



RADIUS Tunnel Attribute Extensions

Feature History

Release	Modification
12.1(5)T	This feature was introduced.
12.2(4)B3	This feature was integrated into Cisco IOS Release 12.2(4)B3.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.

This feature module describes the RADIUS Tunnel Attribute Extensions feature. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 6](#)
- [Glossary, page 7](#)

Feature Overview

The RADIUS Tunnel Attribute Extensions feature introduces RADIUS attribute 90 (Tunnel-Client-Auth-ID) and RADIUS attribute 91 (Tunnel-Server-Auth-ID). Both attributes help support the provision of compulsory tunneling in virtual private networks (VPNs) by allowing the user to specify authentication names for the network access server (NAS) and the RADIUS server.

How It Works

Once a NAS has set up communication with a RADIUS server, you can enable a tunneling protocol. Some applications of tunneling protocols are voluntary, but others involve compulsory tunneling; that is, a tunnel is created without any action from the user and without allowing the user any choice in the matter. In those cases, new RADIUS attributes are needed to carry the tunneling information from the NAS to the RADIUS server to establish authentication. These new RADIUS attributes are listed in [Table 1](#).

**Note**

In compulsory tunneling, any security measures in place apply only to traffic between the tunnel endpoints. Encryption or integrity protection of tunneled traffic must not be considered as a replacement for end-to-end security.

Table 1 RADIUS Tunnel Attributes

Number	IETF RADIUS Tunnel Attribute	Equivalent TACACS+ Attribute	Supported Protocols	Description
90	Tunnel-Client-Auth-ID	tunnel-id	<ul style="list-style-type: none"> Layer 2 Forwarding (L2F) Layer 2 Tunneling Protocol (L2TP) 	Specifies the name used by the tunnel initiator (also known as the NAS ¹) when authenticating tunnel setup with the tunnel terminator.
91	Tunnel-Server-Auth-ID	gw-name	<ul style="list-style-type: none"> Layer 2 Forwarding (L2F) Layer 2 Tunneling Protocol (L2TP) 	Specifies the name used by the tunnel terminator (also known as the Home Gateway ²) when authenticating tunnel setup with the tunnel initiator.

1. When L2TP is used, the NAS is referred to as an L2TP access concentrator (LAC).
2. When L2TP is used, the Home Gateway is referred to as an L2TP network server (LNS).

RADIUS attribute 90 and RADIUS attribute 91 are included in the following situations:

- If the RADIUS server accepts the request and the desired authentication name is different from the default, they must be included it.
- If an accounting request contains Acct-Status-Type attributes with values of either start or stop and pertains to a tunneled session, they should be included in.

Benefits

The RADIUS Tunnel Attribute Extensions feature allows you to specify a name (other than the default) of the tunnel initiator and the tunnel terminator. Thus, you can establish a higher level of security when setting up VPN tunneling.

Restrictions

Your RADIUS server must support tagged attributes to use RADIUS tunnel attributes 90 and 91.

Related Documents

The following documents provide information related to the RADIUS Tunnel Attribute Extensions feature:

- The chapters “Configuring Authentication” and “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*, Release 12.2
- The appendix “RADIUS Attributes” in the *Cisco IOS Security Configuration Guide*, Release 12.2

- The chapter “Configuring Virtual Private Networks” in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

Supported Platforms

Cisco IOS Release 12.1(5)T Only

- AS5300
- AS5800

Cisco IOS Releases 12.2(4)B3 and 12.2(13)T Only

Cisco 6400-NRP-1

Cisco 6400-NRP-2

Cisco 6400-NRP-2SV

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

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://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

Prerequisites

To use RADIUS attributes 90 and 91, you must complete the following tasks:

- Configure your NAS to support AAA.
- Configure your NAS to support RADIUS.
- Configure your NAS to support VPN.

Configuration Tasks

None

Verifying RADIUS Attribute 90 and RADIUS Attribute 91

To verify that RADIUS attribute 90 and RADIUS attribute 91 are being sent in access accepts and accounting requests, use the following command in privileged EXEC mode:

Command	Purpose
Router# <code>debug radius</code>	Displays information associated with RADIUS. The output of this command shows whether attribute 90 and attribute 91 are being sent in access accepts and accounting requests.

Configuration Examples

This section provides the following configuration examples:

- [L2TP Network Server \(LNS\) Configuration Example](#)
- [RADIUS User Profile with RADIUS Tunneling Attributes 90 and 91 Example](#)

L2TP Network Server (LNS) Configuration Example

The following example shows how to configure the LNS with a basic L2F and L2TP configuration using RADIUS tunneling attributes 90 and 91:

```

aaa new-model
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2f-cli-auth-id password 0 l2f-cli-pass
username l2f-svr-auth-id password 0 l2f-svr-pass
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2f
virtual-template 1
terminate-from hostname l2f-cli-auth-id
local name l2f-svr-auth-id
!
vpdn-group 2
accept-dialin
protocol l2tp
virtual-template 2
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface Ethernet1/0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache

```

```

!
interface Virtual-Template1
ip unnumbered Ethernet1/0
ppp authentication pap
!
interface Virtual-Template2
ip unnumbered Ethernet1/0
ppp authentication pap
!
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>
!

```

RADIUS User Profile with RADIUS Tunneling Attributes 90 and 91 Example

The following is an example of a RADIUS user profile that includes RADIUS tunneling attributes 90 and 91. This entry supports two tunnels, one for L2F and the other for L2TP. The tag entries with :1 support L2F tunnels, and the tag entries with :2 support L2TP tunnels.

```

cisco.com Password = "cisco", Service-Type = Outbound
  Service-Type = Outbound,
  Tunnel-Type = :1:L2F,
  Tunnel-Medium-Type = :1:IP,
  Tunnel-Client-Endpoint = :1:"10.0.0.2",
  Tunnel-Server-Endpoint = :1:"10.0.0.3",
  Tunnel-Client-Auth-Id = :1:"l2f-cli-auth-id",
  Tunnel-Server-Auth-Id = :1:"l2f-svr-auth-id",
  Tunnel-Assignment-Id = :1:"l2f-assignment-id",
  Cisco-Avpair = "vpdn:nas-password=l2f-cli-pass",
  Cisco-Avpair = "vpdn:gw-password=l2f-svr-pass",
  Tunnel-Preference = :1:1,
  Tunnel-Type = :2:L2TP,
  Tunnel-Medium-Type = :2:IP,
  Tunnel-Client-Endpoint = :2:"10.0.0.2",
  Tunnel-Server-Endpoint = :2:"10.0.0.3",
  Tunnel-Client-Auth-Id = :2:"l2tp-cli-auth-id",
  Tunnel-Server-Auth-Id = :2:"l2tp-svr-auth-id",
  Tunnel-Assignment-Id = :2:"l2tp-assignment-id",
  Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
  Tunnel-Preference = :2:2

```

Command Reference

No new or modified Cisco IOS commands were added for this feature.

Glossary

Layer 2 Forwarding (L2F)—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.

Layer 2 Tunnel Protocol (L2TP)—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.

L2TP access concentrator (LAC)—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.

L2TP network server (LNS)—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.

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

tunnel—A virtual pipe between the L2TP access concentrator (LAC) and L2TP network server (LNS) that can carry multiple PPP sessions.

virtual private network (VPN)—A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the L2TP network server (LNS) instead of the L2TP access concentrator (LAC).

