



L2TP Tunnel Service Authorization Enhancements

This feature module describes enhancements to the current method of L2TP tunnel service authorization. It includes information on the benefits of the enhancements, supported platforms, related documents, and configuration information.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 2
- Configuration Tasks, page 3
- Configuration Examples, page 6
- Command Reference, page 8
- Glossary, page 11

Feature Overview

These enhancements enable the L2TP access concentrator (LAC) to conduct static or dynamic tunnel service authorization. A static domain name can be configured on the ATM PVC port to override the domain name supplied by the client. If a static domain name is not configured, the LAC conducts dynamic tunnel service authorization, which now includes two steps.

1. **Domain Preauthorization**—The LAC checks the client-supplied domain name against an authorized list configured on the RADIUS server for each PVC. If successful, the LAC proceeds to tunnel service authorization. If domain preauthorization fails, the LAC attempts PPP authentication/authorization for local termination.
2. **Tunnel Service Authorization**—The user profile on the RADIUS server provides a list of domains accessible to the user, enabling tunnel service authorization for the client-supplied domain. If successful, the LAC establishes an L2TP tunnel.

Benefits

Selecting Tunnels by Virtual Connection

Static tunnel service authorization enables all PPP sessions originating from a particular PVC to be sent to the same L2TP tunnel.

Supporting Unstructured Usernames

By configuring static domain names, usernames without domain names can undergo tunnel service authorization.

Preventing Arbitrary Tunnel Creation

Domain preauthorization prevents users from creating tunnels to arbitrary LNSes by simply reconfiguring the domains on the client equipment.

Restrictions

Static tunnel service authorization does not support switched virtual channels (SVCs).

Related Documents

- *Cisco 6400 UAC Software Configuration Guide*
- *Layer 2 Tunnel Protocol* feature module
- *RADIUS VC Logging* feature module

Supported Platforms

The L2TP Tunnel Service Authorization Enhancements are supported on the node route processor (NRP) of the Cisco 6400 universal access concentrator (UAC).

Supported Standards, MIBs, and RFCs

Standards

None.

MIBs

None.

RFCs

No new or modified RFCs are supported by these feature enhancements.

Configuration Tasks

See the following sections for configuration tasks for the L2TP Tunnel Service Authorization Enhancements.

- Configuring a Static Domain Name
- Enabling Domain Preauthorization
- Configuring the LAC to Communicate with the RADIUS Server
- Configuring the RADIUS User Profile for Domain Preauthorization
- Configuring the RADIUS Service Profile for Tunnel Service Authorization

Configuring a Static Domain Name

The static domain name can be configured on the PVC or on the VC class.

To configure the static domain name on the PVC, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface atm 0/0/0[.subinterface-number] {multipoint point-to-point tag-switching}	Specifies the ATM interface and optional subinterface.
Step 2	Router(config-subif)# no ip directed-broadcast	Disables forwarding of directed broadcasts.
Step 3	Router(config-subif)# pvc [name] vpi/vci	Configures a PVC on the ATM interface or subinterface.
Step 4	Router(config-if-atm-vc)# encapsulation aal5mux ppp Virtual-Template number	Sets encapsulation as PPP. Also specifies the virtual template interface to use to clone the new virtual access interface.
Step 5	Router(config-if-atm-vc)# vpn service domain-name	Configures static domain name on the PVC.

To configure the static domain name on the VC class, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# vc-class atm vc-class-name	Create and name a map class.
Step 2	Router(config-vc-class)# encapsulation aal5mux ppp Virtual-Template number	Sets encapsulation as PPP. Also specifies the virtual template interface to use to clone the new virtual access interface.
Step 3	Router(config-vc-class)# vpn service domain-name	Configures static domain name on the VC class.
Step 4	Router(config-vc-class)# exit	Returns to global configuration mode.
Step 5	Router(config)# interface atm 0/0/0[.subinterface-number] {multipoint point-to-point tag-switching}	Specifies the ATM interface and optional subinterface.
Step 6	Router(config-subif)# class-int vc-class-name	Applies VC class to all VCs on the ATM interface or subinterface.

Verifying the Static Domain Name

To verify that you successfully configured the static domain name, use the **show running-config EXEC** command.

Enabling Domain Preauthorization

To enable the LAC to perform domain authorization before tunneling, enter the following command in global configuration mode:

Command	Purpose
Router(config)# vpdn authorize domain	Enables domain preauthorization.

Verifying Domain Preauthorization

To check that you successfully enabled domain preauthorization, use the **show running-config EXEC** command.

Configuring the LAC to Communicate with the RADIUS Server

To enable the LAC to communicate properly with the RADIUS server for tunnel service authorization, enter the following commands in global configuration mode:

Command	Purpose
Router(config)# radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number]	Specifies the RADIUS server host.
Router(config)# radius-server attribute nas-port format d	Selects the ATM VC extended NAS port format for RADIUS accounting features.
Router(config)# radius-server key string	Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
Router(config)# radius-server vsa send authentication	Configures the LAC to recognize and use vendor-specific attributes.

Verifying LAC and RADIUS Server Communication

To check that you successfully configured the LAC to communicate properly with the RADIUS server for tunnel service authorization, use the **show running-config EXEC** command.

Configuring the RADIUS User Profile for Domain Preauthorization

To enable domain preauthorization, use the following configuration in the user profile on the RADIUS server.

