Tunnel Authentication via RADIUS on LNS

The Tunnel Authentication via RADIUS on LNS feature allows a Layer 2 Tunnel Protocol (L2TP) Network Server (LNS) to perform remote authentication and authorization with RADIUS on incoming L2TP network access server (NAS) dial-in connection requests. This feature also allows the L2TP NAS to perform remote authentication and authorization with RADIUS on incoming L2TP tunnel server dial-out connection requests.

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

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

Configuration Information

Configuration information is included in the "Configuring AAA for VPDNs" module in the *Cisco IOS VPDN Configuration Guide*, Release 12.4T, at the following URL:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tvpdn_c/vpc2auht.htm

Command Reference

This section documents modified commands.

- **vpdn tunnel authorization network**
- **vpdn tunnel authorization password**
- **vpdn tunnel authorization virtual-template**

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 of local tunnel authentication and authorization, 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 will perform authentication locally.

Command Modes

Global configuration

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 will be 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 will occur.

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

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 theLayer 2 Tunnel Protocol (L2TP) network access server (NAS) or 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 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 will be used for cloning on the local router. Valid values range from 1 to 200.

Command Default

No default virtual template is specified.

Command Modes

Global configuration

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.