Configuring AAA for VPDNs

This module describes how to configure authentication, authorization, and accounting (AAA) for virtual private dialup networks (VPDNs).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring AAA for VPDNs

- Before configuring AAA for VPDNs, you should understand the concepts in the *VPDN Technology Overview* 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) module and Security Server Protocols module.
- If you plan to configure Layer 2 Tunneling Protocol (L2TP) Forwarding of Point-to-Point Protocol over Ethernet (PPPoE) Tagging Information, it is recommended that you be familiar with RFC 2516 and DSL Forum TR-101 before configuring this feature.

Information About AAA for VPDNs

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.

These 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 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 can 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.

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 the software to customize tunnel attributes for individual users that use a common domain name or DNIS.

Without VPDN per-user configuration, the software sends only the domain name or DNIS to determine VPDN tunnel attribute information. Then, if no VPDN tunnel attributes are returned, the 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 might be different from the format of the full username. For example, the remote AAA server might 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.

The NAS can be configured to perform in these ways:

- 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.
- Use a different character or set of characters as the suffix delimiter.
- 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 optional for L2TP tunnels.

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

VPDN tunnel authentication can be performed in these 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, see the "Additional References section."

RADIUS Tunnel Accounting for L2TP VPDNs

RADIUS tunnel accounting for VPDNs is supported by RFC 2867, which introduces six new RADIUS accounting types. 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).

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 next.

Tunnel-Type Accounting Records

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

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

VPDN-Specific Remote RADIUS AAA Server Configurations

The RADIUS attributes are specific to VPDN configurations. For detailed information on configuring remote RADIUS or TACACS+ servers, see the Additional References section.

VPDN-specific RADIUS attributes provide this functionality:

- 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.
- 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.

L2TP Forwarding of PPPoE Tagging Information

The L2TP Forwarding of PPPoE Tag Information feature allows you to transfer DSL line information from the L2TP access concentrator (LAC) to the L2TP network server (LNS). For example, the LAC transports the actual-rate-up and the actual-rate-down PPPoE tag information to the LNS, which learns about the actual PPPoE transfer speeds that are negotiated by the customer premise equipment (CPE) and the digital subscriber line access multiplexer (DSLAM). The DSLAM inserts the PPPoE tag values for the rate up and the rate down and signals this information during PPPoE establishment with the LAC, which in turn, sends this information to the LNS.

By using the L2TP Forwarding of PPPoE Tag Information feature, you can also override the nas-port-id or calling-station-id VSAs, or both, on the LNS with the Circuit-ID and Remote-ID VSA respectively.

When you configure the **dsl-line-info-forwarding** command in VPDN group or VPDN-template configuration mode, and when the LNS receives one of the specified AV pairs, the LNS sends a matching VSA to the RADIUS server as a AAA request. The associated AAA attributes are:

- AAA_CIRCUIT_ID (RADIUS attribute 87)
- AAA_REMOTE_ID (RADIUS attribute 31)
- DSL Sync Rate VSAs

Enter the **radius-server attribute 87 circuit-id** command to override the nas-port-id with the CIRCUIT_ID VSA. Enter the **radius-server attribute 31 remote-id** command to override the calling-station-id with the REMOTE_ID VSA.

In accordance with DSL Forum 2004-71, the DSL uses the Vendor Specific tag for line identification. The first 2 octets (TAG_TYPE) are PPPOE_TAG_VENDSPEC (0x0105). The next 2 octets (TAG_LENGTH) contain the total length including Sub-options, Sub-option-lengths, and Tag-values. The first four octets of the TAG_VALUE contain the vendor ID. The next octet contains sub-option for Agent Remote ID (0x02). Following octet contains total length of Sub-option-tag in bytes.

The maximum length for the Remote-ID tag is 63 bytes. The Remote-ID tag contains an operator administered string that uniquely identifies the subscriber on the associated DSL line. The Remote-ID tag can be a phone number, an email address, a billing account number, or any other string that can be used by Service Providers as a tracking mechanism.

If the discovery frame has the sub-option 0x01, it indicates the presence of the Circuit-ID tag. A single frame supports Circuit-ID, Remote-ID, or both. If Circuit-ID is present in the same frame, it sends to the RADIUS server through the Nas-Port-ID attribute.

The following example shows an access and accounting request sent to the RADIUS server with remote-ID tag and DSL-Sync-Rate tags:

```
01:24:52: RADIUS/ENCODE: Best Local IP-Address 10.0.73.20 for Radius-Server 128.107.164.254
01:24:52: RADIUS(00000011): Send Access-Request to 192.107.164.254:1645 id 1645/3, len 391
01:24:52: RADIUS:  authenticator 3B 49 F5 7D 8A 6F A4 D7 - 57 99 E6 60 A9 D0 C7 B9
01:24:52: RADIUS:  Vendor, Cisco       [26]  41
01:24:52: RADIUS:   Cisco AVpair       [1]   35  "client-mac-address=0090.bf06.c81c"
01:24:52: RADIUS:  Vendor, Cisco       [26]  39
01:24:52: RADIUS:   Cisco AVpair       [1]   33  "actual-data-rate-upstream=20480"
01:24:52: RADIUS:  Vendor, Cisco       [26]  39
01:24:52: RADIUS:   Cisco AVpair       [1]   33  "actual-data-rate-downstream=512"
01:24:52: RADIUS:  Vendor, Cisco       [26]  39
01:24:52: RADIUS:   Cisco AVpair       [1]   33  "minimum-data-rate-upstream=1024"
01:24:52: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
01:24:52: RADIUS:  User-Name           [1]   16  "pshroff-client"
01:24:52: RADIUS:  CHAP-Password       [3]   19  *
01:24:52: RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
01:24:52: RADIUS:  Vendor, Cisco       [26]  46
01:24:52: RADIUS:   Cisco AVpair       [1]   40  "circuit-id-tag=Ethernet1/0.1:abababababa"
01:24:52: RADIUS:  Vendor, Cisco       [26]  36
01:24:52: RADIUS:   Cisco AVpair       [1]   30  "remote-id-tag=0090.bf06.c81c"
01:24:52: RADIUS:  NAS-Port            [5]   6   268435486
01:24:52: RADIUS:  NAS-Port-Id         [87]  25  "Ethernet1/0.1:abababababa"
01:24:52: RADIUS:  Vendor, Cisco       [26]  41
01:24:52: RADIUS:   Cisco AVpair       [1]   35  "client-mac-address=0090.bf06.c81c"
01:24:52: RADIUS:  Service-Type        [6]   6   Framed                    [2]
01:24:52: RADIUS:  NAS-IP-Address      [4]   6   10.0.73.20
01:24:55: RADIUS(00000011): Send Accounting-Request to 192.107.164.254:1646 id 1646/4, len
 495
01:24:55: RADIUS:  authenticator 22 6F B2 F3 88 B1 03 91 - 4A 70 53 BD 44 A6 A6 0F
01:24:55: RADIUS:  Acct-Session-Id     [44]  19  "1/0/0/30_00000008"
01:24:55: RADIUS:  Vendor, Cisco       [26]  39
01:24:55: RADIUS:   Cisco AVpair       [1]   33  "actual-data-rate-upstream=20480"
01:24:55: RADIUS:  Vendor, Cisco       [26]  39
01:24:55: RADIUS:   Cisco AVpair       [1]   33  "actual-data-rate-downstream=512"
01:24:55: RADIUS:  Vendor, Cisco       [26]  39
01:24:55: RADIUS:   Cisco AVpair       [1]   33  "minimum-data-rate-upstream=1024"
01:24:55: RADIUS:  Vendor, Cisco       [26]  49
01:24:55: RADIUS:   Cisco AVpair       [1]   43  "minimum-data-rate-downstream-low-power=32"
01:24:55: RADIUS:  Vendor, Cisco       [26]  46
01:24:55: RADIUS:   Cisco AVpair       [1]   40  "maximum-interleaving-delay-upstream=64"
01:24:55: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
01:24:55: RADIUS:  User-Name           [1]   16  "pshroff-client"
01:24:55: RADIUS:  Vendor, Cisco       [26]  32
01:24:55: RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
01:24:55: RADIUS:  Acct-Authentic      [45]  6   RADIUS                    [1]
01:24:55: RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
01:24:55: RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
01:24:55: RADIUS:  Vendor, Cisco       [26]  46
01:24:55: RADIUS:   Cisco AVpair       [1]   40  "circuit-id-tag=Ethernet1/0.1:abababababa"
01:24:55: RADIUS:  Vendor, Cisco       [26]  36
01:24:55: RADIUS:   Cisco AVpair       [1]   30  "remote-id-tag=0090.bf06.c81c"
01:24:55: RADIUS:  NAS-Port            [5]   6   268435486
01:24:55: RADIUS:  NAS-Port-Id         [87]  25  "Ethernet1/0.1:abababababa"
01:24:55: RADIUS:  Vendor, Cisco       [26]  41
01:24:55: RADIUS:   Cisco AVpair       [1]   35  "client-mac-address=0090.bf06.c81c"
01:24:55: RADIUS:  Service-Type        [6]   6   Framed                    [2]
01:24:55: RADIUS:  NAS-IP-Address      [4]   6   10.0.73.20
01:24:55: RADIUS:  Acct-Delay-Time     [41]  6   0
01:24:57: RADIUS: Received from id 1646/4 192.107.164.254:1646, Accounting-response, len
20
```

