Tunnel Authentication via RADIUS on Tunnel Terminator

Last Updated: July 18, 2011

The Tunnel Authentication via RADIUS on Tunnel Terminator feature allows tunnel authentication and authorization to occur through a remote RADIUS server instead of local configuration on the tunnel terminator. Thus, users no longer have to configure L2TP access concentrator (LAC) or Layer 2 Tunneling Protocol (L2TP) network server (LNS) data in a virtual private dialup network (VPDN) group when an LNS or LAC is configured for incoming dialin or dialout L2TP tunnel termination; this information can now be added to a remote RADIUS server, providing a more manageable and scalable solution for L2TP tunnel authentication and authorization on the tunnel terminator.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Tunnel Authentication via RADIUS on Tunnel Terminator

Before configuring this feature, you should define a RADIUS server group. For information on completing this task, refer to the chapter "Configuring RADIUS " in the *Cisco IOS Security Configuration Guide: Securing User Services*

Note The service-type in the RADIUS user's profile for the tunnel initiator should always be set to "Outbound."

Restrictions for Tunnel Authentication via RADIUS on Tunnel Terminator

The Tunnel Authentication via RADIUS on Tunnel Terminator feature is applicable only to L2TP; that is, protocols such as (Layer 2 Forwarding) L2F and Point-to-Point Tunneling Protocol (PPTP) are not supported.

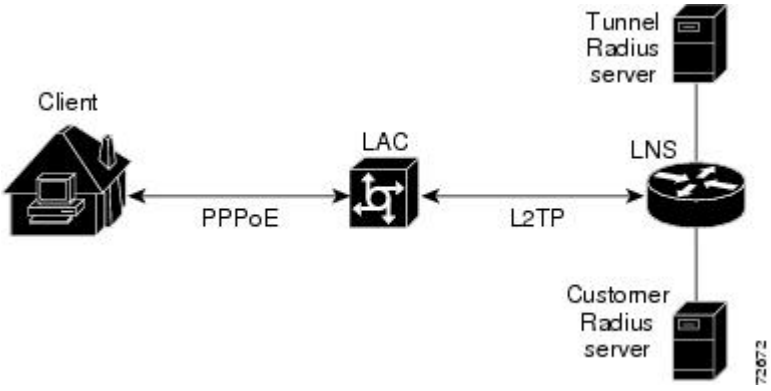
Information About Tunnel Authentication via RADIUS on Tunnel Terminator

The Tunnel Authentication via RADIUS on Tunnel Terminator feature allows the LNS to perform remote authentication and authorization with RADIUS on incoming LAC dialin connection requests. This feature also allows the L2TP LAC to perform remote authentication and authorization with RADIUS on incoming L2TP LNS dialout connection requests.

Before the introduction of this feature, the LNS could only perform L2TP tunnel authentication and authorization locally. These processes can be difficult to maintain across numerous LNSs, especially if the number of VPDN groups is large, because the LAC information must be configured under the VPDN group configurations of the LNS. Remote RADIUS authentication and authorization allows users to store the LAC configurations on the RADIUS server, thereby avoiding the need to store information locally. Thus, the new LAC information can be added to the RADIUS server as necessary, and the group of LNSs can authenticate and authorize by using a common user database on RADIUS.

The figure below and the corresponding steps explain how this feature works.

Figure 1



- After the LNS receives a start-control-connection request (SCCRQ), it starts tunnel authentication and submits a request to RADIUS with the LAC hostname and the dummy password “cisco.” (If the LNS determines that authorization should be performed locally, it will search the VPDN group configurations.)

Note To change the dummy password, use the **vpdn tunnel authorization password** command.

- If the password sent by the LNS matches the password that is configured in the RADIUS server, the server will return attribute 90 (Tunnel-Client-Auth-ID) and attribute 69 (Tunnel-Password) after the LAC information is located. Otherwise, the RADIUS server replies back with an access-reject, and the LNS drops the tunnel.
- The LNS will check for the following attribute information from the RADIUS reply:
  - Attribute 90 (Tunnel-Client-Auth-ID), which is used as the LAC hostname. If this attribute does not match the LAC hostname, the tunnel will be dropped.
  - Attribute 69 (Tunnel-Password), which is used for the L2TP CHAP-like authentication shared secret. This attribute is compared against the LAC challenge attribute-value pair (AVP) that was received in the SCCRQ. If this attribute does not match the AVP, the tunnel will be dropped.
- If both attributes match, the L2TP tunnel will be established. Thereafter, you can proceed with PPP negotiation and authentication with the remote client.

Note PPP remote authentication is done to a potential different customer RADIUS server by a separate access-request/access-accept sequence. The tunnel authorization may be done by a different tunnel RADIUS server.

