U through Z

virtual-template

To specify which virtual template is used to clone virtual access interfaces (VAI), use the **virtual-template** command in BBA group configuration mode and in VPDN group configuration mode. To remove the virtual template from a virtual private dialup network (VPDN) group, use the **no** form of this command.

virtual-template *template-number*
no virtual-template

Syntax Description

template-number	Number of the virtual template that will be used to clone VAIs. The range is 1 to 1000.

Command Default

No virtual template is enabled.

Command Modes

BBA group configuration mode (config-bba-group)

VPDN group configuration (config-vpdn)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	This command was enhanced to enable PPPoE on ATM to accept dial-in PPP over Ethernet (PPPoE) sessions.
12.2(15)T	This command was enhanced to allow IP per-user attributes to be applied to a Layer 2 Tunneling Protocol (L2TP) dial-out session.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command's default configuration was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4 as described in the "Usage Guidelines" section.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

You must first enable a tunneling protocol on the VPDN group by using the **protocol** (VPDN) command before you can enable the **virtual-template** command. Removing or modifying the **protocol** command removes the **virtual-template** command from the VPDN group.

Each VPDN group can clone only VAIs using one virtual template. If you enter a second **virtual-template** command on a VPDN group, it replaces the first **virtual-template** command.

The table below lists the VPDN group commands under which the **virtual-template** command can be entered. Entering the VPDN group command starts VPDN group configuration mode. The table includes the command-line prompt for the VPDN group configuration mode and the type of service configured.

Table 1: VPDN Subgroups

VPDN Group Command	Command Mode Prompt	Type of Service
accept-dialin	`router(config-vpdn-acc-in)#`	Tunnel server
request-dialout	`router(config-vpdn-req-out)#`	L2TP network server (LNS)

When the **virtual-template** command is entered under a **request-dialout** VPDN subgroup, IP and other per-user attributes can be applied to an L2TP dial-out session from an LNS. Before this command was enhanced, IP per-user configurations from authentication, authorization, and accounting (AAA) servers were not supported; the IP configuration comes from the dialer interface defined on the router.

The enhanced **virtual-template** command works in a way similar to configuring virtual profiles and L2TP dial-in. The L2TP VAI is first cloned from the virtual template, which means that configurations from the virtual template interface is applied to the L2TP VAI. After authentication, the AAA per-user configuration is applied to the VAI. Because AAA per-user attributes are applied only after the user has been authenticated, the LNS must be configured to authenticate the dial-out user (configuration authentication is needed for this command).

With the enhanced **virtual-template** command, all software components can now use the configuration present on the VAI rather than what is present on the dialer interface. For example, IP Control Protocol (IPCP) address negotiation uses the local address of the VAI as the router address while negotiating with the peer.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the **virtual-template snmp** command has a new default configuration. Instead of being enabled by default, **no virtual-template snmp** is the default configuration. This setting enhances scaling and prevents large numbers of entries in the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs.

If you configure the **no virtual-template snmp** command, the router no longer accepts the **snmp trap link-status** command under a virtual-template interface. Instead, the router displays a configuration error message such as the following:

```
Router(config)# interface virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual template interface is already registered in the interfaces MIB.

Examples

The following example enables the LNS to accept an L2TP tunnel from an L2TP access concentrator (LAC) named LAC2. A VAI will be cloned from virtual template 1.

```
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname LAC2
```

The following example enables PPPoE on ATM to accept dial-in PPPoE sessions. A VAI for the PPP session is cloned from virtual template 1.

```
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
```

The following partial example shows how to configure an LNS to support IP per-user configurations from a AAA server:

```
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
.
.
.
 request-dialout
  protocol l2tp
  rotary-group 1
  virtual-template 1
 initiate-to ip 10.0.1.194.2
 local name lns
 l2tp tunnel password 7094F3$!5^3
 source-ip 10.0.194.53
!
```

The previous configuration requires a AAA profile such as the following example to specify the per-user attributes:

```
5300-Router1-out  Password = "cisco"
     Service-Type = Outbound
     cisco-avpair = "outbound:dial-number=5550121"
7200-Router1-1  Password = "cisco"
     Service-Type = Outbound
     cisco-avpair = "ip:route=10.17.17.1 255.255.255.255 Dialer1 100 name 5300-Router1"
5300-Router1 Password = "cisco"
     Service-Type = Framed
     Framed-Protocol = PPP
     cisco-avpair = "lcp:interface-config=ip unnumbered loopback 0"
     cisco-avpair = "ip:outacl#1=deny ip host 10.5.5.5 any log"
     cisco-avpair = "ip:outacl#2=permit ip any any"
     cisco-avpair = "ip:inacl#1=deny ip host 10.5.5.5 any log"
     cisco-avpair = "ip:inacl#2=permit ip any any"
     cisco-avpair = "multilink:min-links=2"
     Framed-Route = "10.5.5.6/32 Ethernet4/0"
     Framed-Route = "10.5.5.5/32 Ethernet4/0"
     Idle-Timeout = 100
```

Related Commands

Command	Description
accept-dialin	Configures an LNS to accept tunneled PPP connections from a LAC and to create an accept-dialin VPDN subgroup.
protocol (VPDN)	Specifies the Layer 2 Tunneling Protocol that the VPDN subgroup will use.
request-dialout	Enables an LNS to request VPDN dial-out calls by using L2TP and to create a request-dialout VPDN subgroup.
show vtemplate	Displays information about all configured virtual templates.

Command	Description
vpdn-group	Defines a local, unique group number identifier.

vpdn aaa attribute

To enable reporting of network access server (NAS) authentication, authorization, and accounting (AAA) attributes related to a virtual private dialup network (VPDN) to the AAA server, use the **vpdn aaa attribute** command in global configuration mode. To disable reporting of AAA attributes related to VPDN, use the **no** form of this command.

vpdn aaa attribute {**nas-ip-address** {**vpdn-nas** | **vpdn-tunnel-client**} | **nas-port** {**physical-channel-id** | **vpdn-nas**}}
no vpdn aaa attribute {**nas-ip-address** {**vpdn-nas** | **vpdn-tunnel-client**} | **nas-port**}

Syntax Description

nas-ip-address vpdn-nas	Enables reporting of the VPDN NAS IP address to the AAA server.
nas-ip-address vpdn-tunnel-client	Enables reporting of the VPDN tunnel client IP address to the AAA server.
nas-port vpdn-nas	Enables reporting of the VPDN NAS port to the AAA server.
nas-port physical-channel-id	Enables reporting of the VPDN NAS port physical channel identifier to the AAA server.

Command Default

AAA attributes are not reported to the AAA server.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3NA	This command was introduced.
11.3(8.1)T	This command was integrated into Cisco IOS Release 11.3(8.1)T.
12.1(5)T	This command was modified to support the PPP extended NAS-Port format.
12.2(13)T	The **physical-channel-id** keyword was added
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	The **vpdn-tunnel-client** keyword was added.
12.2(33)XND	The **vpdn-tunnel-client** keyword was added.
12.2(33)SRE	The **vpdn-tunnel-client** keyword was added.
Cisco IOS XE Release 2.5	The **vpdn-tunnel-client** keyword was added.

Usage Guidelines

This command can be used with RADIUS or TACACS+ and is applicable only on the VPDN tunnel server.

The PPP extended NAS-Port format enables the NAS-Port and NAS-Port-Type attributes to provide port details to a RADIUS server when one of the following protocols is configured:

- PPP over ATM
- PPP over Ethernet (PPPoE) over ATM
- PPPoE over 802.1Q VLANs

Before PPP extended NAS-Port format attributes can be reported to the RADIUS server, the **radius-server attribute nas-port format** command with the **d** keyword must be configured on both the tunnel server and the NAS, and the tunnel server and the NAS must both be Cisco routers.

When you configure the **vpdn aaa attribute nas-ip-address vpdn-nas** command, the L2TP network server (LNS) reports the IP address of the last multihop node for multihop over Layer 2 Forwarding (L2F). For multihop over Layer 2 Tunneling Protocol (L2TP), the IP address of the originating NAS is reported.

When you configure the **vpdn aaa attribute nas-ip-address vpdn-tunnel-client** command, the LNS reports the IP address of the last multihop node in the RADIUS NAS-IP-Address attribute for the L2TP multihop. This eases the migration for customers moving from L2F to L2TP.

Note Reporting of NAS AAA attributes related to a VPDN on a AAA server is not supported for Point-to-Point Tunneling Protocol (PPTP) sessions with multihop deployment.

Examples

The following example configures VPDN on a tunnel server and enables reporting of VPDN AAA attributes to the AAA server:

```
vpdn enable
vpdn-group 1
 accept-dialin
  protocol any
  virtual-template 1
!
 terminate-from hostname nas1
 local name ts1
!
vpdn aaa attribute nas-ip-address vpdn-nas
vpdn aaa attribute nas-port vpdn-nas
vpdn aaa attribute nas-port physical-channel-id
```

The following example configures the tunnel server for VPDN, enables AAA, configures a RADIUS AAA server, and enables reporting of PPP extended NAS-Port format values to the RADIUS server. PPP extended NAS-Port format must also be configured on the NAS for this configuration to be effective.

