPDN tunnels, the shared secret can be configured on the tunnel server using the hostname, the local name, or the L2TP tunnel password as described the process documented in this section. The shared secret can be configured on the local peer router in either of the following ways:

- In an L2TP class configuration. Perform the task "Configuring L2TP Control Channel Authentication Parameters" in the "Configuring Client-Initiated Dial-In VPDN Tunneling" module instead of the process documented in this section.
- Using the hostname of the router as described in the process documented in this section.

For PPTP client-initiated VPDN tunnels, authentication parameters may be configured using the hostname or the local name as described in the process documented in this section.

Note If you plan to implement shell-based authentication of VPDN users, it is highly recommended that a separate VPDN group with a distinct local name be created on the tunnel server for users that are authenticated using terminal services, so that only exec VPDN sessions are accepted without authentication.

To configure VPDN tunnel authentication, you must perform one of the following tasks on the NAS and the tunnel server as required. You need not choose the same method to configure the secret on the NAS and the tunnel server. However, the configured password must be the same on both devices.

- Configuring VPDN Tunnel Authentication Using the Hostname, page 83
- Configuring VPDN Tunnel Authentication Using the Local Name, page 84
- Configuring VPDN Tunnel Authentication Using the L2TP Tunnel Password, page 86

VPDN tunnel authentication is optional for L2TP tunnels. Perform the following task on the NAS and the tunnel server if you want to disable VPDN tunnel authentication:

- Disabling VPDN Tunnel Authentication for L2TP Tunnels, page 87

Prerequisites

AAA must be enabled. To enable AAA, perform the task in the "Configuring AAA on the NAS and the Tunnel Server" section.

Configuring VPDN Tunnel Authentication Using the Hostname

Perform this task on the NAS or tunnel server to configure VPDN tunnel authentication using the hostname.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *name*
4. **username** *name* **password** *secret*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**hostname** *name* **Example:** `Router(config)# hostname tunnelserver12`	Specifies or modifies the hostname for the network server.
Step 4	**username** *name* **password** *secret* **Example:** `Router(config)# username nas4 password mysecret`	Establishes a username-based authentication system. • The specified username must be the name of the remote router. • The secret password must be the same on both routers.

What to Do Next

- Once you have configured a secret password on one tunnel endpoint, you must configure the same tunnel secret on the corresponding tunnel endpoint.
- If you are configuring shell-based authentication of VPDN tunnels, you must perform the task in the "Configuring the NAS for Shell-Based Authentication of VPDN Users" section.
- You may perform the task in the "Configuring RADIUS Tunnel Accounting for L2TP VPDNs" section.
- You may configure any of the VPDN-specific remote RADIUS AAA attributes.

Configuring VPDN Tunnel Authentication Using the Local Name

Perform this task on the NAS or tunnel server to configure VPDN tunnel authentication using the local name.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **local name** *host-name*
5. **exit**
6. **username** *name* **password** *secret*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group mygroup`	Enters VPDN group configuration mode and creates a VPDN group.
Step 4	**local name** *host-name* **Example:** `Router(config-vpdn)# local name tunnelserver2`	Specifies a local hostname that the tunnel will use to identify itself.
Step 5	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN group configuration mode.
Step 6	**username** *name* **password** *secret* **Example:** `Router(config)# username nas7 password mysecret`	Establishes a username-based authentication system. • The specified username must be the name of the remote router. • The secret password must be the same on both routers.

What to Do Next

- Once you have configured a secret password on one tunnel endpoint, you must configure the same tunnel secret on the corresponding tunnel endpoint.
- If you are configuring shell-based authentication of VPDN tunnels, you must perform the task in the "Configuring the NAS for Shell-Based Authentication of VPDN Users" section.
- You may perform the task in the "Configuring RADIUS Tunnel Accounting for L2TP VPDNs" section.
- You may configure any of the VPDN-specific remote RADIUS AAA attributes.

Configuring VPDN Tunnel Authentication Using the L2TP Tunnel Password

Perform this task on the NAS or tunnel server to configure VPDN tunnel authentication using the L2TP tunnel password. This task can be used only for VPDN tunnel authentication of L2TP tunnels.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **l2tp tunnel password** *password*
5. **local name** *host-name*
6. **exit**
7. **username** *name* **password** *secret*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group mygroup`	Enters VPDN group configuration mode and creates a VPDN group.
Step 4	**l2tp tunnel password** *password* **Example:** `Router(config-vpdn)# l2tp tunnel password mysecret`	Sets the password that the router will use to authenticate the tunnel.
Step 5	**local name** *host-name* **Example:** `Router(config-vpdn)# local name tunnelserver2`	(Optional) Specifies a local hostname that the tunnel will use to identify itself. • You must perform this step if the remote router does not use the L2TP tunnel password.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-vpdn)# exit`	(Optional) Exits VPDN group configuration mode. • You must perform this step only if the remote router does not use the L2TP tunnel password method of VPDN tunnel authentication.
Step 7	**username** *name* **password** *secret* **Example:** `Router(config)# username nas64 password mysecret`	(Optional) Establishes a username-based authentication system. • You need to perform this step only if the remote router does not use the L2TP tunnel password method of VPDN tunnel authentication. • The specified username must be the name of the remote router. • The password must be the same on both routers.

What to Do Next

- Once you have configured a secret password on one tunnel endpoint, you must configure the same tunnel secret on the corresponding tunnel endpoint.
- If you are configuring shell-based authentication of VPDN tunnels, you must perform the task in the "Configuring the NAS for Shell-Based Authentication of VPDN Users" section.
- You may perform the task in the "Configuring RADIUS Tunnel Accounting for L2TP VPDNs" section.
- You may configure any of the VPDN-specific remote RADIUS AAA attributes.

Disabling VPDN Tunnel Authentication for L2TP Tunnels

Perform this task to disable VPDN tunnel authentication for L2TP tunnels. You must perform this task on both the NAS and the tunnel server to disable VPDN tunnel authentication.

ISUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **no l2tp tunnel authentication**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group mygroup`	Enters VPDN group configuration mode and creates a VPDN group.
Step 4	**no l2tp tunnel authentication** **Example:** `Router(config-vpdn)# no l2tp tunnel authentication`	Disables L2TP tunnel authentication.

What to Do Next

- If you are configuring shell-based authentication of VPDN tunnels, you must perform the task in the "Configuring the NAS for Shell-Based Authentication of VPDN Users" section.
- You may configure any of the VPDN-specific remote RADIUS AAA attributes.

Configuring RADIUS Tunnel Accounting for L2TP VPDNs

RADIUS tunnel accounting for VPDNs is supported by RFC 2867, which introduces six new RADIUS accounting types beginning in Cisco IOS Release 12.3(4)T. The new RADIUS tunnel accounting types are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40), which indicates whether an accounting request marks the beginning of user service (start) or the end (stop).

Without RADIUS tunnel accounting support, VPDN with network accounting will not report all possible attributes to the accounting record file. RADIUS tunnel accounting support allows users to determine tunnel-link status changes. Because all possible attributes can be displayed, users can better verify accounting records with their ISPs.

Enabling tunnel type accounting records allows the router to send tunnel and tunnel-link accounting records to the RADIUS server. The two types of accounting records allow the identification of VPDN tunneling events as described in the following sections.

Tunnel-Type Accounting Records

AAA sends Tunnel-Start, Tunnel-Stop, or Tunnel-Reject accounting records to the RADIUS server to identify the following events:

- A VPDN tunnel is brought up or destroyed.
- A request to create a VPDN tunnel is rejected.

Tunnel-Link-Type Accounting Records

AAA sends Tunnel-Link-Start, Tunnel-Link-Stop, or Tunnel-Link-Reject accounting records to the RADIUS server to identify the following events:

- A user session within a VPDN tunnel is brought up or brought down.
- A user session create request is rejected.

Perform this task to configure a NAS or tunnel server to send tunnel and tunnel-link accounting records to the remote RADIUS server.

Prerequisites

- The router must be running Cisco IOS Release 12.3(4)T or a later release.
- You must perform the tasks in the "Configuring AAA on the NAS and the Tunnel Server" section.
- You must perform the tasks in the "Configuring VPDN Tunnel Authentication" section.
- You must configure the router to use a remote RADIUS AAA server as described in the "Configuring Remote AAA for VPDNs" section.

Restrictions

RADIUS tunnel accounting is supported only for VPDNs using the L2TP protocol.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting network** {**default** | *list-name*} {**start-stop** | **stop-only** | **wait-start** | **none**} **group** *groupname*
4. **vpdn tunnel accounting network** *list-name*
5. **vpdn session accounting network** *list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**aaa accounting network** {**default** | *list-name*} {**start-stop** | **stop-only** | **wait-start** | **none**} **group** *groupname* **Example:** `Router(config)# aaa accounting network list1 start-stop group radius`	Enables network accounting. • **default**—If the default network accounting method-list is configured and no additional accounting configurations are enabled on the interface, network accounting is enabled by default. If either the **vpdn session accounting network** command or the **vpdn tunnel accounting network** command is linked to the **default** method-list, all tunnel and tunnel-link accounting records are enabled for those sessions. • *list-name*—The *list-name* defined in the **aaa accounting** command must be the same as the *list-name* defined in the VPDN command; otherwise, accounting will not occur.
Step 4	**vpdn tunnel accounting network** *list-name* **Example:** `Router(config)# vpdn tunnel accounting network list1`	Enables Tunnel-Start, Tunnel-Stop, and Tunnel-Reject accounting records. • *list-name*—The *list-name* must match the *list-name* defined in the **aaa accounting** command; otherwise, network accounting will not occur.
Step 5	**vpdn session accounting network** *list-name* **Example:** `Router(config)# vpdn session accounting network list1`	Enables Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject accounting records. • *list-name*—The *list-name* must match the *list-name* defined in the **aaa accounting** command; otherwise, network accounting will not occur.