The LAC sends the indicated AV pairs, containing the DSL line information to the LNS, which sends them through AAA to the RADIUS server. The RADIUS server uses the DSL line identification when processing AAA requests.

If you plan to configure L2TP Forwarding of PPPoE Tagging Information, it is recommended that you be familiar with RFC 2516 and DSL Forum TR-101 before configuring this feature.

DSL Sync-Rate VSAs

The DSL uses PPPoE Vendor Specific tags for Sync-Rate tag information. DSL Sync-Rates are encoded as 32-bit binary values, describing the rate in kbps. The tag length is 4 bytes. The table below shows the mandatory DSL Sync-Rate tags and their associated RADIUS VSA.

Table 1: Required DSL Sync-Rate Tags

DSL Line Information	RADIUS VSA	Description
DSL Line Actual-Data-Rate-Upstream AVP	AAA_AT_ACTUAL_RATE_UP	Actual data rate upstream in kbps.
DSL Line Actual-Data-Rate-Downstream AVP	AAA_AT_ACTUAL_RATE_DOWN	Actual data rate downstream in kbps.
DSL Line Minimum-Data-Rate-Upstream AVP	AAA_AT_MIN_RATE_UP	Minimum data rate upstream in kbps.
DSL Line Minimum-Data-Rate-Downstream AVP	AAA_AT_MIN_RATE_DOWN	Minimum data rate downstream in kbps.

PADI/PADR frames might contain an optional DSL Sync-Rate tag. The table below shows DSL line information and their associated RADIUS VSA for the optional DSL Sync-Rate tags.

Table 2: Optional DSL Sync-Rate Tags

DSL Line Information	RADIUS VSA	Description
DSL Line Attainable-Data-Rate-Upstream AVP	AAA_AT_ATTAINABLE_RATE_UP	Attainable data rate upstream in kbps.
DSL Line Attainable-Data-Rate-Downstream AVP	AAA_AT_ATTAINABLE_RATE_DOWN	Attainable data rate downstream in kbps.
DSL Line Maximum-Data-Rate-Upstream AVP	AAA_AT_MAX_RATE_UP	Maximum data rate upstream in kbps.
DSL Line Maximum-Data-Rate-Downstream AVP	AAA_AT_MAX_RATE_DOWN	Maximum data rate downstream in kbps.
DSL Line Minimum-Data-Rate-Upstream -Low-Power AVP	AAA_AT_MIN_RATE_UP_LOW_POWER	Minimum data rate upstream in low power state in kbps.
DSL Line Minimum-Data-Rate-Downstream -Low-Power AVP	AAA_AT_MIN_RATE_DOWN_LOW_POWER	Minimum data rate downstream in low power state in kbps.

DSL Line Information	RADIUS VSA	Description
DSL Line Maximum-Interleaving-Delay-UpStream AVP	AAA_AT_MAX_INTER_DELAY_UP	Maximum interleaving delay upstream in ms.
DSL Line Maximum-Interleaving-Delay-DownStream AVP	AAA_AT_MAX_INTER_DELAY_DOWN	Maximum interleaving delay downstream in ms.
DSL Line Actual-Interleaving-Delay-Upstream AVP	AAA_AT_ACTUAL_INTER_DELAY_UP	Actual interleaving delay upstream in kbps.
DSL Line Actual-Interleaving-Delay-Downstream AVP	AAA_AT_ACTUAL_INTER_DELAY_DOWN	Actual interleaving delay downstream in kbps.

LNS Address Checking

Benefits of LNS Address Checking

The LNS Address Checking feature allows a LAC to check the IP address of the LNS sending traffic to it during the setup of an L2TP tunnel, thus providing a check for uplink and downlink traffic arriving from different interfaces.

The benefit of the LNS Address Checking feature is avoiding the loss of revenue from users sending back traffic through an alternate network.

LNS Address Checking Using a RADIUS Server

Use the Cisco attribute-value pair (AVP), downloaded from a RADIUS server during authentication, to enable IP address checking at the LAC.