- New RADIUS Attributes, page 3

New RADIUS Attributes

To help implement this feature, the following two new Cisco-specific RADIUS attributes have been introduced:

- Cisco:Cisco-Avpair = “vpdn:dout-dialer = <LAC dialer number>”--Specifies which LAC dialer to use on the LAC for a dialout configuration.
- Cisco:Cisco-Avpair = “vpdn:vpdn-vtemplate = <vtemplate number>”--Specifies the virtual template number that will be used for cloning on the LNS for a dialin configuration. (This attribute is the RADIUS counterpart for the virtual-template under the vpdn-group configuration.)

How to Configure Tunnel Authentication via RADIUS on Tunnel Terminator

- Configuring the LNS or LAC for Remote RADIUS Tunnel Authentication and Authorization, page 4
- Verifying Remote RADIUS Tunnel Authentication and Authorization Configurations, page 5
- Verifying Remote RADIUS Tunnel Authentication and Authorization Configurations, page 6

Configuring the LNS or LAC for Remote RADIUS Tunnel Authentication and Authorization

The following task is used to configure an LNS or LAC for incoming dialin or dialout L2TP tunnel termination.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization network** {**default** | *list-name*} *method1* [*method2...*]
4. **vpdn tunnel authorization network** {*method-list-name* | **default**}
5. **vpdn tunnel authorization virtual-template** *vtemplate-number*
6. **vpdn tunnel authorization password** *password*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authorization network** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authorization network mymethodlist group VPDN-Group`	Defines an AAA authorization method list for network services.
Step 4	**vpdn tunnel authorization network** {*method-list-name* | **default**} **Example:** `Router(config)# vpdn tunnel authorization network mymethodlist`	Specifies the AAA authorization method list that will be used for remote tunnel hostname-based authorization. • If the *list-name* argument was specified in the **aaa authorization** command, you use that list name here. • If the default keyword was specified in the **aaa authorization** command, you must choose that keyword, which specifies the default authorization methods that are listed with the **aaa authorization** command here.

	Command or Action	Purpose
Step 5	**vpdn tunnel authorization virtual-template** *vtemplate-number* **Example:** `Router(config)# vpdn tunnel authorization virtual-template 10`	(Optional) Selects the default virtual template from which to clone virtual access interfaces.
Step 6	**vpdn tunnel authorization password** *password* **Example:** `Router(config)# vpdn tunnel authorization password cisco`	(Optional) Configures a "dummy" password for the RADIUS authorization request to retrieve the tunnel configuration that is based on the remote tunnel hostname. **Note** If this command is not enabled, the password will always be "cisco."

Verifying Remote RADIUS Tunnel Authentication and Authorization Configurations

To verify that the L2TP tunnel is up, use the **show vpdn tunnel** command in EXEC mode. One tunnel and one session must be set up.

```
Router# show vpdn tunnel
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions VPDN Group
4571  61568 csidtw13 est    10.0.195.4      1701  1        ?
LocID RemID TunID Intf          Username              State  Last Chg
4     11    4571  Vi4.1         csidtw9@cisco.com       est    00:02:29
%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels
To verify that the AAA authorization RADIUS server is configured on the LNS and that the
LNS can receive attributes 90 and 69 from the RADIUS server, perform the following steps:
```

SUMMARY STEPS

1. Enable the **debug radius** command on the LNS.
2. Enable the **show logging**command on the LNS and ensure that "access-accept" is in the output and that attributes 90 and 69 can be seen in the RADIUS reply.

DETAILED STEPS

Step 1 Enable the **debug radius** command on the LNS.

Step 2 Enable the **show logging**command on the LNS and ensure that "access-accept" is in the output and that attributes 90 and 69 can be seen in the RADIUS reply.

Example:

```
00:32:56: RADIUS: Received from id 21645/5 172.19.192.50:1645, Access-Accept, len 81
```

```
00:32:56: RADIUS:  authenticator 73 2B 1B C2 33 71 93 19 - 62 AC 3E BE 0D 13 14 85
00:32:56: RADIUS:  Service-Type        [6]   6   Outbound                  [5]
00:32:56: RADIUS:  Tunnel-Type         [64]  6   00:L2TP                   [3]
00:32:56: RADIUS:  Tunnel-Medium-Type  [65]  6   00:IPv4                   [1]
00:32:56: RADIUS:  Tunnel-Client-Auth-I[90]  6   00:"csidtw13"
00:32:56: RADIUS:  Tunnel-Password     [69]  8   *
00:32:56: RADIUS:  Vendor, Cisco       [26]  29
00:32:56: RADIUS:   Cisco AVpair       [1]   23  "vpdn:vpdn-vtemplate=1"
```

Verifying Remote RADIUS Tunnel Authentication and Authorization Configurations

To verify that the L2TP tunnel has been established and that the LNS can perform PPP negotiation and authentication with the remote client, perform the following steps:

SUMMARY STEPS

1. Enable the **debug ppp negotiation** and **debug ppp authentication** commands on LNS.
2. Enable the **show logging** command on LNS and observe that LNS receives a PPP CHAP challenge and then sends a PPP CHAP “SUCCESS” to the client.
3. After PPP authentication is successful, observe from the debug output that PPP negotiation has started, that the LNS has received LCP (IPCP) packets, and that negotiation is successful.

