



L2TP Domain Screening

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

- User preauthentication using the **vpdn authen-before-forward** command
- Modifying the domain portion of the username using the **vpn service** command to bind an incoming session to a certain L2TP tunnel

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

History for the L2TP Domain Screening Feature

Release	Modification
12.3(7)XI7	This feature was introduced on the Cisco 10000 series router.
12.2(31)SB2	This feature was integrated into Cisco IOS Release 12.2(31)SB2.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- [Prerequisites for L2TP Domain Screening, page 2](#)
- [Information About L2TP Domain Screening, page 2](#)
- [How to Configure L2TP Domain Screening, page 5](#)
- [Configuration Examples for L2TP Domain Screening, page 12](#)
- [Additional References, page 15](#)



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 15](#)
- [Command Reference, page 16](#)
- [Glossary, page 18](#)

Prerequisites for L2TP Domain Screening

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

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

Information About L2TP Domain Screening

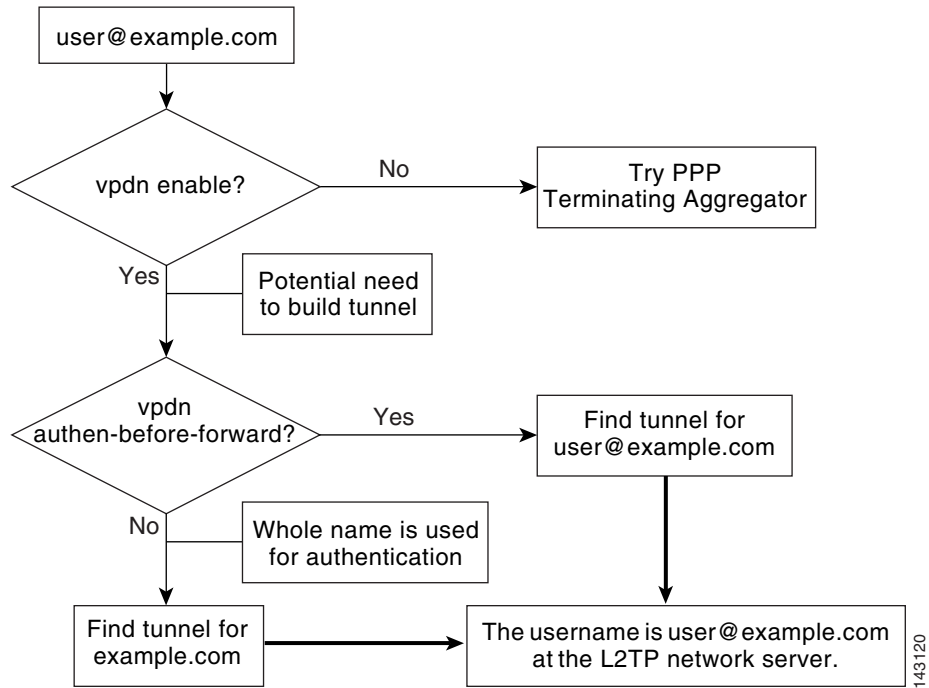
To configure the L2TP Domain Screening feature, you should understand the following concept:

- L2TP tunnel authentication

L2TP Tunnel Authentication

[Figure 1](#) shows the general process flow for tunnel authentication. In this case, the vpdn authen-before-forward process is called if necessary to authenticate the username and domain name to find the correct L2TP tunnel for the session. If no authentication is required, the tunnel match for the domain name is found for the session. In either case, the original username with the original domain is used for session authentication at the L2TP network server.

Figure 1 Normal Tunnel Authentication Without VPN Service



In [Figure 2](#), the same authentication flow proceeds, this time with the VPN service applied to the configuration. Just as before, if the vpdn authen-before-forward process determines that the session must be locally authenticated before being placed into the correct tunnel, authentication proceeds as normal. However, with the vpn service statement applied, the session is placed into the appropriate tunnel for the VPN domain.