The Cisco AVP is:

l2tp-security-ip-address-check=yes

The following RADIUS profile example shows the LNS address checking enabled:

```
example.com Password="example"
Service-Type=Outbound
Cisco-Avpair="vpdn:tunnel-id=tunnel"
Cisco-Avpair="vpdn:tunnel-type=l2tp"
Cisco-Avpair=":ip-address=10.10.10.1"
Cisco-Avpair="vpdn:l2tp-tunnel-password=example"
Cisco-Avpair="vpdn:l2tp-security-ip-address-check=yes"
```

Debugging Dropped Control Packets

Use the LNS Address Checking feature to help troubleshoot dropped control packets. If you configure the **debug vpdn 12x-error** command, informational messages display for each control packet that is dropped in the following format:

```
Tnl <tunnel-ID>
 L2TP: Drop <L2TP-packet-name>
 from y.y.y.y (attempted) x.x.x.x
```

Modified LNS Dead-Cache Handling

The Modified LNS Dead-Cache Handling feature allows you to display and clear (restart) any Layer 2 Tunnel Protocol (L2TP) network server (LNS) entry in a dead-cache (DOWN) state. You can use this feature to generate a Simple Network Management Protocol (SNMP) or system message log (syslog) event when an LNS enters or exits a dead-cache state. Once an LNS exits the dead-cache state, the LNS is able to establish new sessions.

Prior to Cisco IOS XE Release 2.4, networks could not identify the status of a Load Sharing Group (LSG) on a LAC. As a result, it was not possible to know if an LNS is not responding (dead-cache state). An LNS in a dead-cache state causes an LSG to reject a call from an LAC.

Networks also have no method of logging, either though a syslog or SNMP event, when an LNS enters, or is cleared from a dead-cache state.

The Modified LNS Dead-Cache Handling feature allows you to view (identify) and clear (restart) one or more LNS entries in a dead-cache (DOWN) state, and generate either a syslog or SNMP event when an LNS exits or enters a dead-cache state. Once an LNS clears a dead-cache state, the LNS is active and available for new call-session establishments.

How to Configure AAA for VPDNs

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.

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.

Configuring the VPDN Tunnel Authorization Search Order

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

Before You Begin

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

Note Tunnel authorization searches based on the multihop hostname are supported only for multihop tunnel switching deployments.

SUMMARY STEPS

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

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**] | **domain** [**dnis**] [**multihop-hostname**] | **multihop-hostname** [**dnis**] [**domain**]} **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 can 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.

Configuring per-User VPDN on the NAS

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 these tasks on the NAS to configure per-user VPDN:

Prerequisites

The NAS remote RADIUS server must be configured for AAA. See the "Additional References" section.

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 dial-in tunnels.

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 l2tp**
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`	Configures a NAS to request the establishment of an L2TP tunnel to a tunnel server, creates a request-dialin VPDN subgroup, and enters VPDN request dial-in subgroup configuration mode.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-req-in)# protocol l2tp`	Specifies the Layer 2 tunneling protocol that the VPDN group will use.
Step 6	**exit** **Example:** `Router(config-vpdn-req-in)# exit`	Exits to VPDN group configuration mode.

	Command or Action	Purpose
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 tunnels belonging to a VPDN group.

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.

Before You Begin

- You must perform the task in the Enabling VPDN on the NAS and the Tunnel Server, on page 9.

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** | **vpdn-tunnel-client**} | **nas-port** {**physical-channel-id** | **vpdn-nas**}}

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 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.
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** | **vpdn-tunnel-client**} | **nas-port** {**physical-channel-id** | **vpdn-nas**}} **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.

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, see the "Additional References" section.

Remote AAA authentication can be configured on the NAS or the tunnel server in these 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 these tasks to configure remote AAA for VPDNs:

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.

Before You Begin

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

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

Step 3	Do one of the following:
	• **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]
	• **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`
	Example:
	`Router(config)# tacacs-server host 10.2.2.2`
		Specifies a RADIUS server host.
		or
		Specifies a TACACS+ host.

Step 4	Do one of the following:
	• **aaa group server radius** *group-name*
	• **aaa group server tacacs+** *group-name*
	Example:
	`Router(config)# aaa group server radius group1`
	Example:
	`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	Do one of the following: • **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] • **server** *ip-address*	(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.

	Command or Action	Purpose

	Example:
	`Router(config-sg-radius)# server 10.1.1.1 auth-port 1000 acct-port 1646`
	Example:
	`Router(config-sg-radius)# server 10.2.2.2`
		Note Perform this step multiple times to configure multiple RADIUS or TACACS+ servers as part of the server group.

What to Do Next

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

Configuring the Tunnel Terminator for Remote RADIUS AAA for L2TP Tunnels

You can 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.

Before You Begin

- The remote RADIUS AAA server must be configured. For more information on configuring remote RADIUS AAA servers, see the "Additional References" section.
- 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*}]
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.
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*]	Configures the IP address of the RADIUS server for the group server.

	Command or Action	Purpose
	Example: `Router(config-sg-radius)# server 10.1.1.1 auth-port 1000 acct-port 1646`	**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 must perform the task in the “Configuring the Multihop Tunnel Switch to Initiate Outgoing VPDN Tunnels” section.

Verifying and Troubleshooting Remote AAA Configurations

Verifying 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:

Example:

```
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.

Example:

```
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 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:

Example:

```
Router> enable
```

Step 2 **debug radius**
Enter this command on the tunnel server to display RADIUS debugging messages.

Example:

```
Router# debug radius
```

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.

Example:

```
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.

Before You Begin

Enable these 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 the debug output.

DETAILED STEPS

Step 1 **enable**
Enter this command to enable privileged EXEC mode. Enter your password if prompted:

Example:

```
Router> enable
```

Step 2 **show debugging**
Enter this command to display information about the types of debugging that are enabled for your router.

Example:

```
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 the 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:

Example:

```
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.

Before You Begin

Enable these 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 the debug output.

DETAILED STEPS

Step 1 **enable**
Enter this command to enable privileged EXEC mode. Enter your password if prompted:

Example:

```
Router> enable
```

Step 2 **show debugging**
Enter this command to display information about the types of debugging that are enabled for your router.

Example:

```
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 the 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:

Example:

```
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:

Example:

```
Router> enable
```

Step 2 **debug ppp negotiation**

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

Example:

```
Router# debug ppp negotiation
```

Step 3 **debug ppp authentication**

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

Example:

```
Router# debug ppp authentication
```

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.

Example:

```
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.