```
vpdn enable
vpdn-group L2TP-tunnel
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname nas1
 local name ts1
!
aaa new-model
```

```
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
!
radius-server host 172.16.79.76 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key ts123
!
vpdn aaa attribute nas-port vpdn-nas
```

Related Commands

Command	Description
radius-server attribute nas-port format	Selects the NAS-Port format used for RADIUS accounting features.

vpdn aaa override-server

To specify an authentication, authorization, and accounting (AAA) server to be used for virtual private dialup network (VPDN) tunnel authorization other than the default AAA server, use the **vpdn aaa override-server** command in global configuration mode. To return to the default setting, use the **no** form of this command.

vpdn aaa override-server {*aaa-server-ip-addressaaa-server-name*}
no vpdn aaa override-server {*aaa-server-ip-addressaaa-server-name*}

Syntax Description

aaa-server-ip-address	The IP address of the AAA server to be used for tunnel authorization.
aaa-server-name	The name of the AAA server to be used for tunnel authorization.

Command Default

If the AAA server is not specified, the default AAA server configured for network authorization is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN network access server (NAS). Configuring this command restricts tunnel authorization to the specified AAA servers only. This command can be used to specify multiple AAA servers.

For TACACS+ configuration, the **tacacs-server directed-request** command must be configured by using the **restricted** keyword, or authorization will continue with all configured TACACS+ servers.

Examples

The following example enables AAA attributes and specifies the AAA server to be used for VPDN tunnel authorization:

```
aaa new-model
 aaa authorization network default group radius
 vpdn aaa override-server 10.1.1.1
 vpdn enable
 radius-server host 10.1.1.2 auth-port 1645 acct-port 1646
 radius-server key Secret
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
tacacs-server directed-request	Sends only a username to a specified server when a direct request is issued.
vpdn enable	Enables VPDN on the router and directs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.

vpdn aaa untagged

To apply untagged attribute values obtained from the authentication, authorization, and accounting (AAA) RADIUS server to all attribute sets for virtual private dialup network (VPDN) tunnels, use the **vpdn aaa untagged** command in global configuration mode. To disable this function, use the **no** form of this command.

vpdn aaa untagged default
no vpdn aaa untagged default

Syntax Description

default	Sets the untagged attribute value as default.

Command Default

Untagged attribute values are applied to all attribute sets.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(1)T	This command was introduced.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **default** keyword was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Untagged attribute values obtained from the AAA RADIUS server are applied to all attribute sets by default, unless a value for that attribute is already specified in the tagged attribute set. To prevent untagged attribute values from being applied to tagged attribute sets, use the **no** form of this command.

Examples

The following example shows how to disable the application of untagged attribute values to attribute sets:

```
Router# configure terminal
Router(config)# no vpdn aaa untagged default
```

Related Commands

Command	Description
show vpdn	Displays basic information about all active VPDN tunnels.

vpdn authen-before-forward

Note Effective with Cisco Release 12.4(11)T, the support for L2F was removed in Cisco IOS Software.

To configure a network access server (NAS) to request authentication of a complete username before making a forwarding decision for all dial-in Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnels, use the **vpdn authen-before-forward** command in global configuration mode. To disable this configuration, use the **no** form of this command.

vpdn authen-before-forward
no vpdn authen-before-forward

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP or L2F tunnels are forwarded to the tunnel server without first requesting authentication of the complete username.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

To configure the NAS to perform authentication of all dial-in L2TP or L2F sessions before the sessions are forwarded to the tunnel server, configure the **vpdn authen-before-forward** command in global configuration mode.

To configure the NAS to perform authentication of dial-in L2TP or L2F sessions belonging to a specific VPDN group before the sessions are forwarded to the tunnel server, use the **authen-before-forward** command in VPDN group configuration mode.

Enabling the **vpdn authen-before-forward** command instructs the NAS to authenticate the complete username before making a forwarding decision based on the domain portion of the username. A user may be forwarded or terminated locally depending on the information contained in the users RADIUS profile. Users with forwarding information in their RADIUS profile are forwarded based on that information. Users without forwarding information in their RADIUS profile are either forwarded or terminated locally based on the Service-Type in their RADIUS profile. The relationship between forwarding decisions and the information contained in the users RADIUS profile is summarized in the table below.

Table 2: Forwarding Decisions Based on RADIUS Profile Attributes

Forwarding Information Is	Service-Type Is Outbound	Service-Type Is Not Outbound
Present in RADIUS profile	Forward User	Forward User
Absent from RADIUS profile	Check Domain	Terminate Locally

Examples

The following example configures the NAS to request authentication of all dial-in L2TP or L2F sessions before the sessions are forwarded to the tunnel server:

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

Related Commands

Command	Description
authen-before-forward	Configures a NAS to request authentication of a complete username before making a forwarding decision for dial-in L2TP or L2F tunnels belonging to a VPDN group.

vpdn authorize directed-request

To enable virtual private dialup network (VPDN) authorization for directed-request users, use the **vpdn authorize directed-request** command in global configuration mode. To disable VPDN authorization for directed request users, use the **no** form of this command.

vpdn authorize directed-request
no vpdn authorize directed-request

Syntax Description

This command has no keywords or arguments.

Command Default

VPDN authorization for directed-request users is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

When a username includes both a username and a domain portion, such as user@site.com, directed request configuration allows the authorization request to be sent to a specific RADIUS or TACACS+ server based on the domain name portion of the username (site.com). The **vpdn authorize directed-request** command must be enabled to allow VPDN authorization of any directed request user.

Directed request for RADIUS users is enabled by issuing the **radius-server directed-request** command. Directed request for TACACS+ users is enabled by default, and can be disabled by using the **no tacacs-server directed request** command. The **ip host** command must be configured to enable directed requests to RADIUS or TACACS+ servers.

The **vpdn authorize directed-request** command is usually configured on the L2TP network server (LNS). When directed-requests are used on an L2TP access concentrator (LAC) with per-user VPDN configuration, the **authen before-forward** command must be enabled.

Examples

The following example enables VPDN authorization and RADIUS directed requests on an LNS:

```
ip host site.com 10.1.1.1
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server directed-request
vpdn authorize directed-request
```

The following example enables VPDN authorization and TACACS+ directed requests on an LNS:

```
ip host site.com 10.1.1.1
tacacs-server host 10.1.1.1
tacacs-server directed-request
vpdn authorize directed-request
```

The following example enables per-user VPDN and enables VPDN authorization for directed request users on a LAC:

```
vpdn-group 1
 request-dialin
```

```
  protocol l2f
  domain cisco.com
 !
 initiate-to ip 10.1.1.1
 local name local1
 authen before-forward
!
ip host cisco.com 10.1.1.1
vpdn authorize directed-request
!
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server directed-request
```

Related Commands

Command	Description
authen before-forward	Specifies that the VPDN sends the entire structured username to the AAA server the first time the router contacts the AAA server.
ip host	Defines a static hostname-to-address mapping in the host cache.
radius-server directed-request	Allows users logging into a Cisco NAS to select a RADIUS server for authentication.
tacacs-server directed-request	Sends only a username to a specified server when a direct request is issued.

vpdn authorize domain

To enable domain preauthorization on a network access server (NAS), use the **vpdn authorize domain** command in global configuration mode. To disable domain preauthorization, use the **no** form of this command.

vpdn authorize domain
no vpdn authorize domain

Syntax Description

This command has no arguments or keywords.

Command Default

Domain preauthorization is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)DC1	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

A domain preauthorization RADIUS user profile must also be created. See the Examples section and refer to the *Cisco IOS Security Configuration Guide* for information on how to create these profiles.

Examples

Domain Preauthorization Configuration on the LAC Example

The following example shows the configuration necessary for an L2TP access concentrator (LAC) to participate in domain preauthorization:

```
!
aaa new-model
aaa authorization network default local group radius
!
vpdn authorize domain
!
radius-server host 10.9.9.9 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
radius-server key MyKey
radius-server vsa send authentication
!
```

Domain Preauthorization RADIUS User Profile Example

The following example shows a domain preauthorization RADIUS user profile:

```
user = nas-port:10.9.9.9:0/0/0/30.33{
 profile_id = 826
 profile_cycle = 1
 radius=Cisco {
```

```
check_items= {
2=cisco
}
reply_attributes= {
9,1="vpdn:vpn-domain-list=net1.com,net2.com"
6=5
}
}
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

vpdn domain-delimiter

To specify the characters to be used to delimit the domain prefix or domain suffix, use the **vpdn domain-delimiter** command in global configuration mode. To disable this function, use the **no** form of this command.

vpdn domain-delimiter *characters* [{**suffix** | **prefix**}]
no vpdn domain-delimiter *characters* [{**suffix** | **prefix**}]

Syntax Description

characters	One or more specific characters to be used as suffix or prefix delimiters. Available characters are **%**, **-**, **@**, \ , **#**, and **/**. If a backslash (\) is the last delimiter in the command line, enter it as a double backslash (\\).
suffix | **prefix**	(Optional) Usage of the specified characters.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

You can enter one **vpdn domain-delimiter** command to list the suffix delimiters and another **vpdn domain-delimiter** command to list the prefix delimiters. However, no character can be both a suffix delimiter and a prefix delimiter.

This command allows the network access server to parse a list of home gateway DNS domain names and addresses sent by an AAA server. The AAA server can store domain names or IP addresses in the following AV pair:

cisco-avpair = "lcp:interface-config=ip address 10.1.1.1 255.255.255.255.0",

cisco-avpair = "lcp:interface-config=ip address bigrouter@cisco.com,

Examples

The following example lists three suffix delimiters and three prefix delimiters:

```
vpdn domain-delimiter %-@ suffix
vpdn domain-delimiter #/\\ prefix
```

This example allows the following host and domain names:

```
cisco.com#localddr
localddr@cisco.com
```

Related Commands

Command	Description
vpdn enable	Enables VPDN on the router and directs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn history failure	Enables logging of VPDN failures to the history failure table or to sets the failure history table size.
vpdn profile	Specifies how the network access server for the service provider is to perform VPDN tunnel authorization searches.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

vpdn enable

To enable virtual private dialup networking (VPDN) on the router and inform the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present, use the **vpdn enable** command in global configuration mode. To disable, use the **no** form of this command.

vpdn enable
no vpdn enable

Syntax Description

This command has no arguments or keywords.

Command Default

VPDN is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router as described in the Usage Guidelines below.

Usage Guidelines

The **no vpdn enable** command does not automatically disable a VPDN tunnel.

To shut down a VPDN tunnel, use the **clear vpdn tunnel** command or the **vpdn softshut** command.

Cisco 10000 Series Usage Guidelines

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer accepts the **vpdn-group** command if you issue the command before you issue the **vpdn enable** command. Instead, the following warning message displays:

```
% VPDN configuration is not allowed until VPDN is enabled through 'vpdn enable'.
```

In releases prior to Cisco IOS Release 12.2(33)SB, if you issue the **vpdn-group** command before the **vpdn enable** command, the router accepts the command and displays the following warning message:

```
% VPDN is not enabled
```

Examples

The following example enables VPDN on the router:

```
vpdn enable
```

Related Commands

Command	Description
clear vpdn tunnel	Shuts down a specified tunnel and all sessions within the tunnel.
vpdn history failure	Enables logging of VPDN failures to the history failure table or to sets the failure history table size.

Command	Description
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn softshut	Prevents new sessions from being established on a VPDN tunnel without disturbing existing sessions.

vpdn group

To associate a virtual private dialup network (VPDN) group with a customer or VPDN profile, use the **vpdn group** command in customer profile or in VPDN profile configuration mode. To disassociate a VPDN group from a customer or VPDN profile, use the **no** form of this command.

vpdn group *name*
no vpdn group *name*

Syntax Description

name	Name of the VPDN group. **Note** This name should match the name defined for the VPDN group configured with the **vpdn-group** command.

Command Default

No default behavior or values.

Command Modes

Customer profile configuration

VPDN profile configuration (config-vpdn-profile)

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.

Usage Guidelines

Use the **vpdn group** command in customer profile configuration mode or in VPDN profile configuration mode to associate a VPDN group with a customer profile or a VPDN profile, respectively.

VPDN groups are created by using the **vpdn-group** command in global configuration mode.

Examples

The following example creates the VPDN groups named l2tp and l2f and associates both VPDN groups with the VPDN profile named profile32:

```
Router(config)# vpdn-group l2tp
Router(config-vpdn)#
!
Router(config)# vpdn-group l2f
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn profile32
Router(config-vpdn-profile)# vpdn group l2tp
Router(config-vpdn-profile)# vpdn group l2f
```

The following example creates two VPDN groups and configures them under a customer profile named company2:

```
Router(config)# vpdn-group mygroup
Router(config-vpdn)#
!
Router(config)# vpdn-group yourgroup
```

```
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn company2
Router(config-vpdn-profile)# vpdn group mygroup
Router(config-vpdn-profile)# vpdn group yourgroup
```

Related Commands

Command	Description
resource-pool profile customer	Creates a customer profile and enters customer profile configuration mode.
resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
vpdn profile	Associates a VPDN profile with a customer profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

vpdn history failure

To enable logging of virtual private dialup network (VPDN) failures to the history failure table or to set the failure history table size, use the **vpdn history failure** command in global configuration mode. To disable logging of VPDN history failures or to restore the default table size, use the **no** form of this command.

vpdn history failure [**table-size** *entries*]
no vpdn history failure [**table-size**]

Syntax Description

table-size *entries*	(Optional) Sets the number of entries in the history failure table. The range is 20 to 50.

Command Default

VPDN failures are logged by default. The table size is 20 entries

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Logging of VPDN failure events is enabled by default. You can disable the logging of VPDN failure events by issuing the **no vpdn history failure** command.

The logging of a failure event to the history table is triggered by event logging by the syslog facility. The syslog facility creates a failure history table entry, which keeps records of failure events. The table starts with 20 entries, and the size of the table can be expanded to a maximum of 50 entries by using the **vpdn history failure table-size** *entries* command. You can configure the **vpdn history failure table-size** *entries* command only if VPDN failure event logging is enabled.

All failure entries for the user are kept chronologically in the history table. Each entry records the relevant information of a failure event. Only the most recent failure event per user, unique to its name and tunnel client ID (CLID), is kept.

When the total number of entries in the table reaches the configured table size, the oldest record is deleted and a new entry is added.

Examples

The following example disables logging of VPDN failures to the history failure table:

```
no vpdn history failure
```

The following example enables logging of VPDN failures to the history table and sets the history failure table size to 40 entries:

```
vpdn history failure
vpdn history failure table-size 40
```

Related Commands

Command	Description
show vpdn history failure	Displays the content of the failure history table.

vpdn history failure cause normal

To prevent the message "The remote server closed the session" from overwriting useful messages in the virtual private dialup network (VPDN) connection failure log, use the **no vpdn history failure cause normal** command in global configuration mode. To reenable logging of the message (the default), use the **vpdn history failure cause normal** command.

vpdn history failure cause normal
no vpdn history failure cause normal

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled when the VPDN failure log is enabled, but it does not appear in the configuration of a Layer 2 access concentrator (LAC) or Layer 2 network server (LNS) when the running configuration is listed. When the **no** form of this command is configured, the command be listed in the running configuration. See the “Usage Guidelines” section for more information.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(5a)B1	This command was introduced.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.3(4)T8	This command was integrated into Cisco IOS Release 12.3(4)T8.
12.3(7)T3	This command was integrated into Cisco IOS Release 12.3(7)T3.
12.3(8)T6	This command was integrated into Cisco IOS Release 12.3(7)T6.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.

Usage Guidelines

When users are declared as unauthenticated, their termination is recorded in the VPDN failure log. One method for determining why a subscriber cannot establish a PPP session is for the network operator to check the VPDN failure log for connection failure messages. The router can determine and log specific reasons for session termination, such as authentication failure, exceeding the session limit, timer expiration, and so on. However, a peer LAC or LNS sends the message "VPDN-6-CLOSED" to the router for any type of session termination. All other messages at the console and in the failure log appear under abnormal termination at that router, and the message "The remote server closed the session" is also logged in the VPDN connection failure log. So the failure log, which has maximum of 50 messages, gets filled with messages. Once the maximum message length is reached, new messages begin replacing old messages and information about the unauthenticated users is lost.

The **no vpdn logging cause normal** command disables all system logging (syslog) messages with the prefix "VPDN-6-CLOSED." The **no vpdn history failure cause normal** command is used to prevent the message "The remote server closed the session" from being added to the connection failure log.

Both commands are independent so that configuring the **no vpdn logging cause normal** command does not prevent the message "The remote server closed the session" from being logged. And conversely, configuring

the **no vpdn history failure cause normal** command does not prevent the syslog message "VPDN-6-CLOSED" from appearing.

By default, the **vpdn logging cause normal** command is enabled only when VPDN logging is enabled and does not appear in the **show running-config** command display. When configured, the command **no vpdn logging cause normal** appears in the **show running-config** command display only when VPDN logging is enabled.

By default, the **vpdn history failure cause normal** command is enabled only when the VPDN failure log is enabled, and it does not appear in the **show running-config** command display. When configured, the command **no vpdn history failure cause normal** shows up only when the VPDN history log is enabled.

Regardless of whether the **no vpdn logging cause normal** and the **no vpdn history failure cause normal** commands are configured, all other syslog messages except those with prefix "VPDN-6-CLOSED" appear on the console, and the failure table logs all messages except "The remote server closed the session."

Examples

The default behavior of this command enables logging of the message "The remote server closed the session." The following example shows how to disable both the "The remote server closed the session" and "VPDN-6-CLOSED" messages so that the VPDN connection failure log maintains useful messages about session termination:

```
no vpdn logging cause normal
no vpdn history failure cause normal
```

Related Commands

Command	Description
vpdn logging cause normal	Prevents the message "VPDN-6-CLOSED" from overwriting useful messages in the VPDN connection failure log.

vpdn incoming

The **vpdn incoming** command is replaced by the **accept-dialin** command. See the description of the **accept-dialin** command for more information.

vpdn ip udp ignore checksum

Note Effective with Cisco Release 12.4(33)T, the support for L2F is not available in Cisco IOS Software.

To allow the router to ignore User Datagram Protocol (UDP) checksums for Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP) virtual private dialup network (VPDN) traffic, use the **vpdn ip udp ignore checksum** command in global configuration mode. To disable the ignoring of UDP checksums, use the **no** form of this command.

vpdn ip udp ignore checksum
no vpdn ip udp ignore checksum

Syntax Description

This command has no arguments or keywords.

Command Default

Releases prior to Cisco IOS Release 12.3(13) and 12.3(14)T: UDP checksums are not ignored by default.

Cisco IOS Release 12.3(13) and 12.3(14)T and later releases: UDP checksums are ignored by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(13)	This command was modified to be enabled by default.
12.3(14)T	This command was modified to be enabled by default.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Ignoring UDP checksums is beneficial when the remote tunnel endpoint uses UDP checksums and when you want to use fast switching or Cisco Express Forwarding (CEF). If the remote tunnel endpoint uses UDP checksums and the **vpdn ip udp ignore checksum** command is disabled, all tunnel traffic is process-switched.

In Cisco IOS Release 12.3(13) and Cisco IOS Release 12.3(14)T, this command was modified to be enabled by default.

Cisco 10000 Series Router

When you configure this command, the router directly queues L2TP hello packets and hello acknowledgments to the L2TP control process. We recommend that you configure this command in all scaled LAC and LNS L2TP tunnel configurations.

If you do not configure the **vpdn ip udp ignore checksum** command, the L2TP software sends the packet to UDP to validate the checksum. When too many packets are queued to the IP input process, the router starts selective packet discard (SPD), which causes IP packets to be dropped.

Note Head-of-the-line blocking of the IP input process might occur in other non-L2TP configurations. A flush occurring on an input interface indicates that SPD is discarding packets.

Examples

The following example configures the router to ignore UDP checksums, allowing fast switching or CEF:

```
vpdn ip udp ignore checksum
```

The following example disables the ignoring of UDP checksums on the router:

```
no vpdn ip udp ignore checksum
```

vpdn l2tp attribute

To send the attribute value pairs (AVP) in the session creation packets from the L2TP (Layer 2 Tunneling Protocol) Access Controller (LAC) to the L2TP Network Server (LNS), use the **vpdn l2tp attribute** command in global configuration mode. To disable the sending of AVPs, use the **no** form of this command.

vpdn l2tp attribute {**initial-received-lcp-confreq** | **physical-channel-id**}
no vpdn l2tp attribute {**initial-received-lcp-confreq** | **physical-channel-id**}

Syntax Description

initial-received-lcp-confreq	Specifies that the L2TP incoming call connected (ICCN) packets carry a copy of the Initial Received Link Control Protocol (LCP) configure request (CONFREQ) packet received from the PPP client. The attribute value 26 is added to the ICCN packets that are sent to the LNS.
physical-channel-id	Specifies that the L2TP incoming call request (ICRQ) packets carry the physical channel ID AVP. The attribute value 25 is added to the ICRQ packets that are sent to the LNS.

Command Default

The ICCN and the ICRQ packets do not carry the AVPs to the LNS.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

ICRQ and ICCN are the respective first and last of the three message exchanges that are used for establishing sessions with an L2TP tunnel.

Use the **vpdn l2tp attribute initial-received-lcp-confreq** command in global configuration mode to add the Initial Received LCP CONFREQ AVP to the ICCN packets on the LAC.

Use the **vpdn l2tp attribute physical-channel-id** command in global configuration mode to add the Physical Channel ID AVP to the ICRQ packets on LAC.

Examples

The following example shows how to send the Initial Received LCP CONFREQ attribute to the LNS in the ICCN packets:

```
Router(config)# vpdn enable
Router(config)# vpdn l2tp attribute initial-received-lcp-confreq
```

vpdn l2tp attribute clid mask-method

To configure a network access server (NAS) to suppress Layer 2 Tunneling Protocol (L2TP) calling station IDs globally, use the **vpdn l2tp attribute clid mask-method** command in global configuration mode. To disable this function, use the **no** form of this command.

vpdn l2tp attribute clid mask-method {**right** *mask-character characters* | **remove**} [**match** *match-string*]
no vpdn l2tp attribute clid mask-method {**right** *mask-character characters* | **remove**} [**match** *match-string*]

Syntax Description

right	Specifies that the calling station ID will be masked by replacing characters, starting from the right end of the string.
mask-character	Character to be used as a replacement. Only printable characters are accepted.
characters	Number of characters to be replaced.
remove	Specifies that the entire calling station ID will be removed.
match *match-string*	(Optional) Applies the defined masking method only if the string specified by the *match-string* argument is contained in the username.

Command Default

The calling station ID is not masked or dropped.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.3(14)YM2	This command was integrated into Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7301, Cisco 7204VXR, and Cisco 7206VXR routers.

Usage Guidelines

Use the **vpdn l2tp attribute clid mask-method** command to mask the calling station ID in L2TP attribute-value (AV) pair 22 globally for all virtual private dialup network (VPDN) groups configured on the NAS. This command is compatible with both local and remote RADIUS authorization. You can either substitute characters for a portion of the calling station ID or remove the entire calling station ID.

The **l2tp attribute clid mask-method** command can be used to mask the calling station ID for calls associated with a specific VPDN group or VPDN template. This command is compatible with only local authorization.

Examples

The following example shows how to use the **vpdn l2tp attribute clid mask-method** command globally to mask the L2TP calling station ID during authorization if the username contains the string #184.

```
vpdn enable
vpdn l2tp attribute clid mask-method right # 255 match #184
vpdn search-order domain
```

Related Commands

Command	Description
l2tp attribute clid mask-method	Configures a NAS to suppress L2TP calling station IDs for sessions associated with a VPDN group or VPDN template.

vpdn logging

To enable the logging of virtual private dialup network (VPDN) events , use the **vpdn logging** command in global configuration mode. To disable the logging of VPDN events, use the **no** form of this command.

vpdn logging [{**accounting** | **local** | **remote** | **tunnel-drop** | **user**}]
no vpdn logging [{**accounting** | **local** | **remote** | **tunnel-drop** | **user**}]

Syntax Description

accounting	(Optional) Enables the transmission of VPDN event log messages within an authentication, authorization, and accounting (AAA) accounting record.
local	(Optional) Enables logging of VPDN events to the system message log (syslog) locally.
remote	(Optional) Enables logging of VPDN events to the syslog of the remote tunnel endpoint.
tunnel-drop	(Optional) Enables logging of VPDN tunnel-drop events to the syslog.
user	(Optional) Enables logging of VPDN user events to the syslog.

Command Default

All VPDN event logging is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.1	The **user** keyword was introduced in Cisco IOS Release 12.1.
12.2(11)T	The **tunnel-drop** keyword was introduced in Cisco IOS Release 12.2(11)T.
12.2(15)T	The **accounting** keyword was introduced in Cisco IOS Release 12.2(15)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command controls the logging of VPDN events. By default, all VPDN event logging is disabled.

In Cisco IOS Releases 15.0, 12.2(33)XNE, 12.2(33)SRE, XE 2.5 and later, when you use any keyword with the **vpdn logging** command, the status of the primary flag, which is recognized by the configuration element vpdn logging, is evaluated. If all types of vpdn logging are in their default states (the default for the **vpdn logging cause** command is enabled; the defaults for the other VPDN logging types are disabled), the primary flag is turned off, causing the VPDN logging CLI to no longer be generated in the **show running-config** display by the nvgen process. If you configure any VPDN logging type to a nondefault state, the primary flag is turned on and the **vpdn logging** output is displayed in the **show running-config** command output.

To enable the logging of VPDN events to the syslog of the local or the remote tunnel endpoint router, issue the **vpdn logging** command with the **local** or the **remote** keyword.

To log VPDN user events or VPDN tunnel-drop events to the syslog, you must configure the **vpdn logging** command with the **user** or the **tunnel-drop** keyword.

Configuring the **vpdn logging** command with the **accounting** keyword causes VPDN event log messages to be sent to a remote AAA server in a AAA vendor-specific attribute (VSA). This allows the correlation of VPDN call success rates with accounting records.

Note VPDN event logging to the syslog need not be enabled to allow the reporting of VPDN event log messages to a AAA server.

You can configure as many types of VPDN event logging as you want.

Examples

The following example enables VPDN logging locally:

```
vpdn logging local
```

The following example disables VPDN event logging locally, enables VPDN event logging at the remote tunnel endpoint, and enables the logging of both VPDN user and VPDN tunnel-drop events to the syslog of the remote router:

```
no vpdn logging local
vpdn logging remote
vpdn logging user
vpdn logging tunnel-drop
```

The following example disables the logging of VPDN events to the syslog both locally and at the remote tunnel endpoint, and enables the reporting of VPDN event log messages to the AAA server:

```
no vpdn logging local
no vpdn logging remote
vpdn logging accounting
```

Related Commands

Command	Description
vpdn history failure	Enables logging of VPDN failures to the history failure table or sets the failure history table size.

vpdn logging cause normal

To prevent display of the syslog message "VPDN-6-CLOSED" on the router console, use the **no vpdn logging cause normal** command in global configuration mode. To reenable display of the message (the default), use the **vpdn logging cause normal** command.

vpdn logging cause normal
no vpdn logging cause normal

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled when VPDN logging is enabled, but it does not appear in the configuration of a Layer 2 access concentrator (LAC) or Layer 2 network server (LNS) when the running configuration is listed. When the **no** form of this commands is configured, it is listed in the running configuration. See the "Usage Guidelines" section for more information.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(5a)B1	This command was introduced.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.3(4)T8	This command was integrated into Cisco IOS Release 12.3(4)T8.
12.3(7)T3	This command was integrated into Cisco IOS Release 12.3(7)T3.
12.3(8)T6	This command was integrated into Cisco IOS Release 12.3(7)T6.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.

Usage Guidelines

When users are declared as unauthenticated, their termination is recorded in the VPDN failure log. One method for determining why a subscriber cannot establish a PPP session is for the network operator to check the VPDN failure log for connection failure messages. The router can determine and log specific reasons for session termination, such as authentication failure, exceeding the session limit, timer expiration, and so on. However, a peer LAC or LNS sends the message "VPDN-6-CLOSED" to the router for any type of session termination. All other messages at the console and in the failure log appear under abnormal termination at that router, and the message “The remote server closed the session" is also logged in the VPDN connection failure log. So the failure log, which has maximum of 50 messages, is filled with messages. Once the maximum message length is reached, new messages begin replacing old messages and information about the unauthenticated users is lost.

The **no vpdn logging cause normal** command disables all system logging (syslog) messages with the prefix "VPDN-6-CLOSED." The **no vpdn history failure cause normal** command is used to prevent the message “The remote server closed the session" from being added to the connection failure log.

Both commands are independent so that configuring the **no vpdn logging cause normal** command does not prevent the message “The remote server closed the session” from being logged. And conversely, configuring the **no vpdn history failure cause normal** command does not prevent the syslog message "VPDN-6-CLOSED" from appearing.

By default, the **vpdn logging cause normal** command is enabled only when VPDN logging is enabled, and does not appear in the **show running-config** command output. When configured, the command **no vpdn logging cause normal** is listed in the **show running-config** command output only when VPDN logging is enabled.

By default, the **vpdn history failure cause normal** command is enabled only when the VPDN failure log is enabled, and it does not appear in the **show running-config** command output. When configured, the command **no vpdn history failure cause normal** shows up only when the VPDN history log is enabled.

Regardless of whether the **no vpdn logging cause normal** and the **no vpdn history failure cause normal** commands are configured, all other syslog messages except those with prefix "VPDN-6-CLOSED" appear on the console, and the failure table logs all messages except "The remote server closed the session."

Examples

The default behavior of this command enables display of the syslog message "VPDN-6-CLOSED." The following example shows how to disable both the "VPDN-6-CLOSED" and "The remote server closed the session" messages so that the VPDN connection failure log maintains useful messages about session termination:

```
no vpdn logging cause normal
no vpdn history failure cause normal
```

Related Commands

Command	Description
vpdn history failure cause normal	Prevents the message "The remote server closed the session" from overwriting useful messages in the VPDN connection failure log.

vpdn multihop

To enable virtual private dialup network (VPDN) multihop, use the **vpdn multihop** command in global configuration mode. To disable VPDN multihop capability, use the **no** form of this command.

vpdn multihop
no vpdn multihop

Syntax Description

This command has no arguments or keywords.

Command Default

Multihop is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(5)T	This command was introduced.
12.2(8)B	Support was added for dialed number identification service (DNIS)-based multihop capability.
12.2(13)T	Support was added for DNIS-based multihop capability.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, including support for DNIS-based multihop capability.

Usage Guidelines

Use this command to enable multihop VPDN. Multihop VPDN allows packets to pass through multiple VPDN tunnels. Ordinarily, packets are not allowed to traverse more than one tunnel. With multihop enabled, a packet can traverse as many as four tunnels.

VPDN multihop allows a router configured as a tunnel switch to act as both a network access server (NAS) and a tunnel server, receiving packets from an incoming VPDN tunnel and sending them out over an outgoing VPDN tunnel.

A tunnel switch can terminate incoming VPDN tunnels from multiple devices, and initiate outgoing tunnels to one or more tunnel servers. The outgoing tunnel is selected using either a domain name, a remote tunnel name, or a DNIS number. The order in which these criteria are searched by the software is determined by the **vpdn search-order** command.

VPDN multihop must be enabled for a Multichassis Multilink PPP (MMP) stack group deployment to function when incoming calls traverse a VPDN tunnel. For more information on configuring multihop VPDN for MMP, refer to the *Cisco IOS VPDN Configuration Guide* .

Examples

The following example configures the NAS, tunnel switch, and tunnel server to establish a multihop VPDN tunnel using L2TP:

NAS Configuration

```
! Configure the NAS to initiate VPDN dial-in sessions to the tunnel switch
vpdn-group 1
 request-dialin
```

```
  protocol l2tp
  domain cisco.com
!
 initiate-to ip 172.22.66.25
 local name ISP-NAS
```

Tunnel Switch Configuration

```
!Enable multihop
vpdn multihop
!
! Configure the tunnel switch to use the multihop hostname in the authentication search.
 vpdn search-order multihop-hostname domain dnis
!
! Configure the tunnel switch to accept dial-in sessions from the NAS
vpdn-group tunnelin
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname ISP-NAS
 local name ISP-Sw
!
! Configure the tunnel switch to initiate VPDN dial-in sessions to the tunnel server
vpdn-group tunnelout
 request-dialin
  protocol l2tp
  multihop-hostname ISP-NAS
!
 initiate-to ip 10.2.2.2
 local name ISP-Sw
```

Tunnel Server Configuration

```
! Configure the tunnel server to accept dial-in sessions from the NAS
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname ISP-Sw
 local name ENT-TS
```

The following example configures one member of a stack group and a NAS for dial-in L2F VPDN tunneling. Multihop VPDN must be enabled on each stack group member to allow calls to be forwarded to the bundle owner.

Tunnel Server A Configuration

```
!Enable multihop VPDN
vpdn multihop
!
!Configure the tunnel server to accept L2F tunnels from the NAS
vpdn-group group1
 accept-dialin
```

```
  protocol l2f
  virtual-template 1
  exit
 terminate-from 172.18.32.139
!
!Configure the tunnel server as a stack group member
username user1 password mypassword
sgbp group mystack
sgbp member tunnelserverb 10.1.1.2
sgbp member tunnelserverc 10.1.1.3
```

NAS Configuration

```
!Configure the NAS to initiate L2F tunnels
vpdn-group group1
 request-dialin
  protocol l2f
  domain cisco.com
!
!Configure the NAS with the IP address of each tunnel server in the stack group
 initiate-to ip 10.1.1.1
 initiate-to ip 10.1.1.2
 initiate-to ip 10.1.1.3
```

Related Commands

Command	Description
vpdn enable	Enables VPDN networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn search-order	Specifies how a NAS or tunnel switch is to perform VPDN tunnel authorization searches.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

vpdn outgoing

The **vpdn outgoing** command is replaced by the **request-dialin** command. See the description of the **request-dialin** command for more information.

vpdn pmtu

To manually configure a range of allowed path maximum transmission unit (MTU) sizes for a Layer 2 Tunneling Protocol (L2TP) virtual private dialup network (VPDN), use the **vpdn pmtu** command in global configuration mode. To restore the default value, use the **no** form of this command.

vpdn pmtu {**maximum** *bytes* | **minimum** *bytes*}
no vpdn pmtu

Syntax Description

maximum *bytes*	Sets the maximum allowed size, in bytes, for the path MTU. The range is 68 to 65535 bytes.
minimum *bytes*	Sets the minimum allowed size, in bytes, for the path MTU. The range is 68 to 65535 bytes.

Command Default

No maximum or minimum path MTU size is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(25)	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(27)SB.

Usage Guidelines

Use the **vpdn pmtu** command to prevent Denial of Service (DoS) attacks against L2TP VPDN deployments that are performing path MTU discovery (PMTUD). PMTUD for an L2TP VPDN is disabled by default. To enable PMTUD, use the **ip pmtu** command.

When PMTUD is enabled, VPDN deployments are vulnerable to DoS attacks that use crafted Internet Control Message Protocol (ICMP) "fragmentation needed and Don't Fragment (DF) bit set" (code 4) messages, also known as PMTUD attacks.

When an Internet host is performing PMTUD, crafted code 4 ICMP messages can be used to set the path MTU to an impractically low value. This causes higher layer protocols to time out because of a very low throughput, even though the connection is still in the established state. This type of attack is classified as a throughput-reduction attack.

Use the **vpdn pmtu** command to configure a range of acceptable values for the path MTU when PMTUD is enabled. If the device receives a code 4 ICMP message that advertises a next-hop path MTU outside the configured size range, the device ignores the ICMP message and display this log message:

```
%VPDN-5-IGNOREICMPMTU Ignoring received ICMP Type 3 Code 4, due to pmtu min or max setting
```

For information on detecting a PMTUD attack on an L2TP VPDN deployment, see *Cisco Security Advisory Crafted ICMP Messages Can Cause Denial of Service*.

Cisco software releases that support the **ip pmtu** command but do not support the **vpdn pmtu** command are vulnerable to PMTUD attacks. To protect a device running a vulnerable version of software, issue the **no ip pmtu** command to disable PMTUD.

For a complete list of Cisco software rebuild releases that support the**vpdn pmtu** command, see *Cisco Security Advisory Crafted ICMP Messages Can Cause Denial of Service*.

Examples

The following example enables PMTUD for the VPDN group named mygroup and configures the device to accept path MTU values ranging from 576 to 1460 bytes. The device ignores code 4 ICMP messages that specify a path MTU outside of this range.

```
Router(config)# vpdn-group mygroup
Router(config-vpdn)# ip pmtu
!
Router(config)# vpdn pmtu maximum 1460
Router(config)# vpdn pmtu minimum 576
```

Related Commands

Command	Description
ip pmtu	Enables the discovery of the path MTU for Layer 2 traffic.

vpdn profile

To associate a virtual private dialup network (VPDN) profile with a customer profile, use the **vpdn profile** command in customer profile configuration mode. To remove a VPDN profile from a customer profile, use the **no** form of this command.

vpdn profile *name*
no vpdn profile *name*

Syntax Description

name	VPDN profile name.

Command Default

No default behavior or values.

Command Modes

Customer profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.

Usage Guidelines

Use the **vpdn profile** command to associate a VPDN profile with a customer profile.

VPDN profiles can be used to combine session counting over multiple VPDN groups. This ability can be applied to customer profiles by configuring multiple VPDN groups under a VPDN profile and by associating the VPDN profile with the customer profile by using the**vpdn profile** command.

Examples

The following example shows how to create two VPDN groups, configure the VPDN groups under a VPDN profile named profile1, and then associates the VPDN profile with a customer profile named customer12:

```
Router(config)# vpdn-group 1
Router(config-vpdn)#
!
Router(config)# vpdn-group 2
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn profile1
Router(config-vpdn-profile)# vpdn group 1
Router(config-vpdn-profile)# vpdn group 2
!
Router(config)# resource-pool profile customer customer12
Router(config-vpdn-customer)# vpdn profile profile1
```

Related Commands

Command	Description
resource-pool profile customer	Creates a customer profile.
resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.

Command	Description
vpdn group	Associates a VPDN group with a customer or VPDN profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

vpdn redirect

To enable Layer 2 Tunneling Protocol (L2TP) redirect functionality, use the **vpdn redirect** command in global configuration mode. To disable L2TP redirect functionality, use the **no** form of this command.

vpdn redirect
no vpdn redirect

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP redirect functionality is disabled so that current multihop forwarding behavior is preserved.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Configuring this command on the L2TP network access server (NAS) enables the NAS to perform L2TP redirection by sending a new vendor-specific attribute-value (AV) pair to the L2TP tunnel server. Configuring this command on the stack group tunnel server allows the tunnel server to redirect a call by disconnecting it and requesting the NAS to redirect it. The Stack Group Bidding Protocol (SGBP) stack group tunnel servers must have this command enabled to receive redirected calls, or else they receive calls only through the usual multihop forwarding from the tunnel server that first took the call.

Examples

The following example enables the L2TP redirect feature on the NAS:

```
Router(config)# vpdn redirect
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
vpdn redirect attempts	Restricts the number of redirect attempts possible for an L2TP call on the NAS.
vpdn redirect identifier	Configures a VPDN redirect identifier to use for L2TP call redirection on a stack group tunnel server.
vpdn redirect source	Configures the public redirect IP address of an L2TP stack group tunnel server.

vpdn redirect attempts

To restrict the number of redirect attempts possible for a given Layer 2 Tunneling Protocol (L2TP) call on the L2TP network access server (NAS), use the **vpdn redirect attempts** command in global configuration mode. To restore the default value, use the **no** form of this command.

vpdn redirect attempts *number-of-attempts*
no vpdn redirect attempts *number-of-attempts*

Syntax Description

number-of-attempts	Number of redirect attempts, ranging from 1 to 20.

Command Default

A maximum of three redirect attempts are allowed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The number of redirect attempts is by default always restricted to three even if this command is not explicitly configured. The only use of this command is to configure a redirect attempts value other than the default (which is always in effect).

