



RADIUS Tunnel Preference for Load Balancing and Fail-Over

Feature History for RADIUS Tunnel Preference for Load Balancing and Fail-Over

Release	Modification
12.2(4)T	This feature was introduced.
12.2(11)T	This feature was implemented on Cisco access server platforms.
12.2(27)SBA	This feature was integrated into Cisco IOS Release 12.2(27)SBA.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Feature Overview, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 5](#)
- [Configuration Tasks, page 5](#)
- [Configuration Example, page 5](#)
- [Command Reference, page 5](#)
- [Glossary, page 6](#)



Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2001, 2002, 2005 Cisco Systems, Inc. All rights reserved.

Feature Overview

The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature provides load balancing and fail-over virtual private dialup network (VPDN) home gateway (HGW) groups in a standardized fashion. This feature introduces new software functionality; no new command is associated with this feature.

Industry-Standard Rather Than Proprietary Attributes

Until Cisco IOS Release 12.2(4)T, load balancing and fail-over functionality for a Layer 2 Tunnel Protocol network server (LNS) was provided by the Cisco proprietary Vendor Specific Attribute (VSA). In a multivendor network environment, using VSA on a RADIUS server can cause interoperability issues among network access servers (NASs) manufactured by different vendors. Even though some RADIUS server implementations can send VSAs that the requesting NAS can understand, the user still must maintain different VSAs for the same purpose in a single-service profile.

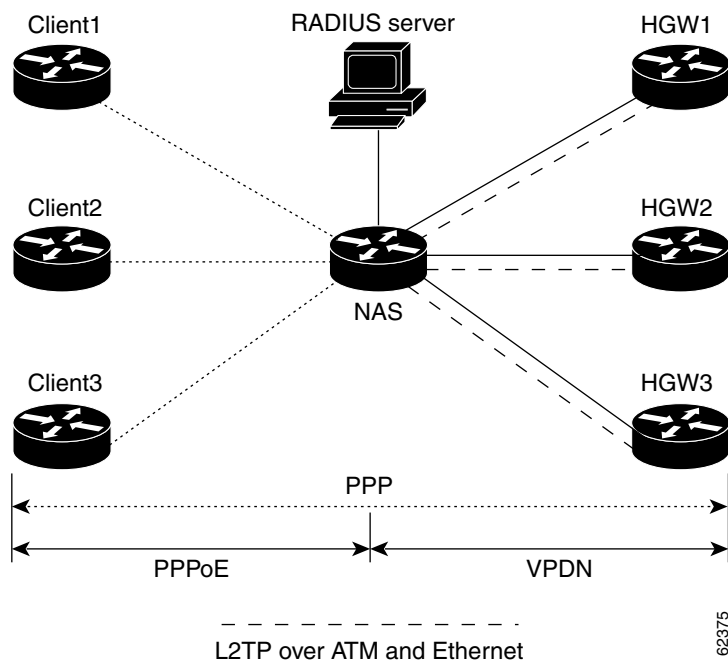
A consensus regarding the tunnel attributes that are to be used in a multivendor network environment is defined in RFC 2868. In RFC 2868, Tunnel-Server-Endpoint, in conjunction with the Tunnel-Medium-Type, specifies the address to which the NAS should initiate a new session. If multiple Tunnel-Server-Endpoint attributes are defined in one tagged attribute group, they are interpreted as equal-cost load-balancing HGWs.

The Tunnel-Preference attribute defined in RFC 2868 can be used as a measure to form load balancing and fail-over HGW groups. When the Tunnel-Preference values of different tagged attribute groups are the same, the Tunnel-Server-Endpoint of those attribute groups is considered to have the same priority unless otherwise specified. When the Tunnel-Preference values of some attribute groups are higher (they have a lower preference) than other attribute groups, their Tunnel-Server-Endpoint attributes will have higher priority values. When an attribute group has a higher priority value, that attribute group will be used for fail-over in case the attribute groups with lower priority values are unavailable for the connections.