Example:

```
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 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 these tasks to enable directed request authorization of VPDN users.

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.

Before You Begin

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip host** {*name* | **t** *modem-telephone-number*} [*tcp-port-number*] *address1* [*address2...address8*]
4. Do one of the following:
   - **radius-server directed-request** [**restricted**]
   - **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 example.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, on page 15.
Step 4	Do one of the following: • **radius-server directed-request** [**restricted**] • **tacacs-server directed-request** [**restricted**] [**no-truncate**] **Example:** `Router(config)# radius-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.

	Command or Action	Purpose
	Example: `Router(config)# tacacs-server directed-request`	
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.

Before You Begin

You must perform the task in the "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. Do one of the following:
   - **radius-server directed-request** [**restricted**]
   - **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.

	Command or Action	Purpose
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 example.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, on page 15.

Step 4	Do one of the following:
	• **radius-server directed-request** [**restricted**]
	• **tacacs-server directed-request** [**restricted**] [**no-truncate**]
	
	Example:
	`Router(config)# radius-server directed-request`
	
	Example:
	`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

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.

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

Before You Begin

- AAA must be enabled on the NAS. See the "Configuring AAA on the NAS and the Tunnel Server" section.
- You must understand the usage guidelines for the **radius-server domain-stripping** command as described in the VPDN command reference.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **radius-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*]
   - **tacacs-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*]
4. Do one of the following:
   - **radius-server domain-stripping strip-suffix** *suffix* [**vrf** *vrf-name*]
   - **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.
Step 3	Do one of the following: • **radius-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*]	(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.

	Command or Action	Purpose

	• **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 @/`
	
	Example:
	`Router(config)# tacacs-server domain-stripping prefix-delimiter %\$ vrf myvrf`
		• **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.

Step 4	Do one of the following: • **radius-server domain-stripping strip-suffix** *suffix* [**vrf** *vrf-name*] • **tacacs-server domain-stripping strip-suffix** *suffix* [**vrf** *vrf-name*] **Example:** `Router(config)# radius-server`	(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 .

	Command or Action	Purpose

	`domain-stripping strip-suffix cisco.com`
	
	Example:
	
	`Router(config)# tacacs-server domain-stripping strip-suffix cisco.net vrf myvrf`
		• **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 can configure a single ruleset to strip multiple specific suffixes by performing this step multiple times.

What to Do Next

You must perform the process 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 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 VPDN deployments, tunnel authentication requires that a single shared secret be configured on both the NAS and the tunnel server. 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 these 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 these 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 can be configured by using the hostname or the local name as described in the process documented in this section.

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.

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

Prerequisites

AAA must be enabled. See 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*	Establishes a username-based authentication system.

	Command or Action	Purpose
	Example: `Router(config)# username nas4 password mysecret`	• 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.

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.

	Command or Action	Purpose
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.

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.
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.

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.

SUMMARY 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.

Configuring RADIUS Tunnel Accounting for L2TP VPDNs

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).

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

Before You Begin

- You must perform the tasks in the Configuring AAA on the NAS and the Tunnel Server, on page 14.
- You must configure the router to use a remote RADIUS AAA server as described in the Configuring Remote AAA for VPDNs, on page 15.
- You must perform the tasks in the "Configuring VPDN Tunnel Authentication" section.

Note 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.
Step 3	**aaa accounting network default**	*list-name*} {**start-stop**	**stop-only**	**wait-start**	**none group** *groupname*	Enables network accounting. • **default** --If the default network accounting method-list is configured and no additional accounting configurations are enabled on the

	Command or Action	Purpose
	Example: `Router(config)# aaa accounting network list1 start-stop group radius`	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.

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

For L2TP tunnels, you can 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.

Before You Begin

- The RADIUS server must be configured for AAA. For more information on configuring remote RADIUS AAA servers, see the "Additional References" section.
- The service type in the RADIUS user profile for the tunnel initiator should always be set to "Outbound."

Note 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, on page 18.

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.

Before You Begin

The RADIUS server must be configured for AAA.

SUMMARY STEPS

1. Do one of the following:
   - *user* **@** *domain.com* **Password =** **"** *secret* **"** **Service-Type = Outbound**
   - *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	Do one of the following:
	• *user* **@** *domain.com* **Password =** **"** *secret* **"** **Service-Type = Outbound**
	• *user.domain.com* **Password =** **"** *secret* **"** **Service-Type = Outbound**
	Example:
	`user@cisco.com Password = "cisco" Service-Type = Outbound`
	Example:
	`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.

	Command or Action	Purpose
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.

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.

Before You Begin

- The RADIUS server must be configured for AAA.
- The NAS must be able 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. Do one of the following:
   - *user* **@** *example.com* **Password = "** *secret* **" Service-Type = Outbound**
   - *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	Do one of the following:
	• *user* **@** *example.com* **Password = "** *secret* **" Service-Type = Outbound**
	• *user.example.com* **Password = "** *secret* **" Service-Type = Outbound**
	Example:
	`user@cisco.com Password = "cisco" Service-Type = Outbound`
	Example:
	`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.

Configuring L2TP Forwarding of PPPoE Tagging Information

Configuring L2TP Forwarding of the PPPoE Tagging Information

On the LAC, perform these steps to configure L2TP Forwarding of PPPoE Tagging Information to populate the circuit-id tag in the nas-port-id attribute and the remote-id tag in the calling-station-id attribute on the LNS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **dsl-line-info-forwarding**
5. **exit**

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 pppoe-group`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**dsl-line-info-forwarding** **Example:** `Router(config-vpdn)# dsl-line-info-forwarding`	Enables the processing of the received PPPoE Vendor-Specific tag in the PADR packet, and sends a matching VSA to the AAA server in RADIUS access and accounting requests.
Step 5	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN group configuration mode.

Overriding L2TP Forwarding of PPPoE Tag Information

You can configure the L2TP Forwarding of PPPoE Tagging Information feature to override the following VSA:

Overriding nas-port VSA with circuit-id

To override the population of the circuit-id tag in the nas-port-id attribute on the LNS, perform these steps on the LNS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 87 circuit-id**
4. **exit**

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 87 circuit-id** **Example:** `Router(config)# radius-server attribute 87 circuit-id`	Overrides the NAS-Port-Id attribute with the Circuit-ID attribute in RADIUS access and accounting requests.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Overriding calling-station-id VSA with remote-id

To override the calling-station-id VSA with the remote-id on the LNS, perform these steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 31 remote-id**
4. **exit**

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 31 remote-id** **Example:** `Router(config)# radius-server attribute 31 remote-id`	Overrides the calling-station-id attribute with Remote-ID attribute in RADIUS access and accounting requests.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Removing L2TP Forwarding of PPPoE Tag Information

Outgoing PADO and PADS packets will have the DSLAM-inserted Vendor-Specific Line-Id tag, and DSLAM must strip the Circuit-Id tag from the packets. If the DSLAM cannot strip the tag, the BRAS must remove it before sending out the packets. This task is accomplished through configuration of the **vendor-tag remote-id strip** command under BBA group configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** *group-name*
4. **vendor-tag remote-id strip**

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	**bba-group pppoe** *group-name* **Example:** `Router(config)# bba-group pppoe pppoe-group`	Defines a PPPoE profile and enters BBA group configuration mode.
Step 4	**vendor-tag remote-id strip** **Example:** `Router(config-bba-group)# vendor-tag remote-id strip`	Enables the BRAS to strip off incoming Vendor-Specific Remote-Id tags from outgoing PADO and PADS packets.

Displaying the Session Activity Log

When the **radius-server attribute nas-port format d** global configuration command is added to the PPPoE Circuit-Id Tag Processing feature configuration on the BRAS (see the Examples Configuring the VPDN Tunnel Authorization Search Order, on page 64 for an example), the report from the **debug radius** privileged EXEC command will include information about the incoming access interface, where discovery frames are received, and about the session being established in PPPoE extended NAS-Port format (format d).

SUMMARY STEPS

1. Enable the **debug radius** command to display a report of session activity. In the example shown in this section:

DETAILED STEPS

Enable the **debug radius** command to display a report of session activity. In the example shown in this section:

- The acct_session_id is 79 or 4F in hexadecimal format.
- In the message *Acct-session-id pre-pended with Nas Port = 0/0/0/200*, the interface on which the PPPoE discovery frames arrived is FastEthernet0/0.200. The 0/0/0 is Cisco format for slot/subslot/port.
- The Acct-Session-Id vendor-specific attribute 44 contains the string *0/0/0/200_0000004F*, which is a combination of the ingress interface and the session identifier.

Note Strings of interest in the **debug radius** output log are presented in bold text for purpose of example only.

Example:

```
Router# debug radius
02:10:49: RADIUS(0000003F): Config NAS IP: 0.0.0.0
02:10:49: RADIUS/ENCODE(0000003F): acct_session_id: 79
02:10:49: RADIUS(0000003F): sending
02:10:49: RADIUS/ENCODE: Best Local IP-Address 10.0.58.141 for Radius-Server 172.20.164.143
02:10:49: RADIUS(0000003F): Send Access-Request to 172.20.164.143:1645 id 1645/65, len 98
02:10:49: RADIUS:  authenticator 1C 9E B0 A2 82 51 C1 79 - FE 24 F4 D1 2F 84 F5 79
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                        [1]
02:10:49: RADIUS:  User-Name           [1]   7   "peer1"
02:10:49: RADIUS:  CHAP-Password       [3]   19  *
02:10:49: RADIUS:  NAS-Port-Type       [61]  6 Ethernet                   [15]
02:10:49: RADIUS:  NAS-Port            [5]   6   200
02:10:49: RADIUS:  NAS-Port-Id         [87]  22  "FastEthernet6/0.200:"
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                     [2]
02:10:49: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.141
02:10:49: RADIUS: Received from id 1645/65 172.20.164.143:1645, Access-Accept, len 32 02:10:49:
RADIUS:  authenticator 06 45 84 1B 27 1F A5 C3 - C3 C9 69 6E B9 C0 6F 94
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                     [2]
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                        [1]
02:10:49: RADIUS(0000003F): Received from id 1645/65
02:10:49: [62]PPPoE 65: State LCP_NEGOTIATION    Event PPP_LOCAL
02:10:49: PPPoE 65/SB: Sent vtemplate request on base Vi2
02:10:49: [62]PPPoE 65: State VACCESS_REQUESTED    Event VA_RESP
02:10:49: [62]PPPoE 65: Vi2.1 interface obtained
02:10:49: [62]PPPoE 65: State PTA_BINDING    Event STAT_BIND
02:10:49: [62]PPPoE 65: data path set to Virtual Acess
02:10:49: [62]PPPoE 65: Connected PTA
02:10:49: [62]PPPoE 65: AAA get dynamic attrs
02:10:49: [62]PPPoE 65: AAA get dynamic attrs
02:10:49: RADIUS/ENCODE(0000003F):Orig. component type = PPoE
02:10:49: RADIUS/ENCODE(0000003F): Acct-session-id pre-pended with Nas Port = 0/0/0/200
02:10:49: RADIUS(0000003F): Config NAS IP: 0.0.0.0
02:10:49: RADIUS(0000003F): sending
02:10:49: RADIUS/ENCODE: Best Local IP-Address 10.0.58.141 for Radius-Server 172.20.164.143
02:10:49: RADIUS(0000003F): Send Accounting-Request to 172.20.164.143:1646 id 1 646/42, len 117
02:10:49: RADIUS:  authenticator 57 24 38 1A A3 09 62 42 - 55 2F 41 71 38 E1 CC 24
02:10:49: RADIUS:  Acct-Session-Id     [44]  20  "0/0/0/200_0000004F"
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                        [1]
02:10:49: RADIUS:  User-Name           [1]   7   "peer1"
02:10:49: RADIUS:  Acct-Authentic      [45]  6 RADIUS                     [1]
02:10:49: RADIUS:  Acct-Status-Type    [40]  6 Start                      [1]
02:10:49: RADIUS:  NAS-Port-Type       [61]  6 Ethernet                   [15]
02:10:49: RADIUS:  NAS-Port            [5]   6   200
02:10:49: RADIUS:  NAS-Port-Id         [87]  22  "FastEthernet6/0.200:"
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                     [2]
02:10:49: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.141
02:10:49: RADIUS:  Acct-Delay-Time     [41]  6   0
```