Examples

The following example configures four redirect attempts:

```
Router(config)# vpdn redirect attempts 4
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
vpdn redirect	Enables L2TP redirect functionality.
vpdn redirect identifier	Configures a VPDN redirect identifier to use for L2TP call redirection on a stack group tunnel server.
vpdn redirect source	Configures the public redirect IP address of an L2TP stack group tunnel server.

vpdn redirect identifier

To configure a virtual private dialup network (VPDN) redirect identifier to use for Layer 2 Tunneling Protocol (L2TP) call redirection on a stack group tunnel server, use the **vpdn redirect identifier** command in global configuration mode. To remove the name of the redirect identifier from the tunnel server, use the **no** form of this command.

vpdn redirect identifier *identifier-name*
no vpdn redirect identifier *identifier-name*

Syntax Description

identifier-name	Name of the redirect identifier to use for call redirection.

Command Default

No identifier name is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **vpdn redirect identifier** command is configured on each of the stack group tunnel servers. To configure the name of the redirect identifier on the network access server (NAS), use the **redirect identifier** command in VPDN group configuration mode.

The NAS compares the configured redirect identifier with the one received from the stack group tunnel server to determine authorization information to redirect the call.

Configuring the redirect identifier is not necessary to perform redirects. If the redirect identifier is not configured, the NAS uses the redirect IP address to obtain authorization information to redirect the call. In that case, the IP address of the new redirected tunnel server must be present in the **initiate-to** command configuration of the VPDN group on the NAS.

The redirect identifier allows new stack group members to be added without the need to update the NAS configuration with their IP addresses. With the redirect identifier configured, a new stack group member can be added and given the same redirect identifier as the rest of the stack group.

If the authorization information for getting to the new redirected tunnel server is different, then you must configure the authorization information via RADIUS using tagged attributes:

```
Cisco:Cisco-Avpair = :0:"vpdn:vpdn-redirect-id=
identifier name
"
```

The NAS chooses the correct tagged parameters to get authorization information for the new redirected tunnel server by first trying to match the redirect identifier (if present) or else by matching the Tunnel-Server-Endpoint IP address.

Examples

The following example configures the redirect identifier named lns1 on a stack group tunnel server:

```
Router(config)# vpdn redirect identifier lns1
```

The following attribute-value (AV) pair configures the RADIUS server with the redirect identifier named lns1 for a tunnel server:

```
Cisco:Cisco-Avpair = :0:"vpdn:vpdn-redirect-id=lns1"
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
vpdn redirect	Enables L2TP redirect functionality.
vpdn redirect attempts	Restricts the number of redirect attempts possible for an L2TP call on the NAS.
vpdn redirect source	Configures the public redirect IP address of an L2TP stack group tunnel server.

vpdn redirect source

To configure the public redirect IP address of a Layer 2 Tunneling Protocol (L2TP) stack group tunnel server, use the **vpdn redirect source** command in global configuration mode. To remove the public redirect IP address of a stack group tunnel server, use the **no** form of this command.

vpdn redirect source *redirect-ip-address*
no vpdn redirect source *redirect-ip-address*

Syntax Description

redirect-ip-address	Public redirect IP address for a stack group tunnel server.

Command Default

If the **vpdn redirect source** command is not configured, then the IP address used for Stack Group Bidding Protocol (SGBP) bidding itself is used as the redirect address (the public redirect address is then omitted in the bid response).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

On the network access server (NAS), this command has no effect.

Examples

The following example configures a public IP address as a redirect source:

```
Router(config)# vpdn redirect source 10.1.1.1
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
vpdn redirect	Enables L2TP redirect functionality.
vpdn redirect attempts	Restricts the number of redirect attempts possible for an L2TP call on the NAS.
vpdn redirect identifier	Configures a VPDN redirect identifier to use for L2TP call redirection on a stack group tunnel server.

vpdn search-order

To specify how a network access server (NAS) or tunnel switch performs virtual private dialup network (VPDN) tunnel authorization searches, use the **vpdn search-order** command in global configuration mode. To restore the default search order, use the **no** form of this command.

vpdn search-order {**dnis** [**domain**] [**multihop-hostname**] | **domain** [**dnis**] [**multihop-hostname**] | **multihop-hostname** [**dnis**] [**domain**]}
no vpdn search-order

Syntax Description

dnis	Searches on the dialed number identification service (DNIS) number.
domain	Searches on the domain name.
multihop-hostname	Searches on the hostname or tunnel ID of the ingress tunnel for a multihop tunnel switch.

Command Default

When this command is disabled, by default the router searches first on the DNIS number provided on ISDN lines and then searches on the domain name. This is equivalent to issuing the **vpdn search-order dnis domain** command.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.
12.2(13)T	The **multihop-hostname** keyword was added.
12.2(28)SB	The **multihop-hostname** keyword was added.

Usage Guidelines

To issue the **vpdn search-order** command, you must include at least one of the search parameter keywords. You can enter multiple keywords, and they can be entered in any order. The order of the keywords specifies the order of precedence given to the search parameters. If you do not issue a particular keyword, no search is performed on that parameter.

Issue the **multihop-hostname** keyword only on a device configured as a multihop tunnel switch.

The configuration shows the **vpdn search-order** command setting only if the command is explicitly configured.

Examples

The following example configures a NAS to perform tunnel authorization searches based on DNIS number only:

```
vpdn search-order dnis
```

The following example configures a tunnel switch to select a tunnel destination based on the multihop hostname first, then on the domain name, and finally on the DNIS number:

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

Related Commands

Command	Description
multihop-hostname	Enables the tunnel switch to initiate a tunnel based on the hostname or tunnel ID of the ingress tunnel.
vpdn multihop	Enables VPDN multihop.

vpdn session accounting

To enable tunnel-link type accounting records to be sent to the RADIUS server, use the **vpdn session accounting** command in global configuration mode. To disable the tunnel-link type accounting records, use the **no** form of this command.

vpdn session accounting {**network** *list-name* | **suppress multihop** {**inbound** | **outbound**}}
no vpdn session accounting {**network** | **suppress**}

Syntax Description

network	Specifies the virtual private dialup network (VPDN) network session accounting method.
list-name	Character string used to name the list of at least one accounting method. The *list-name* value specified in this command must match the *list-name* value defined in the **aaa accounting** command; otherwise, network accounting does not occur.
suppress	Suppresses the accounting options in the VPDN network session.
multihop	Suppresses the multihop attributes in the VPDN network session.
inbound	Suppresses the multihop inbound tunnel attributes in the VPDN network session.
outbound	Suppresses the multihop outbound tunnel attributes in the VPDN network session.

Command Default

Tunnel-link type accounting records are not sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **inbound**, **multihop**, **outbound**, and the **suppress** keywords were added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Before you enable the **vpdn session accounting network** command, you must enable network accounting by using the **aaa accounting** command.

Note If the default network accounting method list is configured and no additional accounting configurations are enabled on the interface, network accounting is enabled by default. If the **vpdn session accounting network** command is linked to the default method list, all tunnel-link accounting records are enabled for those sessions.

This command displays the following tunnel-link accounting type records, which are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40):

- Tunnel-Link-Start (12)--Marks the creation of a tunnel link.
- Tunnel-Link-Stop (13)--Marks the end of a tunnel link.

Note Only some tunnel types (such as Layer 2 Tunneling Protocol [L2TP]) support the multiple links per tunnel; these values should be included for accounting packets for tunnel types that support multiple links per tunnel.

- Tunnel-Link-Reject (14)--Marks the rejection of a tunnel setup for a new link in an existing tunnel. Only some tunnel types (L2TP) support the multiple links per tunnel; this value should be included only in accounting packets for tunnel types that support multiple links per tunnel.

Note If either Tunnel-Link-Start or Tunnel-Link-Stop is enabled, Tunnel-Link-Reject is sent even if it has not been enabled.

Examples

The following example shows how to configure an L2TP access concentrator (LAC) to send tunnel-link type accounting records to the RADIUS server:

```
aaa accounting network m1 start-stop group radius
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 10.1.1.1
 local name ISP_LAC
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
vpdn tunnel accounting network	Enables tunnel type accounting records to be sent to the RADIUS server.

vpdn session-limit

To limit the number of simultaneous virtual private dialup network (VPDN) sessions allowed on a router, use the **vpdn session-limit** command in global configuration mode. To remove a configured session limit restriction, use the **no** form of this command.

vpdn session-limit *sessions*
no vpdn session-limit

Syntax Description

sessions	Maximum number of simultaneous VPDN sessions that are allowed on a router. The range is 1 to 5000.

Command Default

No session limit exists for the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

Use the **vpdn session-limit** command to configure the maximum number of VPDN sessions allowed on the router.

VPDN session limits can be configured globally by using the **vpdn session-limit** command, at the level of a VPDN group by using the **session-limit** (VPDN) command, or for all VPDN groups associated with a particular VPDN template by using the **group session-limit** command.

The hierarchy for the application of VPDN session limits is as follows:

- Globally configured session limits take precedence over session limits configured for a VPDN group or in a VPDN template. The total number of sessions on a router cannot exceed a configured global session limit.
- Session limits configured for a VPDN template are enforced for all VPDN groups associated with that VPDN template. The total number of sessions for all of the associated VPDN groups cannot exceed the configured VPDN template session limit.
- Session limits configured for a VPDN group are enforced for that VPDN group.

Examples

The following example sets a limit of two simultaneous VPDN sessions on the router:

```
vpdn session-limit 2
```

Related Commands

Command	Description
group session-limit	Limits the number of simultaneous VPDN sessions allowed across all VPDN groups associated with a particular VPDN template.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.

Command	Description
session-limit (VPDN)	Limits the number of simultaneous VPDN sessions allowed for a specified VPDN group.

vpdn softshut

To prevent new sessions from being established on a virtual private dialup networking (VPDN) tunnel without disturbing existing sessions, use the **vpdn softshut** command in global configuration mode. To return VPDN tunnels to active service, use the **no** form of this command.

vpdn softshut
no vpdn softshut

Syntax Description

This command has no arguments or keywords.

Command Default

New sessions can be established.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

When this feature is enabled on a network access server (NAS), the potential session is authorized before it is refused. This authorization ensures that accurate accounting records can be kept.

When this feature is enabled on a home gateway, the reason for the session refusal is returned to the NAS. This information is recorded in the VPN history failure table.