RADIUS Entry	Purpose
nas-port: <i>ip-address:slot/subslot/port/vpi.vci</i>	Configures the NAS port username for domain preauthorization.
Password = "cisco"	Sets the fixed password.
User-Service-Type = Outbound-User	Configures the service-type as outbound.
Cisco-AVpair = "vpdn:vpn-domain-list=domain1, domain2,..."	Specifies the domains accessible to the user.

Syntax Description

<i>ip-address</i>	Management IP address of the NSP.
<i>slot/subslot/port</i>	Specify ATM interface.
<i>vpi.vci</i>	VPI and VCI values for the PVC.
<i>domain</i>	Domain to configure as accessible to the user.

Verifying the RADIUS User Profile for Domain Preauthorization

To verify the RADIUS user profile, refer to the user documentation for your RADIUS server.

Configuring the RADIUS Service Profile for Tunnel Service Authorization

To enable tunnel service authorization, use the following configuration in the service profile on the RADIUS server.

RADIUS Entry	Purpose
domain Password "cisco"	Sets the fixed password.
User-Service-Type = Outbound-User	Configures the service-type as outbound.
Cisco-AVpair = "vpdn:tunnel-id=name"	Specifies the name of the tunnel that must match the LNS's VPDN terminate-from hostname.
Cisco-AVpair = "vpdn:l2tp-tunnel-password=secret"	Specifies the secret (password) for L2TP tunnel authentication.
Cisco-AVpair = "vpdn:tunnel-type=l2tp"	Specifies Layer 2 Tunnel Protocol.
Cisco-AVpair = "vpdn:ip-addresses=ip-address"	Specifies IP address of LNS.

Syntax Description

<i>domain</i>	Client-supplied domain.
<i>name</i>	Name of the tunnel that must match the LNS's VPDN terminate-from hostname statement.
<i>secret</i>	Secret (password) used for L2TP tunnel authentication.
<i>ip-address</i>	IP address of LNS.

Verifying the RADIUS Service Profile for Tunnel Service Authorization

To verify the RADIUS service profile, refer to the user documentation for your RADIUS server.

Configuration Examples

This section provides the following configuration examples:

- Static Domain Name Configuration on a PVC
- Static Domain Name Configuration on a VC Class
- Domain Preauthorization Configuration on the LAC
- Domain Preauthorization RADIUS User Profile
- Tunnel Service Authorization Configuration on the LAC
- Tunnel Service Authorization RADIUS Service Profile

Static Domain Name Configuration on a PVC

The following example shows the static domain names “net1.com” and “net2.com” assigned to PVCs on an ATM interface. All PPP sessions originating from PVC 30/33 are sent to the “net1.com” L2TP tunnel, while all PPP sessions originating from PVC 30/34 are sent to the “net2.com” tunnel.

```
!
interface ATM 0/0/0.33 multipoint
  pvc 30/33
    encapsulation aal5cisco ppp Virtual-Template1
    vpn service net1.com
  !
  pvc 30/34
    encapsulation aal5cisco ppp Virtual-Template1
    vpn service net2.com
  !
```

Static Domain Name Configuration on a VC Class

In the following example, the static domain name “net.com” is assigned to a VC class. The VC class is then assigned to the VCs on an ATM subinterface.

```
!
vc-class ATM MyClass
  encapsulation aal5cisco ppp Virtual-Template1
  vpn service net.com
!
interface ATM 0/0/0.99 multipoint
  class-int MyClass
  no ip directed-broadcast
  pvc 20/40
  pvc 30/33
  !
```

Domain Preauthorization Configuration on the LAC

The following example shows the configuration necessary for the 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

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  
  }  
}
```

Tunnel Service Authorization Configuration on the LAC

The following example shows the configuration necessary for the LAC to participate in tunnel service authorization:

```
!  
aaa new-model  
aaa authorization network default local group radius  
!  
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  
!
```

Tunnel Service Authorization RADIUS Service Profile

The following example shows a tunnel service authorization RADIUS service profile:

```
user = net1.com{
  profile_id = 45
  profile_cycle = 18
  member = me
  radius=Cisco {
    check_items= {
      2=cisco
    }
  }
  reply_attributes= {
    9,1="vpdn:tunnel-id=LAC-1"
    9,1="vpdn:l2tp-tunnel_password=MySecret"
    9,1="vpdn:tunnel-type=l2tp"
    9,1="vpdn:ip-addresses=10.10.10.10"
    6=5
  }
}
```

Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

- **vpdn authorize domain**
- **vpn service**

vpdn authorize domain

To enable domain preauthorization on a NAS, use the **vpdn authorize domain** global configuration command. 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.

Defaults Domain preauthorization is disabled by default.

Command Modes Global configuration

Command History	Release	Modification
	12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.

Examples The following example enables domain preauthorization:

```
vpdn authorize domain
```

vpn service

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

vpn service *domain-name*

no vpn service *domain-name*

Syntax Description

<i>domain-name</i>	Static domain name.
--------------------	---------------------

Defaults

No default behavior or values.

Command Modes

ATM VC or VC class

Command History

Release	Modification
12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.

Examples

The following example configures the static domain name of net.com:

```
vpn service net.com
```

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 and PPTP, L2TP provides an industry-wide interoperable method of implementing VPDN.

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 requires tunneling with the L2TP protocol as defined in this document. The connection from the LAC to the remote system is either local or a PPP link.

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).

NAS—Network access server. A device providing local network access to users across a remote access network such as the PSTN. A NAS can also serve as a LAC, LNS, or both.

RADIUS—Remote Access Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

VC—Virtual channel. Logical circuit created to ensure reliable communication between two network devices. A VC is defined by a VPI/VCI pair, and can be either permanent (PVC) or switched (SVC).