What to Do Next

You may configure any of the VPDN-specific remote RADIUS AAA attributes.

Configuring Authentication of L2TP Tunnels at the Tunnel Terminator Remote RADIUS AAA Server

For L2TP tunnels, you may configure the device that terminates the VPDN tunnel to perform remote RADIUS AAA. A remote RADIUS AAA server can be used to perform VPDN tunnel authentication on the tunnel terminator as follows:

- Using a remote RADIUS AAA server on the tunnel server for dial-in VPDNs
- Using a remote RADIUS AAA server on the NAS for dial-out VPDNs

Perform this task on the remote RADIUS AAA server to configure the RADIUS server to authenticate VPDN tunnels at the device that terminates the tunnel.

Prerequisites

- The router must be running Cisco IOS Release 12.3(4)T or a later release.
- The RADIUS server must be configured for AAA. For more information on configuring remote RADIUS AAA servers refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.
- The service type in the RADIUS user profile for the tunnel initiator should always be set to "Outbound."

Restrictions

This task applies only when the device that terminates the VPDN tunnel is performing remote RADIUS AAA. To configure the tunnel terminator to perform remote RADIUS AAA, perform the task in the "Configuring the Tunnel Terminator for Remote RADIUS AAA for L2TP Tunnels" section.

SUMMARY STEPS

1. **service type =** *Outbound*
2. **tunnel-type =** *protocol*
3. **Cisco:Cisco-Avpair = vpdn:dout-dialer =** *NAS-dialer-number*
4. **Cisco:Cisco-Avpair = vpdn:vpdn-vtemplate =** *vtemplate-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**service type =** *Outbound* **Example:** `service type = Outbound`	Specifies the service type.
Step 2	**tunnel-type =** *protocol* **Example:** `tunnel-type = l2tp`	Specifies the tunneling protocol. **Note** L2TP is the only valid protocol for this task.
Step 3	**Cisco:Cisco-Avpair = vpdn:dout-dialer =** *NAS-dialer-number* **Example:** `Cisco:Cisco-Avpair = vpdn:dout-dialer = 2`	Specifies which dialer to use on the NAS for dial-out configuration. **Note** Perform this step only for dial-out configurations.
Step 4	**Cisco:Cisco-Avpair = vpdn:vpdn-vtemplate =** *vtemplate-number* **Example:** `Cisco:Cisco-Avpair = vpdn:vpdn-vtemplate = 1`	Specifies the virtual template number to use on the tunnel server for dial-in configuration. **Note** Perform this step only for dial-in configurations. **Note** This configuration is optional if the **vpdn tunnel authorization virtual-template** command is used in the task in the "Configuring the Tunnel Terminator for Remote RADIUS AAA for L2TP Tunnels" section.

What to Do Next

You may configure any of the other VPDN-specific remote RADIUS AAA attributes.

Configuring DNS Name Support on the NAS Remote RADIUS AAA Server

NAS remote AAA servers can resolve DNS names and translate them into IP addresses. The server will first look up the name in its name cache. If the name is not in the name cache, the server will resolve the name by using a DNS server.

Perform this task on the NAS remote RADIUS AAA server.

Prerequisites

The RADIUS server must be configured for AAA.

SUMMARY STEPS

1. **l2tp-tunnel-password =** *password*
2. **tunnel-type =** *protocol*
3. **ip-addresses =** *DNS-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**l2tp-tunnel-password =** *password* **Example:** `l2tp-tunnel-password = cisco123`	Specifies the password for the VPDN tunnel.
Step 2	**tunnel-type =** *protocol* **Example:** `tunnel-type = l2tp`	Specifies the tunneling protocol.
Step 3	**ip-addresses =** *DNS-name* **Example:** `ip-addresses = cisco`	Instructs the RADIUS server to resolve the DNS name and tunnel calls to the appropriate IP address.

What to Do Next

You may configure any of the other VPDN-specific remote RADIUS AAA attributes.

Configuring L2TP Tunnel Server Load Balancing and Failover on the NAS Remote RADIUS AAA Server

Perform one of the following tasks on the NAS remote RADIUS AAA server to configure tunnel server load balancing and failover:

Releases Prior to Cisco IOS Release 12.2(4)T

- Configuring L2TP Tunnel Server Load Balancing and Failover Using the Cisco Proprietary VSA, page 93

Cisco IOS Release 12.2(4)T and Later Releases

- Configuring L2TP Tunnel Server Load Balancing and Failover Using the RADIUS Tunnel Preference Attribute, page 94

Configuring L2TP Tunnel Server Load Balancing and Failover Using the Cisco Proprietary VSA

Until Cisco IOS Release 12.2(4)T, load balancing and failover functionality for L2TP tunnel servers was provided by the Cisco proprietary Vendor Specific Attribute (VSA). A specially formatted string would be transported within a Cisco VSA "vpdn:ip-addresses" string from the RADIUS server to a NAS for the purpose of tunnel server load balancing and failover. For example, 10.0.0.1 10.0.0.2 10.0.0.3/10.0.0.4 10.0.0.5 would be interpreted as IP addresses 10.0.0.1, 10.0.0.2, and 10.0.0.3 for the first group for load balancing. New sessions are projected to these three addresses based on the least-load-first algorithm. This algorithm uses its local knowledge to select a tunnel server that has the least load to initiate the new session. In this example, the addresses 10.0.0.4 and 10.0.0.5 in the second group have a lower priority and are applicable only when all tunnel servers specified in the first group fail to respond to the new connection request, thereby making 10.0.0.4 and 10.0.0.5 the failover addresses.

Perform this task on the NAS remote RADIUS server to assign tunnel server priorities for load balancing and failover.

Prerequisites

- The RADIUS server must be configured for AAA.

SUMMARY STEPS

1. **ip-addresses =** {*ip-address* | *dns-name*} {**,** | **/**} {*ip-address* | *dns-name*}{**,** | **/**} [*ip-address* | *dns-name*] ...

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ip-addresses =** {*ip-address* | *dns-name*} {**,** | **/**} {*ip-address* | *dns-name*} {**,** | **/**} [*ip-address* | *dns-name*].... **Example:** `ip-addresses = 172.16.171.11, 172.16.171.12, 172.16.171.13/mydomain`	Configures the IP addresses of the tunnel servers that the load will be balanced over. • Separating the IP addresses with a spaces or a comma specifies that the load will be equally balanced over the tunnel servers. • Using a slash to separate IP addresses specifies that the IP addresses after the slash will only be contacted if the other specified tunnel servers are unavailable. • A DNS name can be used in place of an IP address.

What to Do Next

You may configure any of the other VPDN-specific remote RADIUS AAA attributes.

Configuring L2TP Tunnel Server Load Balancing and Failover Using the RADIUS Tunnel Preference Attribute

In a multivendor network environment, using a VSA on a RADIUS server can cause interoperability issues among NASs manufactured by different vendors. Even though some RADIUS server implementations can send VSAs that the requesting NAS can understand, the user still must maintain different VSAs for the same purpose in a single-service profile.

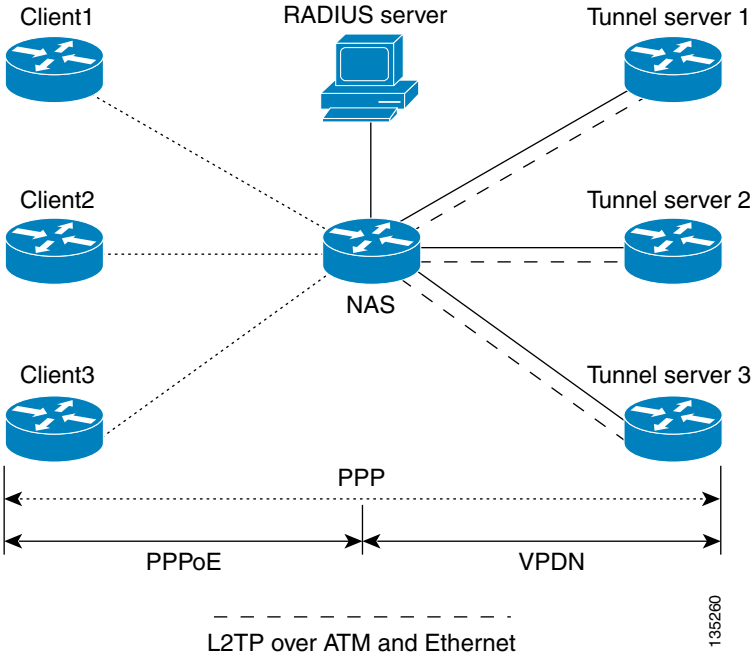
A consensus regarding the tunnel attributes that are to be used in a multivendor network environment is defined in RFC 2868. In RFC 2868, Tunnel-Server-Endpoint specifies the address to which the NAS should initiate a new session. If multiple Tunnel-Server-Endpoint attributes are defined in one tagged attribute group, they are interpreted as equal-cost load-balancing tunnel servers.