Figure 2 Normal Tunnel Authentication with VPN Service Configured

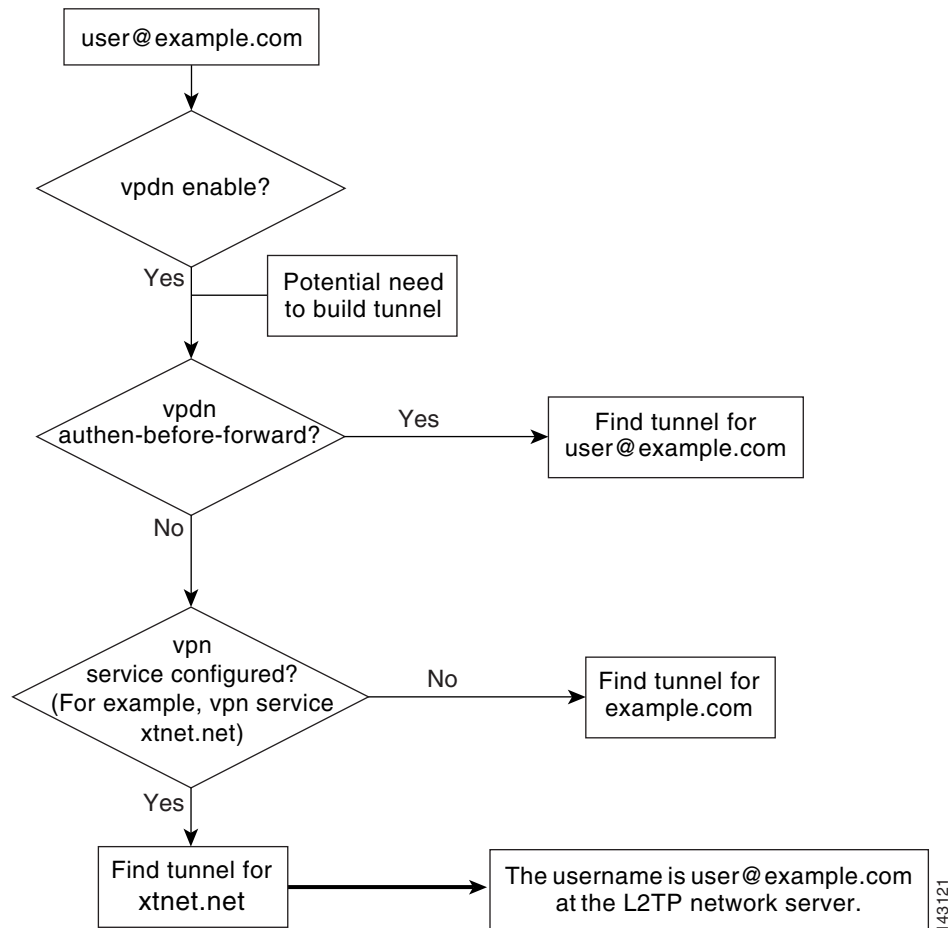


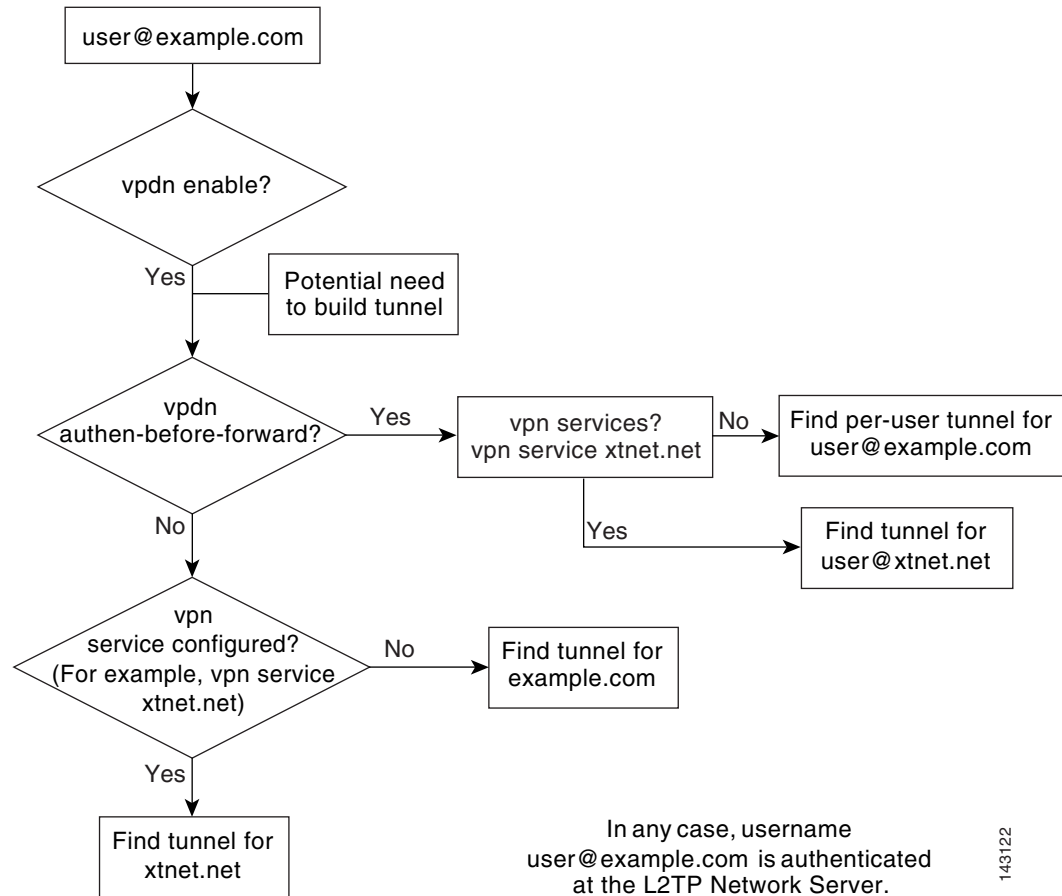
Figure 3 shows the full VPN service application flow. If local authentication at the LAC is required and a VPN service is configured, a local authentication is done with the username provided and the domain of the VPN service provider. This step returns the necessary L2TP tunnel for this VPN session. If VPN service is not configured, local authentication is provided on the username and domain name provided by the subscriber.