```
02:10:49: RADIUS: Received from id 1646/42 172.20.164.143:1646, Accounting-resp onse, len 20
02:10:49: RADIUS:  authenticator 34 84 7E B2 F4 40 B2 7C - C5 B2 4E 98 78 03 8B C0
```

Configuring L2TP Override Forwarding rx-speed and tx-speed Values Received from PPPoE

By default, L2TP obtains the receive-speed (rx-speed) and transmit-speed (tx-speed) values from PPPoE and sends the values to LNS. To override L2TP forwarding of the rx-speed and tx-speed values received from PPPoE, the rx-speed and the tx-speed values should be configured in the RADIUS server, or by using the **l2tp rx-speed** and **l2tp tx-speed** commands in VPDN group configuration or VPDN template configuration mode. The speed values are configured in kbps.

Configuring rx-speed and tx-speed Values When the RADIUS Server Is Not Used

When the RADIUS server is not used, the rx-speed and the tx-speed values can be configured in VPDN group configuration or VPDN template configuration mode. The rx-speed and tx-speed values configured in VPDN group configuration mode are specific to the tunnel and are sent to all sessions under the tunnel.

Perform this task to configure rx-speed and tx-speed values in VPDN group configuration or VPDN template configuration mode when the RADIUS server is not used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn enable**
4. Do one of the following:
   - **vpdn-group** *name*
   - **vpdn-template** *name*
5. **l2tp rx-speed** *value*
6. **l2tp tx-speed** *value*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
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.

Step 4	Do one of the following:
	• **vpdn-group** *name*
	• **vpdn-template** *name*
	
	Example:
	`Router(config)# vpdn-group 1`
	
	Example:
	`Router(config)# vpdn-template 1`
		Enters VPDN group configuration mode.
		or
		Enters VPDN template configuration mode.

Step 5	**l2tp rx-speed** *value* **Example:** `Router(config-vpdn)# l2tp rx-speed 15000`	Sends the rx-speed value to LNS. • If the rx-speed value is not provided, L2TP receives the rx-speed value from PPPoE. **Note** The command is the same irrespective of whether it is entered from VPDN group configuration or VPDN template configuration mode. These steps show how to enter the command from VPDN group configuration mode.
Step 6	**l2tp tx-speed** *value* **Example:** `Router(config-vpdn)# l2tp tx-speed 15000`	Sends the tx-speed value to LNS. • If the tx-speed value is not provided, L2TP receives the tx-speed value from PPPoE.
Step 7	**end** **Example:** `Router(config-vpdn)# end`	Exits VPDN group configuration mode and returns to privileged EXEC mode.

Configuring rx-speed and tx-speed Values on the RADIUS Server

You can configure the rx-speed and tx-speed values on the RADIUS server by Specifying the rx-speed and tx-speed values on the RADIUS server.

The values configured for rx-speed and tx-speed are session oriented. L2TP stores the rx-speed and tx-speed values for every session by using the **vpdn-authen-before-forward** command configured on LAC.

The steps for configuring the default rx-speed and tx-speed values on the RADIUS server are the same as configuring the rx-speed and tx-speed values when the RADIUS server is not used. For configuring rx-speed and tx-speed values on the RADIUS server, see the Configuring rx-speed and tx-speed Values When the RADIUS Server Is Not Used section.

Configuring rx-speed and tx-speed Values from ANCP on the RADIUS Server

ANCP sends the upstream and downstream values to L2TP. The upstream value is the rx-speed value and the downstream value is the tx-speed value.

Perform this task on the RADIUS server to configure rx-speed and tx-speed values from ANCP.

Before You Begin

- The quality of service (QoS) policy must be attached to PPPoE between the client and the LAC.
- The ANCP session and the ANCP neighbor session must be started.
- The average rate traffic shaping value must be configured for the default class by using the **shape average** command in policy-map class configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn enable**
4. Do one of the following:
   - **vpdn-group** *name*
   - **vpdn-template** *name*
5. **l2tp rx-speed ancp** [*value*]
6. **l2tp tx-speed ancp** [*value*]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• 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.

Step 4	Do one of the following:
	• **vpdn-group** *name*
	• **vpdn-template** *name*
	Example:
	`Router(config)# vpdn-group 1`
	Example:
	`Router(config)# vpdn-template 1`
		Enters VPDN group configuration mode.
		or
		Enters VPDN template configuration mode.

Step 5	**l2tp rx-speed ancp** [*value*] **Example:** `Router(config-vpdn)# l2tp rx-speed ancp 15000`	Sends the rx-speed value to LNS if a value is not configured for ANCP. • If the rx-speed value is not configured for ANCP and the rx-speed value is not provided in the command, L2TP sends the rx-speed value configured in VPDN group configuration or VPDN template configuration mode. • If the rx-speed value is not configured in VPDN group configuration or VPDN template configuration mode, L2TP sends the average rate traffic shaping value to LNS. • For ATM interfaces, if the average rate traffic shaping value is not configured, L2TP sends the rx-speed value configured in VC-class configuration mode. If the rx-speed value is not configured in VC-class configuration mode, L2TP sends the rx-speed value obtained from PPPoE. • For Ethernet interfaces, if the average rate traffic shaping value is not configured, L2TP sends the rx-speed value obtained from PPPoE.
Step 6	**l2tp tx-speed ancp** [*value*]	Sends the tx-speed value to LNS if a value is not configured for ANCP.

	Command or Action	Purpose
	Example: `Router(config-vpdn)# l2tp tx-speed ancp 15000`	• If the tx-speed value is not configured for ANCP and the tx-speed is not provided in the command, L2TP sends the tx-speed value configured in VPDN group configuration or VPDN template configuration mode. • If the tx-speed value is not configured in VPDN group configuration or VPDN template configuration mode, L2TP sends the average rate traffic shaping value to LNS. • For ATM interfaces, if the average rate traffic shaping value is not configured, L2TP sends the peak cell rate (PCR) value configured in VC-class configuration mode using the **vbr-nrt** command. If the tx-speed value is not configured in VC-class configuration mode, L2TP sends the tx-speed value obtained from PPPoE. • For Ethernet interfaces, if the average rate traffic shaping value is not configured, L2TP sends the tx-speed value obtained from PPPoE.
Step 7	**end** **Example:** `Router(config-vpdn)# end`	Exits VPDN group configuration mode and returns to privileged EXEC mode.

Configuring rx-speed and tx-speed Values from RAM-min on the RADIUS Server

Perform this task on the RADIUS server to configure the rx-speed and tx-speed values from RAM-min.

Before You Begin

- The quality of service (QoS) policy must be attached to PPPoE between the client and the LAC.
- The average rate traffic shaping value must be configured for the default class using **shape average** command in policy-map class configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn enable**
4. Do one of the following:
   - **vpdn-group** *name*
   - **vpdn-template** *name*
5. **l2tp rx-speed ram-min** [*value*]
6. **l2tp tx-speed ram-min** [*value*]
7. **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	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables VPDN on the router.

Step 4	Do one of the following:
	• **vpdn-group** *name*
	• **vpdn-template** *name*
	Example:
	`Router(config)# vpdn-group 1`
	Example:
	`Router(config)# vpdn-template 1`
		Enters VPDN group configuration mode.
		or
		Enters VPDN template configuration mode.

	Command or Action	Purpose
Step 5	**l2tp rx-speed ram-min** [*value*] **Example:** `Router(config-vpdn)# l2tp rx-speed ram-min 15000`	Sends the rx-speed value to LNS if the average rate traffic shaping value is not configured. • For ATM interfaces, if the average rate traffic shaping value is not configured and the rx-speed value is not provided in the command, L2TP sends the rx-speed value configured in VC-class configuration mode. If the rx-speed value is not configured in VC-class configuration mode, L2TP sends the rx-speed value obtained from PPPoE. • For Ethernet interfaces, if the average rate traffic shaping value is not configured and the rx-speed value is not provided in the command, L2TP sends the rx-speed value obtained from PPPoE.
Step 6	**l2tp tx-speed ram-min** [*value*] **Example:** `Router(config-vpdn)# l2tp tx-speed ram-min 15000`	Sends the tx-speed value to LNS if the average rate traffic shaping value is not configured. • For ATM interfaces, if the average rate traffic shaping value is not configured and the tx-speed value is not provided in the command, L2TP sends the peak cell rate (PCR) value configured using the **vbr-nrt** command in VC-class configuration mode. If the tx-speed value is not configured in VC-class configuration mode, L2TP sends the tx-speed value obtained from PPPoE. • For Ethernet interfaces, if the average rate traffic shaping value is not configured and the tx-speed value is not provided in the command, L2TP sends the tx-speed value obtained from PPPoE.
Step 7	**end** **Example:** `Router(config-vpdn)# end`	Exits VPDN group configuration mode and returns to privileged EXEC mode.

Configuring LNS Address Checking

To allow a LAC to check the IP address of the LNS sending traffic to it during the setup of an L2TP tunnel, thus providing a check for uplink and downlink traffic arriving from different interfaces, follow this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn enable**
4. **vpdn-group** *name*
5. **l2tp security ip address-check**
6. **exit**

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 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 4	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group example`	Creates a VPDN group and enters VPDN group configuration mode.
Step 5	**l2tp security ip address-check** **Example:** `Router(config-vpdn)# l2tp security ip address-check`	Configures the LNS to compare the IP addresses contained in the inbound and outbound message to ensure they are identical. If the IP addresses to not match, the L2TP tunnel is not established.
Step 6	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN group configuration mode.

Configuring Modified LNS Dead-Cache Handling

Identifying an LNS in a Dead-Cache State

With the Modified LNS Dead-Cache Handling feature, you can use the **show vpdn dead-cache** command to display the status of an LNS in an LSG on a LAC and determine if an LNS is not responding (dead-cache state). The **show vpdn dead-cache** command displays the IP address of the nonresponding LNS, and a time entry showing how long the LNS has been down.

This procedure shows how to use the **show vpdn dead-cache** command to display the status of an LNS to determine if it is in a dead-cache state. An LNS in a dead-cache state cannot establish new sessions or calls.

SUMMARY STEPS

1. **enable**
2. **show vpdn dead-cache** {**group** *name* | **all**}
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show vpdn dead-cache** {**group** *name*	**all**} **Example:** `Router# show vpdn dead-cache all`	Displays the status of any LNS in a dead-cache state, including how long the entry has been in the dead-cache state.
Step 3	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

Clearing an LNS in a Dead-Cache State

With the Modified LNS Dead-Cache Handling feature, you can use the **clear vpdn dead-cache** command to clear an LNS entry in the dead-cache based on the IP address of the LNS, clear all LNS dead-cache states in a VPDN group, or clear all dead-cache LNS entries. If you clear an LNS based on its IP address, and the LNS is associated with more than one VPDN group, the LNS is cleared in all the associated VPDN groups.

This procedure shows how to clear an LNS in a dead-cache state. Once an entry clears from the dead-cache state, the entry is available for new session establishments and calls.

Before You Begin

Perform this procedure on the LAC.

SUMMARY STEPS

1. **enable**
2. **clear vpdn dead-cache** {**group** *name* | **ip-address** *ip-address* | **all**}
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear vpdn dead-cache** {**group** *name* | **ip-address** *ip-address* | **all**} **Example:** `Router# clear vpdn dead-cache ip-address 10.10.10.1`	Clears the designated LNS from the dead-cache state.
Step 3	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

Generating an SNMP Event for a Dead-Cache Entry

If you are a manager responsible for a large number of devices, and each device has a large number of objects, it is impractical for you to poll or request information from every object on every device. SNMP trap-directed notification alerts you without solicitation, by sending a message known as a trap of the event. After you receive the event, you can display it and can choose to take an appropriate action based on the event.

To generate an SNMP event when an LNS exits or enters the dead-cache state, follow this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps vpdn dead-cache**
4. **exit**

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	**snmp-server enable traps vpdn dead-cache** **Example:** `Router(config)# snmp-server enable traps vpdn dead-cache`	Enables the generation of an SNMP event whenever an LNS enters or exits the dead-cache state.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Generating a Syslog Event for a Dead-Cache Entry

To view a syslog event when an LNS is added, deleted, or cleared from a dead-cache state, configure the **vpdn logging dead-cache** command. You can use syslog events to help troubleshoot networks.

The table below summarizes the syslog messages generated by using the **vpdn logging dead-cache** command.

Table 3: VPDN Logging Dead-Cache Events

Syslog Message	Description
MM:DD:hh:mm:ss %VPDN-6-VPDN_DEADCACHE_EVENT: LSG dead cache entry <ip-address> added	Added--An entry in the LSG table enters DOWN status, which marks it a dead-cache entry.

Syslog Message	Description
MM:DD:hh:mm:ss %VPDN-6-VPDN_DEADCACHE_EVENT: LSG dead cache entry <ip-address> deleted	Deleted--An entry in the LSG table is removed from DOWN status, which deletes its dead-cache entry from the table.
MM:DD:hh:mm:ss %VPDN-6-VPDN_DEADCACHE_EVENT: LSG dead cache entry <ip-address> cleared	Cleared--An entry in the LSG table is manually cleared.

To generate a syslog event when an LNS enters or exits the dead-cache state, follow this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn logging dead-cache**
4. **exit**

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 logging dead-cache** **Example:** `Router(config)# vpdn logging dead-cache`	Enables the generation of a syslog event when an LNS enters or exits the dead-cache state.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuration Examples for AAA for VPDNs

Examples Configuring the VPDN Tunnel Authorization Search Order

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
```