In Cisco IOS Release 12.2(4)T and later releases, the Tunnel-Preference attribute defined in RFC 2868 can be used to form load balancing and failover tunnel server groups. When the Tunnel-Preference values of different tagged attribute groups are the same, the Tunnel-Server-Endpoint of those attribute groups is considered to have the same priority unless otherwise specified. When the Tunnel-Preference values of some attribute groups are higher (they have a lower preference) than other attribute groups, their Tunnel-Server-Endpoint attributes will have higher priority values. When an attribute group has a higher priority value, that attribute group will be used for failover in case the attribute groups with lower priority values are unavailable for the connections.

Note Support for the Tunnel-Preference attribute was introduced on Cisco access server platforms in Cisco IOS Release 12.2(11)T.

The RADIUS Tunnel-Preference attribute is useful for large multivendor networks that use VPDN Layer 2 tunnels over WAN links such as ATM and Ethernet, such as the configuration shown in Figure 15.

Figure 15 Typical Load Balancing and Failover in a Multivendor Network



In the configuration shown in Figure 15, the NAS uses tunnel profiles downloaded from the RADIUS server to establish load balancing and failover priorities for VPDN Layer 2 tunnels. The Point-to-Point over Ethernet (PPPoE) protocol is used as the client to generate PPP sessions.

When multiple tunnel servers of the same priority are configured, the NAS will select the tunnel server with the lowest number of active sessions. If several tunnel servers have the same number of active sessions, the NAS must use a tie-breaking mechanism to determine which to select.

In Cisco IOS releases prior to 12.4(4)T, the NAS uses a round-robin selection as the tie-breaking mechanism. Because each NAS is aware only of its own session load, multiple NASs using the same round-robin algorithm may unevenly distribute sessions across the tunnel servers (session bunching). Each NAS selects the same tunnel server in the case of a tie because the round-robin tie-breaking mechanism always resolves to the same tunnel server. Session bunching is especially prominent when there is a very low number of sessions on each NAS.

Beginning in Cisco IOS Release 12.4(4)T, the NAS uses a new tie-breaking algorithm. A random selection is made among all peer tunnel servers carrying the same session load. This improved algorithm results in a more even distribution of sessions across tunnel servers, reducing the occurrence of session bunching.

Perform this task on the NAS remote RADIUS server to assign a priority value to each tunnel server for load balancing and failover.

Prerequisites

- The NAS must be running Cisco IOS Release 12.2(4)T or a later release.
- On Cisco access server platforms, you must be running Cisco IOS Release 12.2(11)T or a later release.
- The RADIUS server must be configured for AAA.

Restrictions

- Dial-out VPDN deployments are not supported.
- The maximum number of tunnel servers allowed in the network is 1550, which is 50 per tagged attribute group with a limit of 31 tags.
- This feature requires a RADIUS server implementation that supports RFC 2868.

SUMMARY STEPS

1. **Tunnel-Server-Endpoint = :***tag***: "***ip-address***",**
2. **Tunnel-Preference = :***priority***:***tag***,**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Tunnel-Server-Endpoint = :***tag***: "***ip-address***",** **Example:** `Tunnel-Server-Endpoint = :0:"10.1.1.1",`	Specifies the IP address of a tunnel server.
Step 2	**Tunnel-Preference = :**priority**:**tag**,** **Example:** `Tunnel-Preference = :0:1,`	Specifies the priority of the tunnel server for load balancing and failover. • A lower value for the *priority* argument gives a higher priority to the tunnel server.

What to Do Next

- See the "Configuring L2TP Tunnel Server Load Balancing and Failover using the RADIUS Tunnel Preference Attribute: Example" section for a set of complete RADIUS tunnel profiles using the Tunnel-Preference attribute to define priority levels for load balancing and failover.
- You may configure any of the other VPDN-specific remote RADIUS AAA attributes.

Configuring Tunnel Assignments on the NAS Remote RADIUS AAA Server

Tunnel assignments allow the grouping of users from different per-user or domain RADIUS profiles into the same active tunnel. This functionality prevents the establishment of duplicate tunnels when the tunnel type, tunnel endpoints, and tunnel assignment ID are identical.

Perform this task on the NAS remote RADIUS AAA server for each user and domain that you want to group into the same tunnel.

Prerequisites

- The RADIUS server must be configured for AAA.
- The NAS must be running Cisco IOS Release 12.2(4)T or a later release.

SUMMARY STEPS

1. *user@domain.com* **Password = "***secret***" Service-Type = Outbound**

or

user.domain.com **Password = "***secret***" Service-Type = Outbound**

2. **tunnel-type =** *protocol*
3. **tunnel-server-endpoint =** *ip-address*
4. **tunnel-assignment-id =** *name*

DETAILED STEPS

	Command or Action	Purpose

Step 1	*user***@***domain.com* **Password = "***secret***" Service-Type = Outbound**
	
	or
	
	user.domain.com **Password = "***secret***" Service-Type = Outbound**
	
	Example:
	`user@cisco.com Password = "cisco" Service-Type = Outbound`
	
	or
	
	`user.cisco.com Password = "cisco" Service-Type = Outbound`
		Specifies the user or domain, the tunnel password, and the service type.

Step 2	**tunnel-type =** *protocol* **Example:** `tunnel-type = l2tp`	Specifies the tunneling protocol used. • The tunnel type must be identical for users to be grouped into the same tunnel.
Step 3	**tunnel-server-endpoint =** *ip-address* **Example:** `tunnel-server-endpoint = 10.1.1.1`	Specifies the IP address of the tunnel server that calls from the specified user or domain are tunneled to. • The tunnel server endpoint must be identical for users to be grouped into the same tunnel.
Step 4	**tunnel-assignment-id =** *name* **Example:** `tunnel-assignment-id = group1`	Specifies the tunnel ID that calls from the specified user or domain are assigned. • The tunnel assignment ID must be identical for users to be grouped into the same tunnel.

What to Do Next

You may configure any of the other VPDN-specific remote RADIUS AAA attributes.

Configuring L2TP Tunnel Connection Speed Labeling on the Remote ARS RADIUS AAA Server and the Tunnel Server

Tunnel connection speed labeling allows L2TP sessions to be accepted or denied based on the allowed connection speed that is configured on the Cisco Access Registrar (ARS) RADIUS server for that user. The administrator can configure an ARS RADIUS server to authorize users based on their Service Level Agreement (SLA). Tunnel connection speed information is forwarded to the ARS RADIUS server by default.

Prerequisites

You must be running Cisco IOS Release 12.3(4)T or a later release.

Restrictions

- This feature can be used only with the ARS RADIUS server.
- This feature can be used only with the L2TP tunneling protocol.

Perform the following tasks to configure tunnel connection speed labeling:

- Configuring User Profiles on the ARS RADIUS Server for L2TP Tunnel Connection Speed Labeling, page 98 (required)
- Disabling L2TP Tunnel Connection Speed Labeling on the Tunnel Server, page 99 (optional)
- Configuring L2TP Tunnel Connection Speed Labeling on the Tunnel Server, page 100 (optional)
- Configuring L2TP Tunnel Connection Speed Labeling for a Tunnel Switch, page 101 (optional)

Configuring User Profiles on the ARS RADIUS Server for L2TP Tunnel Connection Speed Labeling

By default, the L2TP tunnel server will forward connection speed information to the AR RADIUS server for authentication. For the AR RADIUS server to perform authentication based on tunnel connection speed information, the user profiles on the ARS RADIUS server must be configured with the allowed connection speed.

Perform this task on the ARS RADIUS server to configure connection speed information in user profiles.

Prerequisites

- The ARS RADIUS server must be configured for AAA. For more information on configuring remote RADIUS AAA servers refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.
- The L2TP tunnel server must be running Cisco IOS Release 12.3(4)T or a later release.

SUMMARY STEPS

1. *user@example.com*
2. **userdefined1 =** [**TX:***speed*[**-***maxspeed*]] [**:**] [**RX:***speed*[**-***maxspeed*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	*user@example.com* **Example:** user@example.com	Specifies the user that the profile is for.
Step 2	**userdefined1 =** [**TX:***speed*[**-***maxspeed*]] [**:**] [**RX:***speed*[**-***maxspeed*]] **Example:** userdefined1 = TX:102400000:RX:96000000-200000000	Specifies the allowable transmission and receiving connection speeds. • A range of connection speeds can be specified. • If no connection speed is specified, any speed will be allowed.

