RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

The RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements feature allows the hostname of the network access server (NAS) to be specified--rather than the IP address of the NAS--in RADIUS attribute 66 (Tunnel-Client-Endpoint). This feature makes it easier for users to remember a hostname instead of a numerical IP address, and helps disguise the numerical IP address of the NAS.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

A Cisco platform that supports VPDN is required. See the Glossary, on page 4 for more information about VPDN.

Restrictions for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

Your Cisco device must be running a Cisco software image that supports virtual private dialup networks (VPDNs).

Information About RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

How the RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements are Used

Virtual Private Networks (VPNs) use Layer 2 Forwarding (L2F) or Layer 2 Tunnel Protocol (L2TP) tunnels to tunnel the link layer of high-level protocols (for example, PPP or asynchronous High-Level Data Link Control (HDLC)). Internet service providers (ISPs) configure their NASs to receive calls from users and forward the calls to the customer tunnel server. Usually, the ISP maintains only information about the tunnel server--the tunnel endpoint. The customer maintains the IP addresses, routing, and other user database functions of the tunnel server users. RADIUS attribute 66 provides the customer with the ability to specify the hostname of the NAS instead of the IP address of the NAS.

Note L2F is not supported on the Cisco ASR 1000 Series Aggregation Services Routers.

How to Configure RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

There are no configuration tasks associated with support for the RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements.

Configuration Examples for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

Setting Up the RADIUS Profile for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements Example

The following example shows a configuration that allows the user to specify the hostname of the NAS using RADIUS attribute 66 (Tunnel-Client-Endpoint) in the RADIUS profile:

```
cisco-avpair = vpdn:l2tp-cm-local-window-size=1024
cisco-avpair = vpdn:l2tp-nosession-timeout=30
cisco-avpair = vpdn:l2tp-cm-retransmit-retries=10
cisco-avpair = vpdn:l2tp-cm-min-timeout=2
cisco-avpair = vpdn:l2tp-hello-interval=60
Service-Type = outbound
Tunnel-Assignment-Id_tag1 = ISP1
Tunnel-Client-Auth-Id_tag1 = LAC1
Tunnel-Client-Endpoint_tag1 = 10.0.0.2
Tunnel-Medium-Type_tag1 = IPv4
Tunnel-Password_tag1 = tunnel1
Tunnel-Server-Auth-Id_tag1 = LNS1
Tunnel-Server-Endpoint_tag1 = 10.0.0.1
Tunnel-Type_tag1 = l2tp
```

Additional References

The following sections provide references related to the RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements feature.

Related Documents

Related Topic	Document Title
RADIUS attribute 66	*Cisco IOS XE Security Configuration Guide: Configuring User Services* , Release 2
Security commands	*Cisco IOS Security Command Reference*

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 XE software 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 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 RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

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 RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements

Feature Name	Releases	Feature Information
RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.9S	The RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements feature allows the hostname of the network access server (NAS) to be specified—rather than the IP address of the NAS—in RADIUS attribute 66 (Tunnel-Client-Endpoint). This feature makes it easier for users to remember a hostname instead of a numerical IP address, and helps disguise the numerical IP address of the NAS. In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Glossary

L2F--Layer 2 Forwarding Protocol. Protocol that supports the creation of secure virtual private dialup networks over the Internet.

L2TP--Layer 2 Tunnel Protocol. Protocol that is one of the key building blocks for virtual private networks in the dial access space and is endorsed by Cisco and other internetworking industry leaders. This protocol

combines the best of Cisco's Layer 2 Forwarding (L2F) protocol and Microsoft's Point-to-Point Tunneling Protocol (PPTP).

Layer 2 Forwarding Protocol--See L2F.

Layer 2 Tunnel Protocol--See L2TP.

Point-to-Point Protocol--See PPP.

PPP--Point-to-Point Protocol. Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

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

Remote Authentication Dial-In User Service--See RADIUS.

virtual private dialup network--See VPDN.

VPDN--virtual private dialup network. A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPDNs 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).