When this command is enabled, use the**show vpdn history failure** command to view records of refused attempts to establish new sessions.

Examples

The following example first enables the **vpdn softshut** command and then shows a syslog message stating that an attempt to establish a new session was refused:

```
Router(config)# vpdn softshut
Router(config)#
00:11:17:%VPDN-6-SOFTSHUT:L2F HGW great_went has turned on softshut and rejected user
user1@cisco.com
Router(config)#
```

Related Commands

Command	Description
show vpdn history failure	Displays the content of the failure history table.
vpdn session-limit	Limits the number of simultaneous VPDN sessions that can be established on a router.

vpdn source-ip

To globally specify an IP address that is different from the physical IP address used to open a virtual private dialup network (VPDN) tunnel, use the **vpdn source-ip** command in global configuration mode. To disable use of the alternate IP address, use the **no** form of this command.

vpdn source-ip *ip-address*
no vpdn source-ip *ip-address*

Syntax Description

ip-address	Alternate IP address.

Command Default

No alternate IP address is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use the **vpdn source-ip** command to specify a single alternate IP address to be used for all tunnels on the device. A single source IP address can be configured globally per device.

Use the **source-ip** command in VPDN group configuration mode to configure an alternate IP address to be used for only those tunnels associated with that VPDN group.

The VPDN group-level configuration overrides the global configuration.

Examples

This example sets a source IP address of 172.24.48.3:

```
vpdn source-ip 172.24.48.3
```

Related Commands

Command	Description
source-ip	Specifies an IP address that is different from the physical IP address used to open a VPDN tunnel for the tunnels associated with a VPDN group.
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server, if one is present.

vpdn tunnel accounting network

To enable tunnel type accounting records to be sent to the RADIUS server, use the **vpdn tunnel accounting network** command in global configuration mode. To disable tunnel type accounting records, use the **no** form of this command.

vpdn tunnel accounting network *list-name*
no vpdn tunnel accounting network *list-name*

Syntax Description

list-name	Character string used to name the list of at least one accounting method. The *list-name* value must match the *list-name* value defined in the **aaa accounting** command; otherwise, network accounting does not occur.

Command Default

Tunnel type accounting records are not sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Before you enable the **vpdn tunnel accounting network** command, you must enable network accounting by using the **aaa accounting** command.

Note If the default network accounting method list is configured and no additional accounting configurations are enabled on the interface, network accounting is enabled by default. If the **vpdn tunnel accounting network** command is linked to the default method list, all tunnel accounting records are enabled for those sessions.

This command displays the following tunnel accounting type records, which are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40):

- Tunnel-Start (9)--Marks the beginning of a tunnel setup with another node.
- Tunnel-Stop (10)--Marks the end of a tunnel connection to or from another node.
- Tunnel-Reject (11)--Marks the rejection of a tunnel setup with another node.

Note If either Tunnel-Start or Tunnel-Stop are enabled, Tunnel-Reject is sent even if it has not been enabled.

Examples

The following example shows how to configure an L2TP access concentrator (LAC) to send tunnel type accounting records to the RADIUS server:

```
! The method list defined in the VPDN command must be the same as the method list defined
! in aaa accounting command; otherwise, accounting will not occur.
aaa accounting network m1 start-stop group radius
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 10.1.1.1
 local name ISP_LAC
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
vpdn session accounting network	Enables tunnel-link type accounting records to be sent to the RADIUS server.

vpdn tunnel authorization network

To enable the Layer 2 Tunnel Protocol (L2TP) tunnel server or network access server (NAS) to perform remote authentication, authorization, and accounting (AAA) tunnel authentication and authorization, use the **vpdn tunnel authorization network** command in global configuration mode. To disable remote tunnel authentication and authorization and return to the default setting, use the **no** form of this command.

vpdn tunnel authorization network {*list-name* | **default**}
no vpdn tunnel authorization network {*list-name* | **default**}

Syntax Description

list-name	Character string used to name the list of at least one accounting method. If the *list-name* argument was specified in the **aaa authorization network** command, you must use the same list name with the **vpdn tunnel authorization network** command.
default	Specifies the default authorization methods that are listed with the **aaa authorization network** command. If the **default** keyword was specified in the **aaa authorization network** command, you must use the **default** keyword with the **vpdn tunnel authorization network** command.

Command Default

If this command is not enabled, the device performs authentication locally.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use this command to specify the authorization method list that is used for remote tunnel hostname-based authorization. The method list (named or default) is defined using the **aaa authorization network** command.

If a method list for tunnel authorization is not specified via the **aaa authorization network** command, local authorization using the local virtual private dialup network (VPDN) group configuration occurs.

Note This method list is only for L2TP tunnel authorization and termination; it is not intended for domain or dialed number identification service (DNIS)-based authorization that is typically done on the tunnel terminator. Thus, this command can be enabled only on the tunnel terminator--the NAS for dial-out and the tunnel server for dial-in.

Examples

The following example shows how to configure the tunnel server to enable remote RADIUS tunnel authentication and authorization:

```
! Define a RADIUS server group
Router(config)# aaa group server radius VPDN-group
```

```
Router(config-sg-radius)# server 10.102.48.91 auth-port 1645 acct-port 1646
Router(config-sg-radius)# exit
Router(config)# aaa authorization network mymethodlist group VPDN-Group

Router(config)# vpdn tunnel authorization network mymethodlist
Router(config)# vpdn tunnel authorization virtual-template 10
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

vpdn tunnel authorization password

To configure a password for the RADIUS authentication request to retrieve the tunnel configuration that is based on the remote tunnel hostname, use the **vpdn tunnel authorization password** command in global configuration mode. To return to the default password, use the **no** form of this command.

vpdn tunnel authorization password *password*
no vpdn tunnel authorization password *password*

Syntax Description

password	Character string, which is truncated after 25 characters.

Command Default

The password is set to "cisco."

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command can be used on either the Layer 2 Tunneling Protocol (L2TP) network access server (NAS) or on the L2TP tunnel server when remote RADIUS tunnel authentication is enabled.

Examples

The following example shows how to set the password to configure the tunnel server to enable remote RADIUS tunnel authentication and authorization and how to set the password to mypassword:

```
Router(config)# aaa authorization network mymethodlist group VPDN-Group

Router(config)# vpdn tunnel authorization network mymethodlist
Router(config)# vpdn tunnel authorization virtual-template 10
Router(config)# vpdn tunnel authorization password mypassword
```

Related Commands

Command	Description
vpdn tunnel authorization network	Enables the L2TP tunnel server or NAS to perform remote AAA tunnel authentication and authorization.

vpdn tunnel authorization virtual-template

To select the default virtual template from which to clone virtual access interfaces, use the **vpdn tunnel authorization virtual-template** command in global configuration mode. To remove the default virtual template, use the **no** form of this command.

vpdn tunnel authorization virtual-template *vtemplate-number*
no vpdn tunnel authorization virtual-template *vtemplate-number*

Syntax Description

vtemplate-number	The default virtual template number that is used for cloning on the local router. The range is 1 to 200.

Command Default

No default virtual template is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command should be used if a virtual template is not specified in the local virtual private dialup network (VPDN) group (for local authentication) or in a remote RADIUS configuration (via the vpdn-vtemplate attribute).

Note This command applies only on the L2TP tunnel server.

Examples

The following example shows how to configure the tunnel server to enable remote RADIUS tunnel authentication and authorization and how to specify a default virtual template:

```
! Define a RADIUS server group
Router(config)# aaa group server radius VPDN-group

Router(config-sg-radius)# server 10.102.48.91 auth-port 1645 acct-port 1646
Router(config-sg-radius)# exit
! RADIUS configurations only
Router(config)# aaa authorization network mymethodlist group VPDN-Group

Router(config)# vpdn tunnel authorization network mymethodlist
! Can be used for local vpdn-group tunnel authentication or remote RADIUS tunnel
! authentication
Router(config)# vpdn tunnel authorization virtual-template 10
```

Related Commands

Command	Description
vpdn tunnel authorization network	Enables the L2TP tunnel server or NAS to perform remote AAA tunnel authentication and authorization.

vpdn-group

To create a virtual private dialup network (VPDN) group and to enter VPDN group configuration mode, use the **vpdn-group** command in global configuration mode. To remove the group, use the **no** form of this command.

vpdn-group *name*
no vpdn-group *name*

Syntax Description

name	Name of the VPDN group.

Command Default

VPDN groups are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router as described in the Usage Guidelines section.
Cisco IOS XE Release 3.3S	This command was modified. The message for duplicate configurations was enhanced to include more information as described in the Usage Guidelines section.

Usage Guidelines

Use the **vpdn-group** command to configure VPDN parameters that are always applied to that VPDN group. System default settings for VPDN parameters are applied for any settings not configured in the individual VPDN group or in the associated VPDN template.

VPDN groups are associated with the global VPDN template by default. You can associate individual VPDN groups with a named VPDN template instead. Associating a VPDN group with a named VPDN template disassociates the VPDN group from the global VPDN template.

If you create two VPDN groups with the same configuration, this message displays:

```
% Warning, the vpdn groups group1 and group2 have the same configuration
```

You should change one of the group configurations to eliminate the duplicate configuration. Leaving the duplicate configurations in place can lead to unexpected (and unsupported) results.