What to Do Next

- If the inclusion of RADIUS attribute 77 in authentication requests has previously been disabled on the tunnel server, you must perform the task in the "Configuring L2TP Tunnel Connection Speed Labeling on the Tunnel Server" section.
- You may perform the task in the "Configuring L2TP Tunnel Connection Speed Labeling for a Tunnel Switch" section.
- You may configure any of the other VPDN-specific remote RADIUS AAA attributes.

Disabling L2TP Tunnel Connection Speed Labeling on the Tunnel Server

By default, the L2TP tunnel server will forward connection speed information to the RADIUS server for authentication. To disable authentication based on connection speeds, you must choose to not include RADIUS attribute 77 in the access request.

Perform this task on the tunnel server to disable authentication based on connection speeds.

Prerequisites

- You must first perform the tasks in the "Configuring AAA on the NAS and the Tunnel Server" section and the "Configuring VPDN Tunnel Authentication" section.
- The tunnel server must be running Cisco IOS Release 12.3(4)T, Cisco IOS Release 12.2(28)SB, or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no radius-server attribute 77 include-in-access-req**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no radius-server attribute 77 include-in-access-req** **Example:** `Router(config)# no radius-server attribute 77 include-in-access-req`	Disables the sending of connection speed information to the RADIUS server in the access request.

What to Do Next

You may configure any of the other VPDN-specific remote RADIUS AAA attributes.

Configuring L2TP Tunnel Connection Speed Labeling on the Tunnel Server

Perform this task on the L2TP tunnel server to enable authentication based on connection speeds if it has been previously disabled.

Prerequisites

- You must first perform the tasks in the "Configuring AAA on the NAS and the Tunnel Server" section and the "Configuring VPDN Tunnel Authentication" section.
- You must be running Cisco IOS Release 12.3(4)T, Cisco IOS Release 12.2(28)SB, or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 77 include-in-access-req**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute 77 include-in-access-req** **Example:** `Router(config)# radius-server attribute 77 include-in-access-req`	Sends connection speed information to the RADIUS server in the access request. **Note** The **radius-server attribute 77 include-in-access-req** command is enabled by default. You need to perform this task only if you have previously disabled the **radius-server attribute 77 include-in-access-req** command. **Note** When the **radius-server attribute 77 include-in-access-req** command is enabled, it is not visible in NVGEN. This is because the **radius-server attribute 77 include-in-access-req** command is enabled by default.

What to Do Next

You may configure any of the other VPDN-specific remote RADIUS AAA attributes.

Configuring L2TP Tunnel Connection Speed Labeling for a Tunnel Switch

Perform this task on the tunnel switch to enable L2TP tunnel connection speed labeling for a tunnel switch node. This configuration allows the access request to be sent to the RADIUS server before the tunnel switch forwards the session to the next hop.

Prerequisites

- You must first perform the tasks in the "Configuring AAA on the NAS and the Tunnel Server" section and the "Configuring VPDN Tunnel Authentication" section.
- You must be running Cisco IOS Release 12.3(4)T or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn authen-before-forward**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn authen-before-forward** **Example:** `Router(config)# vpdn authen-before-forward`	Requests authentication and authorization of an L2TP tunnel before it is forwarded to the tunnel server.

What to Do Next

You may configure any of the other VPDN-specific remote RADIUS AAA attributes.

Configuring Secure Tunnel Authentication Names on the NAS Remote RADIUS AAA Server

The NAS AAA server can be configured with authentication names other than the default names for the NAS and the NAS AAA server, providing a higher level of security during VPDN tunnel establishment.

RADIUS tunnel authentication name attributes allows you to specify a name other than the default name for the tunnel initiator and for the tunnel terminator. These authentication names are specified using RADIUS tunnel attributes 90 and 91.

Perform this task on the remote RADIUS AAA server. This task applies to NAS-initiated tunnels using either L2TP or L2F.

Prerequisites

- The RADIUS server must be configured for AAA.
- The NAS must be running Cisco IOS Release 12.2(13)T or a later release to recognize RADIUS attributes 90 and 91.
- The RADIUS server must support tagged attributes to use RADIUS tunnel attributes 90 and 91. Tagged attributes are defined in RFC 2868, *RADIUS Tunnel Authentication Attributes*.

SUMMARY STEPS

1. *user@example.com* **Password =** "*secret*" **Service-Type = Outbound**

   or

   user.example.com **Password =** "*secret*" **Service-Type = Outbound**

2. **Tunnel-Client-Auth-Id = {:1 | :2}: "***NAS-name***"**
3. **Tunnel-Server-Auth-Id = {:1 | :2}: "***tunnel-server-name***"**

DETAILED STEPS

	Command or Action	Purpose
Step 1	*user*@*example.com* **Password =** "*secret*" **Service-Type = Outbound** or *user.example.com* **Password =** "*secret*" **Service-Type = Outbound** **Example:** user@cisco.com Password = "cisco" Service-Type = Outbound or user.cisco.com Password = "cisco" Service-Type = Outbound	Specifies the user or domain, the tunnel password, and the service type.
Step 2	**tunnel-client-auth-id =** {**:1** | **:2**}**: "***NAS-name***"** **Example:** tunnel-client-auth-id = :2:NAS36	Specifies the name used by the NAS when it authenticates tunnel setup with the tunnel server. • **:1**—Specifies L2F tunnels. • **:2**—Specifies L2TP tunnels.
Step 3	**tunnel-server-auth-id =** {**:1** | **:2**}**:** "*tunnel-server-name*" **Example:** tunnel-server-auth-id = :2:TS14	Specifies the name used by the tunnel server when it authenticates tunnel setup with the NAS. • **:1**—Specifies L2F tunnels. • **:2**—Specifies L2TP tunnels.

What to Do Next

You may configure any of the other VPDN-specific remote RADIUS AAA attributes.

Configuring the NAS for Shell-Based Authentication of VPDN Users

Shell-based authentication of VPDN users provides terminal services (shell login or exec login) for VPDN users. With shell-based authentication enabled, when clients dial in to the NAS, authentication occurs in character mode. Once authentication is complete, PPP starts and a tunnel is established based on either DNIS or domain.

Enabling shell-based authentication of VPDN users provides the following capabilities:

- Authentication of a dial-in user session occurs at the NAS before PPP is started or a tunnel is established. If authentication fails, the user session can be terminated before tunneling resources are used.

- Authentication of a PPP user can be performed using authentication methods other than CHAP and Password Authentication Protocol (PAP). A character-mode login dialog such as username/password or username/challenge/password, Secure ID, or Safeword can be used. PPP authentication data is preconfigured or entered before PPP starts. Authentication is completed without any further input from the user.

For the NAS to perform shell-based VPDN authentication, it must be configured for AAA, PPP must be configured to bypass authentication, and DNIS must be enabled.

Perform this task to configure the NAS for shell-based authentication of VPDN users.

Prerequisites

- You must be running Cisco IOS Release 12.2(2)T or a later release.
- The dialup line interface can be configured with the **autoselect during-login** command to allow smooth login terminal services.
- The dialup line interface can be configured with the **autocommand ppp** command. This denies the PPP user access to the exec shell, but allows entry to tunneled PPP.
- RPMS can be configured.
- Multilink PPP (MLP) can be configured.
- You must perform the task in the "Configuring AAA on the NAS and the Tunnel Server" section.
- You must perform the task in the "Configuring the NAS for Remote AAA for Dial-In VPDNs" section.
- You must perform the task in the "Configuring VPDN Tunnel Authentication" section. It is highly recommended that a separate VPDN group with a distinct local name be created on the tunnel server for users that are authenticated using terminal services, so that only the exec VPDN sessions are accepted without authentication.
- The remote RADIUS server must be configured for AAA. For detailed information about configuring remote RADIUS servers, refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.
- For increased security, it is recommended that you provide additional protection of the L2TP tunnel using L2TP security. For information on configuring L2TP security, see the "Configuring Additional VPDN Features" module.
- To use the **aaa dnis map authentication group** aaa-server-group configuration command, you must first enable AAA, define a AAA server group, and enable DNIS mapping.

Restrictions

- Per-user virtual profiles on the tunnel server are not supported.
- Callback is not supported.
- Only those login schemes supported by the NAS exec login features are supported.
- If VPDN fails to be established (for example, Resource Pool Manager Server (RPMS) denies the session), the dialup call is terminated. An exec PPP session is not terminated locally on the NAS if the desired VPDN session fails to be established because the user was presumed authenticated by an AAA server at the remote enterprise.