DETAILED STEPS

Step 1 Enable the **debug ppp negotiation** and **debug ppp authentication** commands on LNS.

Step 2 Enable the **show logging** command on LNS and observe that LNS receives a PPP CHAP challenge and then sends a PPP CHAP “SUCCESS” to the client.

Example:

```
00:38:50: ppp3 PPP: Received LOGIN Response from AAA = PASS
00:38:50: ppp3 PPP: Phase is FORWARDING, Attempting Forward
00:38:50: Vi4.1  Tnl/Sn4571/4 L2TP: Session state change from wait-for-service-selection to
established
00:38:50: Vi4.1 PPP: Phase is AUTHENTICATING, Authenticated User
00:38:50: Vi4.1 CHAP: O SUCCESS id 1 len 4
```

Step 3 After PPP authentication is successful, observe from the debug output that PPP negotiation has started, that the LNS has received LCP (IPCP) packets, and that negotiation is successful.

Example:

```
00:38:50: Vi4.1 IPCP: State is Open
00:38:50: Vi4.1 IPCP: Install route to 200.1.1.4
```

Configuration Examples for Tunnel Authentication via RADIUS on Tunnel Terminator

L2TP Network Server Configuration Example

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

```
! Define a RADIUS server group
aaa group server radius VPDN-group
 server 64.102.48.91 auth-port 1645 acct-port 1646
!
! RADIUS configurations only
aaa authorization network mymethodlist group VPDN-Group
vpdn tunnel authorization network mymethodlist
vpdn tunnel authorization virtual-template 10
```

RADIUS User Profile for Remote RADIUS Tunnel Authentication Example

The following are examples of RADIUS user profiles for the LNS to terminate L2TP tunnels from a LAC. In the first user profile, the final line is optional if the **vpdn tunnel authorization virtual-template** command is used. Also, the first RADIUS user profile is for L2TP dialin, and the second RADIUS user profile is for L2TP dialout.

The service-type in the RADIUS user's profile for the tunnel initiator should always be set to "Outbound."

```
csidtw13  Password = "cisco"
        Service-Type = Outbound,
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Client-Auth-ID = :0:"csidtw13",
        Tunnel-Password = :0:"cisco"
        Cisco:Cisco-Avpair = "vpdn:vpdn-vtemplate=1"
csidtw1 Password = "cisco"
        Service-Type = Outbound,
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Client-Auth-ID = :0:"csidtw1",
        Tunnel-Password = :0:"cisco"
        Cisco:Cisco-Avpair = "vpdn:dout-dialer=2"
```

Additional References

The following sections provide references related to the Tunnel Authentication via RADIUS on Tunnel Terminator feature.

Related Documents

Related Topic	Document Title
VPNs	*Cisco IOS VPDN Configuration Guide* , Release 12.4T
RADIUS Attributes	*Cisco IOS Security Configuration Guide: Securing User Services* , Release 15.0.

Standards

Standard	Title
None.	--

MIBs

MIB	MIBs Link
None.	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
RFC 2868	RADIUS Attributes for Tunnel Protocol Support

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Tunnel Authentication via RADIUS on Tunnel Terminator

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

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

Table 1 Feature Information for Tunnel Authentication via RADIUS on Tunnel Terminator

Feature Name	Releases	Feature Information
Tunnel Authentication via RADIUS on Tunnel Terminator	12.2(15)B 12.3(4)T	The Tunnel Authentication via RADIUS on Tunnel Terminator feature allows tunnel authentication and authorization to occur through a remote RADIUS server instead of local configuration on the tunnel terminator. In 12.2(15)B, this feature was introduced on the Cisco 6400 series, Cisco 7200 series, and Cisco 7400 series. In 12.3(4)T, this feature was integrated into the Cisco IOS. The following commands were introduced or modified: **vpdn tunnel authorization network**, **vpdn tunnel authorization password**, **vpdn tunnel authorization virtual-template**.

Glossary

L2TP --Layer 2 Tunnel Protocol. A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

LAC --L2TP access concentrator. A network access server (NAS) to which the client directly connects and through which PPP frames are tunneled to the L2TP network server (LNS). The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. The LAC may tunnel any

protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F network access server.

LNS --L2TP network server. A termination point for L2TP tunnels and an access point where PPP frames are processed and passed to higher layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single medium over which L2TP tunnels arrive. The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.