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

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

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

Figure 3 **New Operation with VPN Service**



143122

How to Configure L2TP Domain Screening

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

This section contains the following procedures:

- [Configuring L2TP Domain Screening with Global Preauthentication, page 5](#) (required)
- [Configuring a RADIUS User Profile for L2TP Domain Screening with Global Preauthentication, page 8](#) (required)
- [Configuring L2TP Domain Screening with Per-VPDN Group Preauthentication, page 8](#) (required)

Configuring L2TP Domain Screening with Global Preauthentication

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router(config)# aaa new-model	Enables the authentication, authorization, and accounting (AAA) access control system.
Step 4	aaa authentication ppp {default list-name} method1 [method2...] Example: Router(config)# aaa authentication ppp default group radius	Specifies using RADIUS authentication for PPP authentication.

	Command or Action	Purpose
Step 5	<pre>aaa authorization {network exec commands level reverse-access configuration} {default list-name} method1 [method2...]</pre> <p>Example: Router(config)# aaa authorization network default group radius</p>	<p>Specifies running authorization for all network-related service requests and uses group radius as the default method for authorization.</p> <p>This command is required for the AAA server to provide VPDN attributes.</p>
Step 6	<pre>radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number]</pre> <p>Example: Router(config)# radius-server host 23.5.6.100 auth-port 1645 acct-port 1646</p>	<p>Specifies the AAA server that will supply the network access server or L2TP access concentrator (LAC) with the VPDN attributes for the user.</p>
Step 7	<pre>radius-server key {0 string 7 string string}</pre> <p>Example: Router(config)# radius-server key cisco</p>	<p>Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.</p>
Step 8	<pre>vpdn enable</pre> <p>Example: Router(config)# vpdn enable</p>	<p>Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database or on a remote authorization server (home gateway), if one is present.</p>
Step 9	<pre>vpdn authen-before-forward</pre> <p>Example: Router(config)# vpdn authen-before-forward</p>	<p>Enables authentication of all dial-in L2TP sessions before the sessions are forwarded to the tunnel server (global preauthentication).</p>
Step 10	<pre>interface atm interface-number</pre> <p>Example: Router(config)# interface atm 4/0</p>	<p>Defines an ATM interface.</p>
Step 11	<pre>ip address ip-address mask</pre> <p>Example: Router(config-if)# ip address 3.0.0.2 255.255.0.0</p>	<p>Sets the primary IP address for this interface.</p>
Step 12	<pre>pvc vpi/vci</pre> <p>Example: Router(config-if)# pvc 1/20</p>	<p>Enters ATM VC configuration mode for the interface identified by this virtual path identifier/virtual channel identifier pair.</p>
Step 13	<pre>encapsulation aal5snap</pre> <p>Example: Router(config-if-atm-vc)# encapsulation aal5snap</p>	<p>Configures the encapsulation type for this PVC range. The global default encapsulation option is aal5snap.</p>

	Command or Action	Purpose
Step 14	<code>protocol pppoe</code> Example: Router(config-if-atm-vc)# protocol pppoe	Enables PPP over Ethernet sessions for this PVC.
Step 15	<code>vpn service domain-name [replace-authen-domain]</code> Example: Router(config-if-atm-vc)# vpn service domain.com replace-authen-domain	Replaces the domain field with the domain name during preauthentication.
Step 16	<code>end</code> Example: Router(config-if-atm-vc)# end	Ends the current configuration session and returns to privileged EXEC mode.