- Although an exec VPDN tunnel server accepts a tunneled PPP session without authenticating the PPP clients, the tunnel itself must be mutually authenticated by both the NAS and the tunnel server. To further reduce security risks, create a separate VPDN group with a distinct local name on the tunnel server so that only the exec VPDN sessions are accepted without authentication.
- If a DNIS is mapped to a AAA server, the DNIS should also be mapped to a corresponding tunnel server in the VPDN configuration.
- The AAA server and the tunnel server, both of which can be mapped to by either a DNIS or domain name, must belong to the same enterprise and must be accessible to the NAS.
- When configuring AAA authentication at login, do not use "local" as a value for the *method-name* argument of the **aaa authentication login** command. Specifying "local" as a *method-name* would allow an end user to tunnel to a remote tunnel server after local authentication.
- The AAA server group mapped to by the DNIS is intended to authenticate users that are to be connected to the tunnel server network, and thus must not be used for authenticating local users.
- The **ppp dnis** command must not be used on the exec VPDN dialup interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa dnis map enable**
4. **aaa dnis map** *dnis-number* **authentication login group** *server-group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa dnis map enable** **Example:** `Router(config)# aaa dnis map enable`	Enables DNIS mapping for locating a AAA server.
Step 4	**aaa dnis map** *dnis-number* **authentication login group** *server-group-name* **Example:** `Router(config)# aaa dnis map 7777 authentication login group EXEC-VPDN-login-servers`	Maps a DNIS number to a particular authentication server group (this server group is used for AAA authentication).

What to Do Next

See the "Configuring Shell-Based Authentication of VPDN Users: Examples" section for detailed examples of shell-based authentication of VPDN users configurations.

Configuration Examples for AAA for VPDNs

This section contains the following configuration examples:

Configuring the VPDN Tunnel Authorization Search Order: Examples

The following configuration example enables VPDN and configures a tunnel authorization search order that will be used instead of the default search order of DNIS number, then domain.

```
vpdn enable
vpdn search-order domain dnis
```

The following example enables VPDN and multihop, and configures a tunnel authorization search order of multihop hostname first, then domain, then DNIS number. This configuration is used only on a tunnel switch.

```
vpdn enable
vpdn multihop
vpdn search-order multihop-hostname domain dnis
```

Configuring per-User VPDN on the NAS: Examples

The following example enables VPDN and configures global per-user VPDN on the NAS for all dial-in VPDN tunnels. The first time the NAS contacts the remote RADIUS AAA server, the entire structured username will be sent rather than just the domain name or DNIS number.

```
vpdn enable
vpdn authen-before-forward
```

The following example enables VPDN and configures per-user VPDN on the NAS for dial-in VPDN tunnels belonging to the VPDN group named cisco1. The first time the NAS contacts the remote RADIUS AAA server, the entire structured username will be sent rather than just the domain name or DNIS number.

```
vpdn enable
vpdn-group cisco1
 request-dialin
  protocol l2tp
  exit
 authen-before-forward
```

Configuring AAA on the NAS and the Tunnel Server: Examples

The following example enables VPDN and local authentication and authorization on the NAS or the tunnel server:

```
vpdn enable
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
aaa authorization network default local
```

The following examples enables VPDN and configures the NAS and the tunnel server for dial-in VPDN tunnels when remote RADIUS AAA authentication occurs at the NAS:

NAS Configuration

```
vpdn enable
!
aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default radius
aaa accounting network default start-stop radius
radius-server host 10.1.1.1 auth-port 1939 acct-port 1443
vpdn aaa untagged
```

Tunnel Server Configuration

```
vpdn enable
!
aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default radius
aaa accounting network default start-stop radius
vpdn aaa attribute nas-ip-address vpdn-nas
vpdn aaa untagged
```

The *Basic TACACS+ Configuration Example* document provides a basic configuration of TACACS+ for user dialup authentication to a NAS.

Configuring Remote AAA for VPDNs on the L2TP Tunnel Terminator: Examples

The following example enables VPDN and configures the NAS and the tunnel server for dial-in VPDN tunnels with remote RADIUS AAA authentication occurring at the tunnel server. A sample RADIUS user profile for the remote RADIUS AAA server is also shown.

NAS Configuration

```
vpdn enable
!
aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default radius
aaa accounting network default start-stop radius
radius-server host 10.1.1.1 auth-port 1939 acct-port 1443
vpdn aaa untagged
```

Tunnel Server Configuration

```
vpdn enable
!
aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default mymethodlist group myvpdngroup
radius-server host 10.2.2.2 auth-port 1939 acct-port 1443
aaa group server radius myvpdngroup
 server 10.2.2.2 auth-port 1939 acct-port 1443
!
vpdn tunnel authorization network mymethodlist
vpdn tunnel authorization virtual-template 1
```

RADIUS User Profile

```
csidtw13  Password = "cisco"
        Service-Type = Outbound,
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Client-Auth-ID = :0:"csidtw13",
        Tunnel-Password = :0:"cisco"
        Cisco:Cisco-Avpair = "vpdn:vpdn-vtemplate=1"
```

Configuring Directed Request Authorization of VPDN Users: Examples

The following example enables VPDN and configures remote RADIUS AAA with VPDN authentication of directed request users on the tunnel server:

```
vpdn enable
!
aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default mymethodlist group myvpdngroup
radius-server host 10.3.3.3 auth-port 1939 acct-port 1443
aaa group server radius myvpdngroup
```

```
 server 10.3.3.3 auth-port 1939 acct-port 1443
!
ip host website.com 10.3.3.3
radius-server directed-request
vpdn authorize directed-request
```

The following example enables VPDN and configures per-user VPDN, remote TACACS+ AAA, and VPDN authentication of directed request users on the NAS:

```
vpdn enable
vpdn-group 1
 request-dialin
  protocol l2tp
  domain website.com
!
 initiate-to 10.3.3.3
 local name local1
 authen-before-forward
!
aaa new-model
aaa authentication login default tacacs
aaa authentication ppp default tacacs
aaa authorization network default mymethod group mygroup
radius-server host 10.4.4.4 auth-port 1201 acct-port 1450
aaa group server tacacs mygroup
 server 10.3.3.3 auth-port 1201 acct-port 1450
!
ip host website.com 10.3.3.3
radius-server directed-request
vpdn authorize directed-request
```

Configuring Domain Name Prefix and Suffix Stripping: Examples

The following example configures the router to parse the username from right to left and sets the valid suffix delimiter characters as @, \, and $. If the full username is cisco/user@cisco.com$cisco.net, the username “cisco/user@cisco.com” will be forwarded to the RADIUS server because the $ character is the first valid delimiter encountered by the NAS when parsing the username from right to left.

```
radius-server domain-stripping right-to-left delimiter @\$
```

The following example configures the router to strip the domain name from usernames only for users associated with the VRF instance named abc. The default suffix delimiter @ will be used for generic suffix stripping.

```
radius-server domain-stripping vrf abc
```

The following example enables prefix stripping using the character / as the prefix delimiter. The default suffix delimiter character @ will be used for generic suffix stripping. If the full username is cisco/user@cisco.com, the username “user” will be forwarded to the TACACS+ server.

```
tacacs-server domain-stripping prefix-delimiter /
```

The following example enables prefix stripping, specifies the character / as the prefix delimiter, and specifies the character # as the suffix delimiter. If the full username is cisco/user@cisco.com#cisco.net, the username “user@cisco.com” will be forwarded to the RADIUS server.

```
radius-server domain-stripping prefix-delimiter / delimiter #
```

The following example enables prefix stripping, configures the character / as the prefix delimiter, configures the characters $, @, and # as suffix delimiters, and configures per-suffix stripping of the suffix cisco.com. If the full username is cisco/user@cisco.com, the username "user" will be forwarded to the TACACS+ server. If the full username is cisco/user@cisco.com#cisco.com, the username "user@cisco.com" will be forwarded.

```
tacacs-server domain-stripping prefix-delimiter / delimiter $@#
tacacs-server domain-stripping strip-suffix cisco.com
```

The following example configures the router to parse the username from right to left and enables suffix stripping for usernames with the suffix cisco.com. If the full username is cisco/user@cisco.net@cisco.com, the username "cisco/user@cisco.net" will be forwarded to the RADIUS server. If the full username is cisco/user@cisco.com@cisco.net, the full username will be forwarded.

```
radius-server domain-stripping right-to-left
radius-server domain-stripping strip-suffix cisco.com
```

The following example configures a set of global stripping rules that will strip the suffix cisco.com using the delimiter @, and a different set of stripping rules for usernames associated with the VRF named myvrf:

```
radius-server domain-stripping strip-suffix cisco.com
!
radius-server domain-stripping prefix-delimiter # vrf myvrf
radius-server domain-stripping strip-suffix cisco.net vrf myvrf
```

Configuring VPDN Tunnel Authentication: Examples

The following example configures VPDN tunnel authentication using the hostname on a NAS and the local name on the tunnel server. Note that the secret password configured for each device matches.

NAS Configuration

```
hostname NAS1
username tunnelserver1 password supersecret
```

Tunnel Server Configuration

```
vpdn-group 1
 local name tunnelserver1
 exit
username NAS1 password supersecret
```

The following example configures VPDN tunnel authentication using the local name on the NAS and the L2TP tunnel password on the tunnel server. Note that the secret password configured for each device matches.

NAS Configuration

```
vpdn-group 2
 local name NAS6
!
username tunnelserver12 password verysecret
```

Tunnel Server Configuration

```
vpdn-group 4
 l2tp tunnel password verysecret
```

```
 local name tunnelserver12
 exit
username NAS6 password verysecret
```

The following example configures VPDN tunnel authentication using the L2TP tunnel password on both the NAS and the tunnel server. Note that the secret password configured for each device matches.