Examples Configuring per-User VPDN on the NAS

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
```

Examples Configuring AAA on the NAS and the Tunnel Server

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.

Examples Configuring Remote AAA for VPDNs on the L2TP Tunnel Terminator

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"
```

Examples Configuring Directed Request Authorization of VPDN Users

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 example.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 example.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 example.com 10.3.3.3
radius-server directed-request
vpdn authorize directed-request
```

Examples Configuring Domain Name Prefix and Suffix Stripping

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 */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
```

Examples Configuring VPDN Tunnel Authentication

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
```

Example Configuring RADIUS Tunnel Accounting on a NAS

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 GigabitEthernet0/0/0
 ip address 10.1.27.74 255.255.255.0
 no ip mroute-cache
 duplex half
 speed auto
 no cdp enable
!
interface GigabitEthernet0/1/0
 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
```

Example Configuring RADIUS Tunnel Accounting on a Tunnel Server

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
```

Example Configuring Tunnel Assignments on the NAS RADIUS AAA Server

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"
```

Examples Configuring rx-speed and tx-speed Values

The following example shows how to configure average rate traffic shaping value for the default class in policy-map class configuration mode:

```
interface GigabitEthernet3/1/0.30880387
  encapsulation dot1Q 3088 second-dot1q 20
  ancp neighbor name ancp-neighbor id 0016.fa11.0488 client-ID "12.124.234.132/0.0.0.0 eth
 3/4/1.32"
  pppoe enable group test2
  service-policy output speed:ether:22000:1200:06/0
!
policy-map speed:ether:22000:1200:06/0
     class class-default
    shape average 10281000 !10,281 Mbps is so-called Rate Adaptive Mode (RAM) MIN value!
!
```

The following example shows how to configure rx-speed and tx-speed values for an ATM interface when the rx-speed and tx-speed values, including 0, 0, are not configured in the RADIUS server. The average rate traffic shaping value is configured for the Ethernet interface. If the average rate traffic shaping value for the default class in policy-map class configuration mode is not configured, the rx-speed and tx-speed values specified in the **l2tp rx-speed** and **l2tp tx-speed** commands are configured for the ATM interface.

```
Interface ATM 1/0/4.2
vpdn-template 2
l2tp rx-speed ram-min 8000
l2tp tx-speed ram-min 8000
```

The following example shows how to configure rx-speed and tx-speed values for an Ethernet interface when the rx-speed and tx-speed values, including 0, 0, are not configured in the RADIUS server. The rx-speed and tx-speed values configured for ANCP is configured for the Ethernet interface. If the rx-speed and tx-speed

values are not configured for ANCP, the rx-speed and tx-speed values specified in the **l2tp rx-speed** and **l2tp tx-speed** commands are configured for the Ethernet interface.

```
Interface Ethernet 3/0/1.3
vpdn-template 1
l2tp rx-speed ancp 15000
l2tp tx-speed ancp 15000
```

Example Configuring Secure Authentication Names

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
```

Examples Configuring LNS Address Checking

The following shows an example configuration for the client router.