Configuring a RADIUS User Profile for L2TP Domain Screening with Global Preauthentication

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

The following example shows a user profile for user_1@xnet.net; the IP address in the profile is the LNS interface connected to the LAC.

```
[ /Radius/UserLists/Default/user_1@xnet.net ]
```

```
Name = user_1@xnet.net
```

```
Description = TEST
```

```
Password = <encrypted>
```

```
Enabled = TRUE
```

```
cisco-avpair = vpdn:tunnel-type=l2tp
```

```
cisco-avpair = vpdn:l2tp-tunnel-password=tunnel
```

```
cisco-avpair = vpdn:l2tp-hello-interval=60
```

```
cisco-avpair = vpdn:ip-addresses=103.1.1.1
```

```
cisco-avpair = vpdn:tunnel-id=LAC1-1
```

```
Framed-protocol = PPP
```

```
Service-Type = Outbound
```

Configuring L2TP Domain Screening with Per-VPDN Group Preauthentication

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication ppp** { default | list-name } method1 [method2...]
5. **aaa authorization** { network | exec | commands level | reverse-access | configuration } { default | list-name } method1 [method2...]
6. **vpdn enable**
7. **vpdn-group** name
8. **request-dialin**
9. **protocol l2tp**
10. **domain** domain-name
11. **exit**
12. **authen-before-forward**
13. **initiate-to ip** ip-address
14. **end**
15. **configure terminal**
16. **interface atm** interface-number
17. **ip address** ip-address mask
18. **pvc** vpi/vci
19. **encapsulation aal5snap**
20. **protocol pppoe**
21. **vpn service** domain-name [replace-authen-domain]
22. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router(config)# aaa new-model	Enables the authentication, authorization, and accounting (AAA) access control system.

	Command or Action	Purpose
Step 4	<p>aaa authentication ppp {default list-name} method1 [method2...]</p> <p>Example: Router(config)# aaa authentication ppp default local</p>	Specifies using local authentication for PPP authentication.
Step 5	<p>aaa authorization {network exec commands level reverse-access configuration} {default list-name} method1 [method2...]</p> <p>Example: Router(config)# aaa authorization network default local</p>	<p>Specifies running authorization for all network-related service requests and uses local authentication as the default method for authorization.</p> <p>This command is required for the AAA server to provide VPDN attributes.</p>
Step 6	<p>vpdn enable</p> <p>Example: Router(config)# vpdn enable</p>	Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database or on a remote authorization server (home gateway), if one is present.
Step 7	<p>vpdn-group name</p> <p>Example: Router(config)# vpdn-group l2tp</p>	Creates a VPDN group and associates a name with it.
Step 8	<p>request-dialin</p> <p>Example: Router(config-vpdn)# request-dialin</p>	Configures the VPDN group to request an L2TP dial-in tunnel.
Step 9	<p>protocol l2tp</p> <p>Example: Router(config-vpdn-req-in)# protocol l2tp</p>	Specifies the tunneling protocol to be used by the VPDN group.
Step 10	<p>domain domain-name</p> <p>Example: Router(config-vpdn-req-in)# domain screen.com</p>	Specifies the domain name of users who will be forwarded to the tunnel server.
Step 11	<p>exit</p> <p>Example: Router(config-vpdn-req-in)# exit</p>	Returns to VPDN configuration mode.
Step 12	<p>authen-before-forward</p> <p>Example: Router(config-vpdn)# authen-before-forward</p>	Enables authentication of dial-in L2TP sessions associated with this VPDN group before the sessions are forwarded to the tunnel server (per-VPDN group preauthentication).
Step 13	<p>initiate-to ip ip-address</p> <p>Example: Router(config-vpdn)# initiate-to ip 2.2.2.2</p>	Specifies an IP address to be used for L2TP tunneling.