NAS Configuration

```
vpdn-group l2tp
 l2tp tunnel password rathersecret
```

Tunnel Server Configuration

```
vpdn-group 46
 l2tp tunnel password rathersecret
```

L2TP Domain Screening: Examples

This section provides the following configuration examples:

- L2TP Domain Screening with Global Preauthentication: Example, page 111
- L2TP Domain Screening with per-VPDN Group Preauthentication: Example, page 113

L2TP Domain Screening with Global Preauthentication: Example

The following partial sample configuration shows the L2TP Domain Screening feature with global preauthentication.

```
Router# show running-config
!
.
.
.
hostname esr1-client
.
.
.
aaa new-model
!
aaa authentication login mylist enable line
aaa authentication ppp default group radius
aaa authorization network default group radius
!
aaa nas port extended
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip host example-2 10.0.0.253
!
vpdn enable
vpdn authen-before-forward
vpdn ip udp ignore checksum
vpdn search-order domain
!
vpdn-group 1

 accept-dialin
 protocol pppoe
```

```
 virtual-template 1
pppoe limit per-mac 2
pppoe limit per-vc 2
pppoe limit per-vlan 2
pppoe limit max-sessions 2
!
ppp hold-queue 80000
no virtual-template snmp
!
.
.
.
!
interface Loopback1
 no ip address
!
interface FastEthernet0/0/0
 ip address 10.5.11.7 255.255.0.0
 speed 100
 full-duplex
 hold-queue 4096 in
 hold-queue 4096 out
!
interface GigabitEthernet1/0/0
 no ip address
 negotiation auto
!
!
interface ATM4/0/0.101 multipoint
 atm pppatm passive
 range pvc 52/101 52/101
 encapsulation aal5autoppp Virtual-Template1
!
 pvc-in-range 52/101
 vpn service znet.net1 replace-authen-domain
!
!
interface ATM5/0/0
 no ip address
 no ip mroute-cache
 no atm pxf queuing
 atm clock INTERNAL
 no atm auto-configuration
 no atm ilmi-keepalive
 no atm address-registration
 no atm ilmi-enable
!
interface ATM5/0/0.101 multipoint
 atm pppatm passive
 range pvc 51/101 51/101
 encapsulation aal5autoppp Virtual-Template1
 !
  pvc-in-range 51/101
vpn service znet.net1 replace-authen-domain
 !
!
.
.
.
radius-server attribute nas-port format d
radius-server host 10.5.6.100 auth-port 1645 acct-port 1646
radius-server retransmit 4
radius-server timeout 15
radius-server key cisco
```

```
!
control-plane
!

call admission limit 90
!
.
.
.
!
end
```

L2TP Domain Screening with per-VPDN Group Preauthentication: Example

The following partial sample configuration shows the L2TP Domain Screening feature with per-VPDN group preauthentication.

```
Router# show running-config
!
.
.
.
hostname esr1-client
.
.
.
aaa new-model
!
!
aaa authentication login mylist enable line
aaa authentication ppp default local
aaa authorization network default local
!
aaa nas port extended
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip host example-2 10.0.0.253
!
!
vpdn enable
vpdn ip udp ignore checksum
vpdn search-order domain
!
vpdn-group 1
 accept-dialin
 protocol pppoe
 virtual-template 1
 pppoe limit per-mac 2
 pppoe limit per-vc 2
 pppoe limit per-vlan 2
 pppoe limit max-sessions 2
!
!
vpdn-group LAC_1
 request-dialin
 protocol l2tp
 domain znet.net1
 initiate-to ip 10.1.1.1
 local name LAC1-1
 authen-before-forward
```

```
 l2tp tunnel password 0 tunnel
!
ppp hold-queue 80000
no virtual-template snmp
username LAC1-1 nopassword
username LNS1-1 nopassword
username user-1-1@znet.net1 password 0 sanfran_1_1
.
.
.
!
interface ATM4/0/0.101 multipoint
 atm pppatm passive
 range pvc 52/101 52/101
 encapsulation aal5autoppp Virtual-Template1
!
 pvc-in-range 52/101
 vpn service znet.net1 replace-authen-domain
 !
!
interface ATM5/0/0
 no ip address
 no ip mroute-cache
 no atm pxf queuing
 atm clock INTERNAL
 no atm auto-configuration
 no atm ilmi-keepalive
 no atm address-registration
 no atm ilmi-enable
!
interface ATM5/0/0.101 multipoint
 atm pppatm passive
 range pvc 51/101 51/101
 encapsulation aal5autoppp Virtual-Template1
 !
 pvc-in-range 51/101
 vpn service znet.net1 replace-authen-domain
 !
.
.
.
radius-server attribute nas-port format d
!
control-plane
!
call admission limit 90
!
.
.
.
end
```

Configuring RADIUS Tunnel Accounting on a NAS: Example

The following example configures a NAS for remote AAA, configures a dial-in VPDN deployment, and enables the sending of tunnel and tunnel-link accounting records to the RADIUS server:

```
aaa new-model
!
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting network m1 start-stop group radius
```

```
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$IDjH$iL7puCja1RMlyOM.JAeuf/
enable password secret
!
username ISP-LAC password 0 tunnelpass
!
resource-pool disable
!
ip subnet-zero
ip cef
no ip domain-lookup
ip host myhost 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
 request-dialin
 protocol l2tp
 domain cisco.com
 initiate-to ip 10.1.26.71
 local name ISP-LAC
!
isdn switch-type primary-5ess
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
controller T1 7/4
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
interface FastEthernet0/0
 ip address 10.1.27.74 255.255.255.0
 no ip mroute-cache
 duplex half
 speed auto
 no cdp enable
!
interface FastEthernet0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
interface Serial7/4:23
 ip address 10.0.0.2 255.255.255.0
 encapsulation ppp
 dialer string 2000
 dialer-group 1
 isdn switch-type primary-5ess
 ppp authentication chap
!
interface Group-Async0
 no ip address
 shutdown
 group-range 1/00 3/107
!
```

```
ip default-gateway 10.1.27.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.27.254
no ip http server
ip pim bidir-enable
!
dialer-list 1 protocol ip permit
no cdp run
!
radius-server host 172.19.192.26 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
```

Configuring RADIUS Tunnel Accounting on a Tunnel Server: Example

The following example configures a tunnel server for remote AAA, configures a dial-in VPDN deployment, and enables the sending of tunnel and tunnel-link accounting records to the RADIUS server:

```
aaa new-model
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnelpass
username user1@cisco.com password 0 lab
username user2@cisco.com password 0 lab
!
spe 1/0 1/7
 firmware location system:/ucode/mica_port_firmware
!
spe 2/0 2/9
 firmware location system:/ucode/mica_port_firmware
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 10.24.80.28 10.47.0.0
ip host myhost 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
accept-dialin
 protocol l2tp
 virtual-template 1
 terminate-from hostname ISP_NAS
 local name ENT_TS
!
isdn switch-type primary-5ess
!
fax interface-type modem
mta receive maximum-recipients 0
!
interface Loopback0
```

```
 ip address 10.0.0.101 255.255.255.0
!
interface Loopback1
 ip address 10.0.0.201 255.255.255.0
!
interface Ethernet0
 ip address 10.1.26.71 255.255.255.0
 no ip mroute-cache
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool vpdn-pool1
 ppp authentication chap
!
interface Virtual-Template2
 ip unnumbered Loopback1
 peer default ip address pool vpdn-pool2
 ppp authentication chap
!
interface FastEthernet0
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
speed auto
 no cdp enable
!
ip local pool vpdn-pool1 10.0.0.2 10.0.0.200
ip local pool vpdn-pool2 10.0.0.1 10.0.0.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 10.1.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
dialer-list 1 protocol ip permit
no cdp run
!
radius-server host 172.16.192.80 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
```

Configuring DNS Name Support on the NAS Remote RADIUS AAA Server: Example

The following AV pair instructs the RADIUS server to resolve the DNS name cisco and tunnel calls to the appropriate IP addresses:

```
9,1="vpdn:ip-addresses = cisco"
```

Configuring L2TP Tunnel Server Load Balancing and Failover Using the Cisco Proprietary VSA: Examples

The following example shows a RADIUS profile that will equally balance the load between three tunnel servers:

```
user = cisco.com
profile_id = 29
profile_cycle = 7
radius=Cisco
check_items=
2=cisco

reply_attributes= {
9,1="vpdn:l2tp-tunnel-password=cisco123"
9,1="vpdn:tunnel-type=l2tp"
9,1="vpdn:ip-addresses=172.16.171.11 172.16.171.12 172.16.171.13"
9,1="vpdn:tunnel-id=tunnel"
}
}
}
```

The following example shows a RADIUS profile that will equally balance calls between 172.16.171.11 and 172.16.171.12. If both of those tunnel servers are unavailable, the RADIUS server will tunnel calls to 172.16.171.13.

```
user = cisco.com
profile_id = 29
profile_cycle = 7
radius=Cisco
check_items=
2=cisco

reply_attributes= {
9,1="vpdn:l2tp-tunnel-password=cisco123"
9,1="vpdn:tunnel-type=l2tp"
9,1="vpdn:ip-addresses=172.16.171.11 172.16.171.12/172.16.171.13"
9,1="vpdn:tunnel-id=tunnel"
}
```