Cisco 10000 Series Usage Guidelines

In Cisco IOS Release 12.2(33)SB and later releases, the router does not accept the **vpdn-group** command if you issue the command before you issue the **vpdn enable** command. Instead, this message displays:

```
% VPDN configuration is not allowed until VPDN is enabled through 'vpdn enable'.
```

In releases prior to Cisco IOS Release 12.2(33)SB, if you issue the **vpdn-group** command before the **vpdn enable** command, the router accepts the command and displays this message:

```
% VPDN is not enabled
```

Examples

The following example configures a source IP address for tunnels associated with the VPDN group named tunneling. This source IP address overrides any configured global source IP address for tunnels associated with this VPDN group.

```
Router(config)# vpdn enable
Router(config)# vpdn-group tunneling
Router(config-vpdn)# source-ip 10.1.1.2
```

The following example configures two VPDN parameters in a VPDN template named l2tp. The named VPDN template is associated with the VPDN group named l2tp_tunnels.

```
Router(config)# vpdn enable
Router(config)# vpdn-template l2tp
Router(config-vpdn-templ)# l2tp tunnel busy timeout 65
Router(config-vpdn-templ)# l2tp tunnel password tunnel4me
Router(config-vpdn-templ)# exit
Router(config)# vpdn-group l2tp_tunnels
Router(config-vpdn)# source vpdn-template l2tp_tunnels
Router(config-vpdn-profile)# vpdn group yourgroup
```

Related Commands

Command	Description
vpdn enable	Enables VPDN on the router and directs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.
vpdn profile	Associates a VPDN profile with a customer profile.

vpdn-template

To create a virtual private dialup network (VPDN) template and enter VPDN template configuration mode, use the **vpdn-template** command in global configuration mode. To delete a VPDN template, use the **no** form of this command.

vpdn-template [*name*]
no vpdn-template [*name*]

Syntax Description

name	(Optional) Name of a VPDN template.

Command Default

No VPDN template exists. The system default values are applied to individual VPDN groups for any parameters that are not configured in the individual VPDN group.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)B	This command was introduced on the Cisco 7200 series and Cisco 7401ASR routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T without support for the *name* argument.
12.2(13)T	The *name* argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use this command to configure values for VPDN parameters in a VPDN template. A single unnamed VPDN template can be configured. Multiple named VPDN templates can be configured. A VPDN group can be associated with only one VPDN template.

Values configured in the global (unnamed) VPDN template are applied to all VPDN groups by default. A VPDN group can be disassociated from the global VPDN template, or associated with a named VPDN template. Associating a VPDN group with a named VPDN template automatically disassociates it from the global VPDN template.

The values configured in a VPDN template are applied to all associated VPDN groups unless specific values are configured for individual VPDN groups. VPDN parameters that are not specified in the individual VPDN group or in the associated VPDN template are assigned system default values.

The hierarchy for the application of VPDN parameters to a VPDN group is as follows:

- VPDN parameters configured for the individual VPDN group are always applied to that VPDN group.
- VPDN parameters configured in the associated VPDN template are applied for any settings not specified in the individual VPDN group configuration.
- System default settings for VPDN parameters are applied for any settings not configured in the individual VPDN group or the associated VPDN template.

Not all commands that are available for configuring a VPDN group can be used to configure a VPDN template. The table below lists the commands that can be used to configure the VPDN template.

Table 3: Commands Available for VPDN Template Configuration

Command Name	Description
default (VPDN)	Removes a VPDN subgroup configuration, or resets it to its default value.
description	Adds a description for a VPDN group.
group session-limit	Specifies the maximum number of concurrent sessions allowed across all VPDN groups associated with a particular VPDN template.
ip mtu adjust	Enables automatic adjustment of the IP maximum transmission unit (MTU) on a virtual access interface.
ip pmtu	Enables the discovery of the path MTU for Layer 2 traffic.
ip precedence (VPDN)	Sets the precedence value in the VPDN Layer 2 encapsulation header.
ip tos (VPDN)	Sets the type of service (ToS) bits in the VPDN Layer 2 encapsulation header.
l2f ignore-mid-sequence	Configures the router to ignore message identifier (MID) sequence numbers for sessions in a Layer 2 Forwarding (L2F) tunnel.
l2f tunnel busy timeout	Configures the amount of time that the router waits before attempting to recontact an L2F peer that was previously busy.
l2f tunnel retransmit initial retries	Configures the number of times that the router attempts to send the initial control packet for tunnel establishment before considering an L2F peer busy.
l2f tunnel retransmit retries	Configures the number of times the router attempts to resend an L2F tunnel control packet before tearing the tunnel down.
l2f tunnel timeout setup	Configures the amount of time that the router waits for a confirmation message after sending out the initial L2F control packet before considering a peer busy.
l2tp attribute clid mask-method	Configures a network access server (NAS) to provide Layer 2 Tunnel Protocol (L2TP) calling line ID suppression for local authorization.
l2tp drop out-of-order	Instructs a NAS or tunnel server using L2TP to drop packets that are received out of order.
l2tp hidden	Enables L2TP attribute-value (AV) pair hiding, which encrypts the value of sensitive AV pairs.
l2tp ip udp checksum	Enables IP User Datagram Protocol (UDP) checksums on L2TP payload packets.
l2tp security crypto-profile	Configures IP Security (IPSec) protection of L2TP sessions associated with a VPDN group.
l2tp sequencing	Enables sequencing for packets sent over an L2TP tunnel.

Command Name	Description
l2tp tunnel authentication	Enables L2TP tunnel authentication.
l2tp tunnel bearer capabilities	Sets the bearer-capability value used by the Cisco router.
l2tp tunnel busy timeout	Configures the amount of time that the router waits before attempting to recontact an L2TP peer that was previously busy.
l2tp tunnel framing capabilities	Sets the framing-capability value used by the Cisco router.
l2tp tunnel hello	Sets the number of seconds between sending hello keepalive packets for an L2TP tunnel.
l2tp tunnel password	Sets the password the router uses to authenticate the tunnel.
l2tp tunnel receive-window	Configures the number of packets allowed in the local receive window for an L2TP control channel.
l2tp tunnel retransmit initial retries	Configures the number of times that the router attempts to send out the initial L2TP control packet for tunnel establishment before considering a peer busy.
l2tp tunnel retransmit initial timeout	Configures the amount of time that the router waits before resending an initial L2TP control packet to establish a tunnel.
l2tp tunnel retransmit retries	Configures the number of retransmission attempts made for an L2TP control packet.
l2tp tunnel retransmit timeout	Configures the amount of time that the router waits before resending an L2TP control packet.
l2tp tunnel timeout no-session	Configures the time a router waits after an L2TP tunnel becomes empty before tearing down the tunnel.
l2tp tunnel timeout setup	Configures the amount of time that the router waits for a confirmation message after sending the initial L2TP control packet before considering a peer busy.
l2tp tunnel zlb delay	Configures the delay time before a zero length bit (ZLB) control message must be acknowledged.
local name	Specifies a local hostname that the tunnel uses to identify itself.
pptp flow-control receive-window	Specifies how many packets the Point-to-Point Tunnel Protocol (PPTP) client can send before it must wait for the acknowledgment from the tunnel server.
pptp flow-control static-rtt	Specifies the timeout interval of the PPTP tunnel server between sending a packet to the client and receiving a response.
pptp tunnel echo	Specifies the period of idle time on the PPTP tunnel that triggers an echo message from the tunnel server to the client.

Command Name	Description
redirect identifier	Configures a VPDN redirect identifier to use for L2TP call redirection on a NAS.
relay pppoe bba-group	Configures the PPP over Ethernet (PPPoE) broadband access (BBA) group that responds to PPPoE Active Discovery (PAD) messages.
vpn	Specifies that the source and destination IP addresses of a given VPDN group belong to a specified VPN routing and forwarding instance (VRF).

Examples

The following example enters VPDN template configuration mode and configures two VPDN parameters in the global VPDN template:

```
Router(config)# vpdn-template
Router(config-vpdn-templ)# local name myrouter
Router(config-vpdn-templ)# ip mtu adjust
```

The following example creates a VPDN template named l2tp, enters VPDN template configuration mode, configures two VPDN parameters in the VPDN template, and associates the VPDN group named l2tptunnels with the VPDN template:

```
Router(config)# vpdn-template l2tp
Router(config-vpdn-templ)# l2tp tunnel busy timeout 65
Router(config-vpdn-templ)# l2tp tunnel password 7 tunnel4me
!
Router(config)# vpdn-group l2tptunnels
Router(config-vpdn)# source vpdn-template l2tp
```

The following example configures a VPDN template called customer1 and applies a group session limit of 50 to all VPDN groups associated with that VPDN template:

```
Router(config)# vpdn-template customer1
Router(config-vpdn-templ)# group session-limit 50
```

Related Commands

Command	Description
group session-limit	Specifies the maximum number of concurrent sessions allowed across all VPDN groups associated with a particular VPDN template.
source vpdn-template	Associates a VPDN group with a VPDN template.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

vpn

To specify that the source and destination IPv4 addresses of a given virtual private dialup network (VPDN) group belong to a specified virtual private network (VPN) routing and forwarding (VRF) instance, use the **vpn** command in VPDN group or VPDN template configuration mode. To disassociate all IPv4 addresses in a VPDN group from a VRF, use the **no** form of this command.

vpn {**vrf** *vrf-name* | **id** *vpn-id*}
no vpn

Syntax Description

vrf *vrf-name*	Name of the VRF instance to be associated with the IPv4 addresses of the VPDN group.
id *vpn-id*	VPN ID of the VRF to be associated with the IPv4 addresses of the VPDN group.

Command Default

VPDN groups are not associated with a VRF.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI7	This command was integrated into Cisco IOS Release 12.3(7)XI7 and implemented on the Cisco 10000 series routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB for the PRE2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **vpn** command to configure the software to look up a VPDN source or destination IPv4 address in a specific VPN routing table instead of the global routing table.

Before you can issue the **vpn** command, a VRF instance must be created by using the **ip vrf** command.

The **vpn** command can be used with both dial-in and dial-out VPDN scenarios.

Examples

The following example associates the IP addresses configured in the VPDN group named group1 with the VRF named vrf-second:

```
vpdn-group group1
 request-dialin
 protocol l2tp
!
 vpn vrf vrf-second
```

```
 source-ip 172.16.1.9
 initiate-to ip 172.16.1.1
```

The following example associates the IP addresses configured in the VPDN group named group2 with the VPN ID 11:2222:

```
vpdn-group group2
 request-dialin
 protocol l2tp
!
 vpn id 11:2222
 source-ip 172.16.1.9
 initiate-to ip 172.16.1.1
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.
show vpdn tunnel	Displays information about active Layer 2 tunnels for a VPDN.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.