	Command or Action	Purpose
Step 14	end Example: Router(config-vpdn)# end	Returns to privileged EXEC mode.
Step 15	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 16	interface atm interface-number Example: Router(config)# interface atm 4/0	Defines an ATM interface.
Step 17	ip address ip-address mask Example: Router(config-if)# ip address 3.0.0.2 255.255.0.0	Sets the primary IP address for this interface.
Step 18	pvc vpi/vci Example: Router(config-if)# pvc 1/20	Enters ATM VC configuration mode for the interface identified by this virtual path identifier/virtual channel identifier pair.
Step 19	encapsulation aal5snap Example: Router(config-if-atm-vc)# encapsulation aal5snap	Configures the encapsulation type for this PVC range. The global default encapsulation option is aal5snap .
Step 20	protocol pppoe Example: Router(config-if-atm-vc)# protocol pppoe	Enables PPP over Ethernet sessions for this PVC.
Step 21	vpn service domain-name [replace-authen-domain] Example: Router(config-if-atm-vc)# vpn service domain.com replace-authen-domain	Replaces the domain field with the domain name during preauthentication.
Step 22	end Example: Router(config-if-atm-vc)# end	Ends the current configuration session and returns to privileged EXEC mode.

Configuration Examples for L2TP Domain Screening

This section provides the following configuration examples:

- [L2TP Domain Screening with Global Preauthentication: Example, page 12](#)
- [L2TP Domain Screening with Per-VPDN Group Preauthentication: Example, page 14](#)

L2TP Domain Screening with Global Preauthentication: Example

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

```
Router# show running-config
!
.
.
.
hostname esr1_client
.
.
.
aaa new-model
!
aaa authentication login mylist enable line
aaa authentication ppp default group radius
aaa authorization network default group radius
!
aaa nas port extended
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip host zeppelin-2 1.0.0.253
!
vpdn enable
vpdn authen-before-forward
vpdn ip udp ignore checksum
vpdn search-order domain
!
vpdn-group 1

    accept-dialin
    protocol pppoe
    virtual-template 1
    pppoe limit per-mac 2
    pppoe limit per-vc 2
    pppoe limit per-vlan 2
    pppoe limit max-sessions 2
    !
    ppp hold-queue 8000
    no virtual-template snmp
    !
.
.
.
!
interface Loopback1
    no ip address
    !
interface FastEthernet0/0/0
```

```
ip address 23.5.11.7 255.255.0.0
speed 100
full-duplex
hold-queue 4096 in
hold-queue 4096 out
!
interface GigabitEthernet1/0/0
no ip address
negotiation auto
!
!
interface ATM4/0/0.101 multipoint
atm pppatm passive
range pvc 52/101 52/101
encapsulation aal5autoppp Virtual-Template1
!
pvc-in-range 52/101
vpn service znet.net1 replace-authen-domain
!
!
interface ATM5/0/0
no ip address
no ip mroute-cache
no atm pxf queuing
atm clock INTERNAL
no atm auto-configuration
no atm ilmi-keepalive
no atm address-registration
no atm ilmi-enable
!
interface ATM5/0/0.101 multipoint
atm pppatm passive
range pvc 51/101 51/101
encapsulation aal5autoppp Virtual-Template1
!
pvc-in-range 51/101
vpn service znet.net1 replace-authen-domain
!
!
.
.
.
radius-server attribute nas-port format d
radius-server host 23.5.6.100 auth-port 1645 acct-port 1646
radius-server retransmit 4
radius-server timeout 15
radius-server key cisco
!
control-plane
!

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

L2TP Domain Screening with Per-VPDN Group Preauthentication: Example

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

```

Router# show running-config
!
.
.
hostname esr1_client
.
.
aaa new-model
!
!
aaa authentication login mylist enable line
aaa authentication ppp default local
aaa authorization network default local
!
aaa nas port extended
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip host zeppelin-2 1.0.0.253
!
!
vpdn enable
vpdn ip udp ignore checksum
vpdn search-order domain
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
 pppoe limit per-mac 2
 pppoe limit per-vc 2
 pppoe limit per-vlan 2
 pppoe limit max-sessions 2
!
!
vpdn-group LAC_1
 request-dialin
  protocol l2tp
  domain znet.net1
 initiate-to ip 103.1.1.1
 local name LAC1-1
 authen-before-forward
 l2tp tunnel password 0 tunnel
!
ppp hold-queue 8000
no virtual-template snmp
username LAC1-1 nopassword
username LNS1-1 nopassword
username user_1_1@znet.net1 password 0 sanfran_1_1
.
.
.
!
interface ATM4/0/0.101 multipoint
 atm pppatm passive

```