Configuring L2TP Tunnel Server Load Balancing and Failover using the RADIUS Tunnel Preference Attribute: Example

The following RADIUS configuration specifies four tunnel server profiles with different priority values specified in the Tunnel-Preference attribute field. The NAS will preferentially initiate L2TP tunnels to the tunnel server with the lowest configured priority value. If two tunnel server profiles have the same priority value configured, they will be considered equal and load balancing will occur between them.

```
net3 Password = "cisco" Service-Type = Outbound
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Server-Endpoint = :0:"10.1.3.1",
        Tunnel-Assignment-Id = :0:"1",
        Tunnel-Preference = :0:1,
        Tunnel-Password = :0:"secret"

        Tunnel-Type = :1:L2TP,
        Tunnel-Medium-Type = :1:IP,
        Tunnel-Server-Endpoint = :1:"10.1.5.1",
        Tunnel-Assignment-Id = :1:"1",
        Tunnel-Preference = :1:1,
        Tunnel-Password = :1:"secret"
```

```
        Tunnel-Type = :2:L2TP,
        Tunnel-Medium-Type = :2:IP,
        Tunnel-Server-Endpoint = :2:"10.1.4.1",
        Tunnel-Assignment-Id = :2:"1",
        Tunnel-Preference = :2:1,
        Tunnel-Password = :2:"secret"

        Tunnel-Type = :3:L2TP,
        Tunnel-Medium-Type = :3:IP,
        Tunnel-Server-Endpoint = :3:"10.1.6.1",
        Tunnel-Assignment-Id = :3:"1",
        Tunnel-Preference = :3:1,
        Tunnel-Password = :3:"secret"
```

Configuring Tunnel Assignments on the NAS RADIUS AAA Server: Example

The following examples configure the RADIUS server to group sessions in a tunnel:

Per-User Configuration

```
user@cisco.com Password = "cisco" Service-Type = Outbound,
       tunnel-type = :1:L2TP,
       tunnel-server-endpoint = :1:"10.14.10.54",
       tunnel-assignment-Id = :1:"router"

client@cisco.com Password = "cisco" Service-Type = Outbound,
       tunnel-type = :1:L2TP,
       tunnel-server-endpoint = :1:"10.14.10.54",
       tunnel-assignment-Id = :1:"router"
```

Domain Configuration

```
eng.cisco.com Password = "cisco" Service-Type = Outbound,
        tunnel-type = :1:L2TP,
        tunnel-server-endpoint = :1:"10.14.10.54",
        tunnel-assignment-Id = :1:"router"

sales.cisco.com Password = "cisco" Service-Type = Outbound,
        tunnel-type = :1:L2TP,
        tunnel-server-endpoint = :1:"10.14.10.54",
        tunnel-assignment-Id = :1:"router"
```

Configuring L2TP Tunnel Connection Speed Labeling: Examples

The following example shows an ARS RADIUS server profile configuration for three users of the service cisco.com. Each user has a different configuration for allowable connection speeds.

```
#    cisco.com/
#        Name = cisco.com
#        Description = Domain
#        Password = <encrypted>
#        AllowNullPassword = FALSE
#        Enabled = TRUE
#        Group~ =
#        BaseProfile~ =
#        AuthenticationScript~ =
#        AuthorizationScript~ =
#        UserDefined1 =
#        Attributes/
```

```
#            cisco-avpair = vpdn:tunnel-id=aaa_lac
#            cisco-avpair = vpdn:tunnel-type=l2tp
#            cisco-avpair = vpdn:ip-addresses=10.1.1.3
#            cisco-avpair = vpdn:l2tp-tunnel-password=lab
#            service-type = outbound
#        CheckItems/

#    Euser1@cisco.com/
#        Name = Euser1@cisco.com
#        Description = PPPoE-Only-Tx-Accept
#        Password = <encrypted>
#        AllowNullPassword = FALSE
#        Enabled = TRUE
#        Group~ =
#        BaseProfile~ =
#        AuthenticationScript~ =
#        AuthorizationScript~ =
#        UserDefined1 = TX:102400000
#        Attributes/
#        CheckItems/
#
#    Euser11@cisco.com/
#        Name = Euser11@cisco.com
#        Description = PPPoE-Range-RX-Accept
#        Password = <encrypted>
#        AllowNullPassword = FALSE
#        Enabled = TRUE
#        Group~ =
#        BaseProfile~ =
#        AuthenticationScript~ =
#        AuthorizationScript~ =
#        UserDefined1 = RX:96000000-200000000
#        Attributes/
#        CheckItems/
#
#    Euser8@cisco.com/
#        Name = Euser8@cisco.com
#        Description = PPPoE-Both-TXRX-Reject
#        Password = <encrypted>
#        AllowNullPassword = FALSE
#        Enabled = TRUE
#        Group~ =
#        BaseProfile~ =
#        AuthenticationScript~ =
#        AuthorizationScript~ =
#        UserDefined1 = TX:5600000:RX:64000000
#        Attributes/
#        CheckItems/
```

The following example configures the .tcl script to be the OutgoingScript of the service that has been created:

```
Name = check-info
Description =
Type = local
IncomingScript~ =
OutgoingScript~ = checkConnect-Info
OutagePolicy~ = RejectAll
OutageScript~ =
UserList = dialin-users
```

Connection speed information is forwarded by the tunnel server to the RADIUS AAA server for authentication by default. The following example disables the forwarding of connection speed information to the RADIUS AAA server:

```
Router(config)# no radius-server attribute 77 include-in-access-req
```

The following example enables the forwarding of connection speed information to the RADIUS AAA server from the tunnel server if it has been previously disabled:

```
Router(config)# radius-server attribute 77 include-in-access-req
```

The following example enables the forwarding of connection speed information to the RADIUS AAA server from a tunnel switch before the session is forwarded to the next hop:

```
Router(config)# vpdn authen-before-forward
```

Configuring Secure Authentication Names: Example

The following is an example of a RADIUS user profile that includes RADIUS tunneling attributes 90 and 91. This entry supports two tunnels, one for L2F and the other for L2TP. The tag entries with :1 support L2F tunnels, and the tag entries with :2 support L2TP tunnels.

```
cisco.com Password = "cisco", Service-Type = Outbound
    Service-Type = Outbound,
    Tunnel-Type = :1:L2F,
    Tunnel-Medium-Type = :1:IP,
    Tunnel-Client-Endpoint = :1:"10.0.0.2",
    Tunnel-Server-Endpoint = :1:"10.0.0.3",
    Tunnel-Client-Auth-Id = :1:"l2f-cli-auth-id",
    Tunnel-Server-Auth-Id = :1:"l2f-svr-auth-id",
    Tunnel-Assignment-Id = :1:"l2f-assignment-id",
    Cisco-Avpair = "vpdn:nas-password=l2f-cli-pass",
    Cisco-Avpair = "vpdn:gw-password=l2f-svr-pass",
    Tunnel-Preference = :1:1,
    Tunnel-Type = :2:L2TP,
    Tunnel-Medium-Type = :2:IP,
    Tunnel-Client-Endpoint = :2:"10.0.0.2",
    Tunnel-Server-Endpoint = :2:"10.0.0.3",
    Tunnel-Client-Auth-Id = :2:"l2tp-cli-auth-id",
    Tunnel-Server-Auth-Id = :2:"l2tp-svr-auth-id",
    Tunnel-Assignment-Id = :2:"l2tp-assignment-id",
    Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
    Tunnel-Preference = :2:2
```

Configuring Shell-Based Authentication of VPDN Users: Examples

The following example configures dial-in lines 1 through 8 on the NAS to support shell-based authentication of VPDN users:

```
line 1 8
!assuming all logins on lines 1-8 is to be authenticated at 172.69.71.85
  login authentication ExceVPDN-Login
  autoselect during-login
  autocommand ppp
  modem InOut
  transport input all
  transport output none
  stopbits 1
  speed 115200
```

The following example configures a NAS for shell-based authentication of VPDN users based on DNIS information:

```
vpdn enable
vpdn search-order dnis
!
aaa new-model
aaa authentication login Exec-VPDN-login group Exec-VPDN-Login-Servers
aaa authentication ppp Exec-VPDN-ppp if-needed group Exec-VPDN-Login-Servers
aaa authorization network default group Exec-VPDN-Login-Servers
aaa authorization network no_author none
!
!The following configuration creates a RADIUS server group named Exec-VPDN-Login Servers.
radius-server host 172.69.69.72 auth-port 1645 acct-port 1646
aaa group server radius Exec-VPDN-Login-Servers
 server 171.69.69.72 auth-port 1645 acct-port 1646
!
!The following configuration maps DNIS 7777 to the RADIUS server group named
!Exec-VPDN-Login Servers. Authentication requests from users at DNIS 7777 will be
!forwarded to the RADIUS server at 10.1.10.1.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group ExecVPDN-Login-Servers
aaa dnis map 7777 authentication login group ExecVPDN-Login-Servers
```