```
hostname Client
!
enable password example
!
no aaa new-model
!
vpdn enable
!
bba-group pppoe 1
 virtual-template 1
!
interface <interface toward LAC>
 pppoe enable group 1
!
interface Virtual-Template 1
 ip unnumbered <interface>
 ppp pap sent-username@example.com
!
end
```

The following shows an example configuration for the LAC.

```
hostname LAC
```

```
!
enable password example
!
no aaa new-model
!
vpdn enable
!
vpdn-group 1
 request-dialin
 protocol l2tp
 domain example.com
 initiate-to ip <lns 1 IP address>
 l2tp tunnel password 0 example
!
bba-group pppoe 1
 virtual-template 1
!
interface Virtual-Template 1
 no ip address
 ppp authentication pap
!
interface <interface>
 pppoe enable group 1
!
end
```

The following shows an example configuration for the LNS 1.

```
hostname LNS1
!
enable password example
!
aaa authentication ppp default local
!
vpdn enable
!
vpdn-group 1
!Default L2TP VPDN group
 accept-dialin
 protocol l2tp
 virtual-template 1
 l2tp tunnel password 0 example
!
vpdn-group 2
 request-dialin
 protocol l2tp
 domain example.com
 initiate-to ip <lns 2 IP address>
 l2tp tunnel password 0 example
!
interface Virtual-Template 1
 ip unnumbered <interface>
 ppp authentication pap
!
end
```

Examples Configuring Modified LNS Dead-Cache Handling

The following show an example configuration from the **show vpdn dead-cache all** command:

```
Router> enable
Router# show vpdn dead-cache all
vpdn-group     ip address     down time
exampleA     192.168.2.2     00:10:23
exampleB     192.168.4.2     00:10:16
exampleB     192.168.4.3     00:10:15
exampleB     192.168.4.4     00:10:12
```

The following shows an example configuration to clear an LNS, based on its IP address, from the dead-cache state:

```
Router# clear vpdn dead-cache ip-address 192.168.4.4
Router#
*Sept. 30 22:58:32 %VPDN-6-VPDN_DEADCACHE_CHANGE: LSG dead cache entry 192.168.4.4 cleared
LAC# show vpdn dead-cache all
vpdn-group     ip address     down time
exampleA     192.168.2.2     00:10:28
exampleB     192.168.4.2     00:10:21
exampleB     192.168.4.3     00:10:20
```

The following shows an example configuration to clear an LNS group from the dead-cache state:

```
Router# clear vpdn dead-cache group exampleB
Router#
*Sept. 30 22:58:32 %VPDN-6-VPDN_DEADCACHE_CHANGE: LSG dead cache entry 192.168.4.2 cleared
*Sept. 30 22:58:32 %VPDN-6-VPDN_DEADCACHE_CHANGE: LSG dead cache entry 192.168.4.3 cleared
Router# show vpdn dead-cache all
vpdn-group     ip address     down time
exampleA     192.168.2.2     00:10:31
```

Where to Go Next

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

- To configure a NAS-initiated tunneling deployment, proceed to the Configuring NAS-Initiated Dial-In VPDN Tunneling module.
- To configure a multihop MMP or multihop tunnel switching VPDN deployment, proceed to the Configuring Multihop VPDN module.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
VPDN technology overview	VPDN Technology Overview module
VPDN commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS VPDN Command Reference*
Information about configuring AAA	Authentication, Authorization, and Accounting (AAA) module
Layer 2 Tunnel Protocol	*Layer 2 Tunnel Protocol*

Related Topic	Document Title
Information about configuring RADIUS and TACACS	Security Server Protocols module
Security commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*
Dial Technologies commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Dial Technologies Command Reference*

Standards

Standard	Title
DSL Forum 2004-72	--

MIBs

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

RFCs

RFC	Title
RFC 2516	*A Method for Transmitting PPP Over Ethernet (PPPoE)*
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*
RFC 2868	*RADIUS Tunnel Authentication Attributes*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for AAA for VPDNs

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for AAA for VPDNs

Feature Name	Releases	Feature Information
Configurable Domain Name Prefix and Suffix Stripping for the RADIUS server	Cisco IOS XE Release 2.1	This feature allows the NAS to be configured to strip prefixes, suffixes, or both from the full username. The reformatted username is then forwarded to the remote AAA server. The following command was introduced or modified by this feature: **radius-server domain-stripping**.
RADIUS Attribute 82: Tunnel Assignment ID	Cisco IOS XE Release 2.1	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. No commands were introduced or modified by this feature.

Feature Name	Releases	Feature Information
RADIUS Tunnel Attribute Extensions	Cisco IOS XE Release 2.1	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. No commands were introduced or modified by this feature.
RFC-2867 RADIUS Tunnel Accounting	Cisco IOS XE Release 2.1	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 commands were introduced or modified by this feature: **aaa accounting**, **vpdn session accounting network**, **vpdn tunnel accounting network**.
Tunnel Authentication via RADIUS on Tunnel Terminator	Cisco IOS XE Release 2.1	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 commands were introduced by this feature: **vpdn tunnel authorization network**, **vpdn tunnel authorization password**, **vpdn tunnel authorization virtual-template**.
L2TP Forwarding of PPPoE Tagging Information	Cisco IOS XE Release 2.4	This feature was introduced on Cisco ASR 1000 Series Routers.

Feature Name	Releases	Feature Information
LNS Address Checking	Cisco IOS XE Release 2.4	This feature allows an LAC, which is receiving data from a LNS, to check the IP address of the LNS prior to establishing an L2TP tunnel. The following command was introduced by this feature: **l2tp security ip address-check**.
Modified LNS Dead-Cache Handling	Cisco IOS XE Release 2.4	This feature displays and clears (restarts) any LNS entry in a dead-cache (DOWN) state. The following commands were introduced by this feature: **clear vpdn dead-cache**, **show vpdn dead-cache**. The following commands were modified by this feature: **snmp-server enable traps**, **vpdn logging**.
Configurable Domain Name Prefix and Suffix Stripping for the TACACS+ server	Cisco IOS XE Release 2.5	This feature allows the NAS to be configured to strip prefixes, suffixes, or both from the full username. The reformatted username is then forwarded to the remote AAA server. The following command was introduced or modified by this feature: **tacacs-server domain-stripping**.
ANCP values configuration support on LNS	Cisco IOS XE Release 3.2S	This feature allows L2TP to send the rx-speed and tx-speed values configured in VPDN group configuration or VPDN template configuration mode, or the rx-speed and the tx-speed values configured on the RADIUS server, to LNS. The following commands were introduced by this feature: **l2tp rx-speed**, **l2tp tx-speed**.