```

range pvc 52/101 52/101
  encapsulation aal5autoppp Virtual-Template1
!
pvc-in-range 52/101
  vpn service znet.net1 replace-authen-domain
!
!
interface ATM5/0/0
  no ip address
  no ip mroute-cache
  no atm pxf queuing
  atm clock INTERNAL
  no atm auto-configuration
  no atm ilmi-keepalive
  no atm address-registration
  no atm ilmi-enable
!
interface ATM5/0/0.101 multipoint
  atm pppatm passive
  range pvc 51/101 51/101
    encapsulation aal5autoppp Virtual-Template1
  !
  pvc-in-range 51/101
    vpn service znet.net1 replace-authen-domain
  !
.
.
.
radius-server attribute nas-port format d
!
control-plane
!
call admission limit 90
!
.
.
.
end

```

Additional References

The following sections provide references related to the L2TP Domain Screening feature.

Related Documents

Related Topic	Document Title
Layer 2 Tunnel Protocol	<i>Layer 2 Tunnel Protocol</i> feature module
Commands for dial-in technologies	<i>Cisco IOS Dial Technologies Command Reference</i>
Configuring RADIUS	<i>Cisco IOS Security Configuration Guide, Release 12.2</i>

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

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

Command Reference

This section documents modified commands only.

- [vpn service](#)

vpn service

To configure a static domain name, use the **vpn service** command in ATM VC, ATM VC class or VC class configuration mode or in PVC range configuration mode. To remove a static domain name, use the **no** form of this command.

vpn service *domain-name* [**replace-authen-domain**]

no vpn service *domain-name* [**replace-authen-domain**]

Syntax Description

<i>domain-name</i>	Static domain name.
replace-authen-domain	(Optional) Specifies that when a static name is configured and VPDN preauthentication is configured, the domain name specified for VPN service replaces the domain field in the username for authentication.

Defaults

No default behavior or values

Command Modes

ATM VC configuration
ATM VC class configuration
PVC range configuration

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.
12.3(7)X17	The replace-authen-domain keyword was added and this command was integrated into Cisco IOS Release 12.2(7)X17.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **vpn service** command in a permanent virtual circuit (PVC), VC class configuration, or PVC range configuration so that PPP over ATM (PPPoA) or PPP over Ethernet over ATM (PPPoEoA) sessions in those PVCs will be forwarded according to the domain name supplied, without starting PPP.

To replace the VPN service domain name with the domain name from the username during preauthentication, use this command with the **replace-authen-domain** keyword, in conjunction with the **vpdn authen-before-forward** command.

Examples

In the following partial example, VPDN group 1 is selected for PPPoA session forwarding based on the domain name example.com:

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain example.com
 initiate-to ip 10.1.1.1 priority 1
```

```

.
.
.
interface ATM1/0.1 multipoint
 pvc 101
  encapsulation aal5mux ppp virtual-Template 1
  vpn service example.net

```

In the following partial example using the **replace-authen-domain** keyword, the domain field is replaced by the domain name during preauthentication:

```

vpdn-group 1
 request-dialin
  protocol l2tp
  domain example.net
  authen-before-forward
  initiate-to ip 10.1.1.1 priority 1
.
.
.
interface atm 4/0
 ip address 3.0.0.2 255.255.0.0
 pvc 1/20
 encapsulation aal5mux ppp virtual-Template 1
  vpn service example.net replace-authen-domain

```

Related Commands

Command	Description
vpdn authen-before-forward	Enables authentication of all dial-in L2TP sessions before the sessions are forwarded to the tunnel server (global preauthentication).

Glossary

L2TP—Layer 2 Tunnel Protocol. An Internet Engineering Task Force (IETF) standards track protocol defined in RFC 2661 that provides tunneling of PPP. Based upon the best features of L2F (Layer 2 Forwarding Protocol) and PPTP (Point-to-Point Tunneling Protocol), L2TP provides an industry-wide interoperable method of implementing VPDN.

LNS—L2TP network server. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP access concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC. Analogous to the Layer 2 Forwarding (L2F) home gateway (HGW).

LAC—L2TP access concentrator. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP network server (LNS). The LAC sits between an LNS and a remote system and forwards packets to and from each. Packets sent from the LAC to the LNS require tunneling with the L2TP protocol. The connection from the LAC to the remote system is either local or a PPP link.

NAS—Network access server. Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the public switched telephone network (PSTN)).

VPDN—Virtual private dial-up network. Also known as virtual private dial network. A VPDN is a network that extends remote access to a private network using a shared infrastructure. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) to extend the Layer 2 and higher parts of the network connection from a remote user across an internet service provider (ISP) network to a private network. VPDNs are a cost effective method of establishing a long-distance, point-to-point connection between remote dial users and a private network.

VPN—Virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