The following example uses the global RADIUS server definition list for PPP authentication on the NAS if authentication is needed:

```
aaa authentication ppp ExecVPDN-ppp if-needed group radius
!PPP config for line 1
int async 1
ip unnumbered e0
encap ppp
async mode interactive
ppp authentication pap ExecVPDN-ppp
```

The following example configures the tunnel server to accept VPDN tunnels without performing PPP authentication:

```
vpdn-group 1
  accept-dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname host1_no_authen
  l2tp tunnel authentication
  l2tp password no_authen_secret
  local name host2_no_authen
!
interface Virtual-Template1
  ip unnumbered Ethernet0/0
  no keepalive
  ppp authorization no_author
!
```

The following example configures the tunnel server to accept VPDN tunnels with PPP authentication enabled:

```
vpdn-group 2
  accept-dialin
  protocol l2tp
  virtual-template 2
  terminate-from hostname authen_on
  l2tp tunnel authentication
  l2tp password no_authen_secret
  local name host2_autne_on
```

```
!
interface Virtual-Template1
  ip unnumbered Ethernet0/0
  no keepalive
  ppp authentication pap
```

Where to Go Next

Depending on the type of VPDN deployment you are configuring, you should perform the tasks in one of the following modules:

- To configure a client-initiated tunneling deployment, proceed to the "Configuring Client-Initiated Dial-In VPDN Tunneling" module.
- To configure a NAS-initiated tunneling deployment, proceed to the "Configuring NAS-Initiated Dial-In VPDN Tunneling" module.
- To configure a dial-out VPDN tunneling deployment, proceed to the "Configuring Additional VPDN Features" module.
- To configure a multihop MMP or multihop tunnel switching VPDN deployment, proceed to the "Configuring Multihop VPDN" module.

Additional References

The following sections provide references related to configuring AAA for VPDNs.

Related Documents

Related Topic	Document Title
VPDN technology overview	"VPDN Technology Overview"
VPDN commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS VPDN Command Reference*, Release 12.4
Information about configuring AAA	"Authentication, Authorization, and Accounting (AAA)" part of the *Cisco IOS Security Configuration Guide*, Release 12.4
Layer 2 Tunnel Protocol	*Layer 2 Tunnel Protocol* feature module
Information about configuring RADIUS and TACACS	"Security Server Protocols" part of the *Cisco IOS Security Configuration Guide*, Release 12.4
Security commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*, Release 12.4
Information about RPMS	"Configuring Resource Pool Management" chapter of the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4
Dial Technologies commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Dial Technologies Command Reference*, Release 12.4

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
• CISCO-VPDN-MGMT-MIB • CISCO-VPDN-MGMT-EXT-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*
RFC 2868	*RADIUS Tunnel Authentication Attributes*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for AAA for VPDNs

Table 5 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or later appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

If you are looking for information on a feature in this technology that is not documented here, see the "VPDN Features Roadmap."

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Table 5 Feature Information for AAA for VPDNs

Feature Name	Software Releases	Feature Configuration Information
L2TP Domain Screening, Rules Based	12.2(31)SB2	This feature allows per-user L2TP tunnel setup by creating customized Policy Manager match rules. The following sections provide information about this feature: • L2TP Domain Screening, Rules Based, page 44 • Configuring L2TP Domain Screening, Rules Based, page 56 The L2TP Domain Screening, Rules Based feature allows per-user L2TP tunnel setup by creating customized Policy Manager match rules by combining the following three features: • Create a temporary memory to hold the value of identifier types received by policy manager, using the **set variable** command in configuration-control-policymap-class mode • Match the contents, stored in temporary memory of identifier types received by policy manager, against a specified *matching-pattern* and perform the substitution defined in *rewrite-pattern*, using the **substitite** command in configuration-control-policymap-class mode • Authenticate a request for an Intelligent Service Gateway (ISG) subscriber session, using the **authenticate** command in control policy-map class configuration mode These three commands work together to allows you to construct rules to customize specific policy behavior to allow an L2TP tunnel setup by creating customized Policy Manager match rules.
L2TP Tunnel Selection Load Balancing with Random Algorithm	12.2(31)SB2	This feature allows the NAS to use a new tie-breaking algorithm and is transparent to any user. A random selection is made among all peer tunnel servers carrying the same session load. This improved algorithm results in a more even distribution of sessions across tunnel servers, reducing the occurrence of session bunching.

Table 5 Feature Information for AAA for VPDNs

Feature Name	Software Releases	Feature Configuration Information
L2TP Domain Screening	12.2(28)SB	This feature introduces the ability to modify the domain portion of the username seamlessly when you enter into a Virtual Private Network (VPN) service. The following sections provide information about this feature: • L2TP Domain Screening, page 41 • Configuring L2TP Domain Screening, page 50 The L2TP Domain Screening feature allows per-user L2TP tunnel setup by combining the following two features: • User preauthentication using the **vpdn authen-before-forward** command • Modifying the domain portion of the username using the **vpn service** command to bind an incoming session to a certain L2TP tunnel These two commands work together to make sure that the appropriate domain has been screened before access is allowed to an L2TP tunnel for the user session.
L2TP Tunnel Connection Speed Labeling	12.3(4)T	This feature introduces the ability to accept or deny an L2TP session based on the allowed connection speed that is configured on the Cisco ARS RADIUS server for that user. The RADIUS server can authorize users based on their SLA. The following sections provide information about this feature: • VPDN-Specific Remote RADIUS AAA Server Configurations, page 47 • Configuring L2TP Tunnel Connection Speed Labeling on the Remote ARS RADIUS AAA Server and the Tunnel Server, page 98 No commands were introduced or modified by this feature.
RADIUS Attribute 82: Tunnel Assignment ID	12.2(4)T	This feature allows the L2TP NAS to group users from different per-user or domain RADIUS profiles into the same active tunnel if the tunnel endpoints, tunnel type, and Tunnel-Assignment-ID are identical. The following sections provide information about this feature: • VPDN-Specific Remote RADIUS AAA Server Configurations, page 47 • Configuring Tunnel Assignments on the NAS Remote RADIUS AAA Server, page 96 No commands were introduced or modified by this feature.

Table 5 Feature Information for AAA for VPDNs

Feature Name	Software Releases	Feature Configuration Information
RADIUS Tunnel Attribute Extensions	12.2(13)T	This feature introduces RADIUS attribute 90 and RADIUS attribute 91. Both attributes help support the provision of compulsory tunneling in VPDNs by allowing the user to specify authentication names for the NAS and the RADIUS server. The following sections provide information about this feature: • VPDN-Specific Remote RADIUS AAA Server Configurations, page 47 • Configuring Secure Tunnel Authentication Names on the NAS Remote RADIUS AAA Server, page 102 No commands were introduced or modified by this feature.
RADIUS Tunnel Preference for Load Balancing and Fail-Over	12.2(4)T 12.2(11)T	This feature provides industry-standard load balancing and failover functionality for multi-vendor networks. Support for Cisco access server platforms was introduced in Cisco IOS Release 12.2(11)T. The following sections provide information about this feature: • Configuring L2TP Tunnel Server Load Balancing and Failover on the NAS Remote RADIUS AAA Server, page 93 • Configuring L2TP Tunnel Server Load Balancing and Failover using the RADIUS Tunnel Preference Attribute: Example, page 118
RFC-2867 RADIUS Tunnel Accounting	12.3(4)T	This feature introduces six new RADIUS accounting types that are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40), which indicates whether an accounting request marks the beginning of user service (start) or the end (stop). The following sections provide information about this feature: • RADIUS Tunnel Accounting for L2TP VPDNs, page 46 • Configuring RADIUS Tunnel Accounting for L2TP VPDNs, page 88 The following commands were introduced or modified by this feature: **aaa accounting**, **vpdn session accounting network**, **vpdn tunnel accounting network**.

Table 5 Feature Information for AAA for VPDNs

Feature Name	Software Releases	Feature Configuration Information
Shell-Based Authentication of VPDN Users	12.2(2)T	This feature provides terminal services for VPDN users to support rollout of wholesale dial networks. The following sections provide information about this feature: • Shell-Based Authentication of VPDN Users, page 47 • Configuring the NAS for Shell-Based Authentication of VPDN Users, page 103 The following command was modified by this feature: **aaa dnis map authentication group**.
Tunnel Authentication via RADIUS on Tunnel Terminator	12.3(4)T	This feature allows the L2TP tunnel server to perform remote authentication and authorization with RADIUS on incoming L2TP NAS dial-in connection requests. This feature also allows the L2TP NAS to perform remote authentication and authorization with RADIUS on incoming L2TP tunnel server dial-out connection requests. The following sections provide information about this feature: • VPDN-Specific Remote RADIUS AAA Server Configurations, page 47 • Configuring the Tunnel Terminator for Remote RADIUS AAA for L2TP Tunnels, page 66 • Verifying and Troubleshooting Remote AAA Configurations, page 68 The following commands were introduced by this feature: **vpdn tunnel authorization network**, **vpdn tunnel authorization password**, **vpdn tunnel authorization virtual-template**.