Until Cisco IOS Release 12.2(4)T, a specially formatted string would be transported within a Cisco VSA “vpdn:ip-addresses” string to a NAS for the purpose of HGW load balancing and fail-over. For example, 10.0.0.1 10.0.0.2 10.0.0.3/2.0.0.1 2.0.0.2 would be interpreted as IP addresses 10.0.0.1, 10.0.0.2, and 10.0.0.3 for the first group for load balancing. New sessions are projected to these three addresses based on the least-load-first algorithm. This algorithm uses its local knowledge to select an HGW that has the least load to initiate the new session. In this example, the addresses 2.0.0.1 and 2.0.0.2 in the second group have a lower priority and are applicable only when all HGWs specified in the first group fail to respond to the new connection request, thereby making 2.0.0.1 and 2.0.0.2 the fail-over addresses. See the section “[Configuration Example](#)” for an example of how to configure these fail-over addresses in a RADIUS tunnel profile.

Load Balancing and Fail-Over in a Multivendor Network

The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature was designed for large multivendor networks that use VPDN Layer 2 tunnels over WAN links such as ATM and Ethernet, such as the configuration shown in [Figure 1](#).

Figure 1 Typical Load Balancing and Fail-Over in a Multivendor Network

In the configuration shown in [Figure 1](#), the NAS uses tunnel profiles downloaded from the RADIUS server to establish VPDN Layer 2 tunnels for load balancing and fail-over. The Point-to-Point over Ethernet (PPPoE) protocol is used as the client to generate PPP sessions.

Benefits

The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature provides industry-standard load balancing and fail-over functionality for an LNS, rather than requiring the use of a Cisco proprietary VSA. The feature conforms to the tunnel attributes that are to be used in a multivendor network environment as defined in RFC 2868, thereby eliminating interoperability issues among NASs manufactured by different vendors.

Restrictions

The following restrictions and limitations apply to the RADIUS Tunnel Preference for Load Balancing and Fail-Over feature:

- This feature does not support VPDN dial-out networks; it is designed only for dial-in applications.
- The maximum number of LNSs allowed in the network is 1550, which is 50 per tag attribute group and a limit of 31 tags.
- This feature requires a RADIUS server implementation to support RFC 2868.

Related Features and Technologies

The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature is used in VPDNs. Additionally, familiarity with the following technologies and protocols is recommended:

- ATM
- Ethernet
- L2TP and L2F
- PPP and PPPoE
- RADIUS servers

See the next section for a list of documentation that describes these technologies and protocols.

Related Documents

- “Basic Dial-in VPDN Configuration Using VPDN Groups” at http://www.cisco.com/warp/public/793/access_dial/2.html
- *Cisco IOS Dial Technologies Command Reference*, Release 12.2
- *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2, the chapters in the part “Virtual Templates, Profiles, and Networks”
- *Cisco IOS Security Command Reference*, Release 12.2
- *Cisco IOS Security Configuration Guide*, Release 12.2, the chapter “Configuring RADIUS” and the appendix “RADIUS Attributes”
- “Which VPN Solution is Right for You?” at http://www.cisco.com/warp/public/707/which_vpn.html
- *Cisco IOS Wide-Area Networking Command Reference*, Release 12.2
- *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2, the chapter “Configuring Broadband Access: PPP and Routed Bridge Encapsulation”

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

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

RFCs

RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

Prerequisites

Configuring VPDNs and HGW groups is beyond the scope of this document. Refer to the documentation listed in the section [“Related Documents”](#) for the tasks and commands to configure these types of networks.

Configuration Tasks

This feature has no new configuration commands; however, see the next section for an example of how to implement the RADIUS Tunnel Preference for Load Balancing and Fail-Over feature in a RADIUS tunnel profile.

Configuration Example

The following example shows how to create RADIUS tunnel profiles:

```
net3 Password = "cisco" Service-Type = Outbound
    Tunnel-Type = :0:L2TP,
    Tunnel-Medium-Type = :0:IP,
    Tunnel-Server-Endpoint = :0:"1.1.3.1",
    Tunnel-Assignment-Id = :0:"1",
    Tunnel-Preference = :0:1,
    Tunnel-Password = :0:"welcome"

    Tunnel-Type = :1:L2TP,
    Tunnel-Medium-Type = :1:IP,
    Tunnel-Server-Endpoint = :1:"1.1.5.1",
    Tunnel-Assignment-Id = :1:"1",
    Tunnel-Preference = :1:1,
    Tunnel-Password = :1:"welcome"

    Tunnel-Type = :2:L2TP,
    Tunnel-Medium-Type = :2:IP,
    Tunnel-Server-Endpoint = :2:"1.1.4.1",
    Tunnel-Assignment-Id = :2:"1",
    Tunnel-Preference = :2:1,
    Tunnel-Password = :2:"welcome"

    Tunnel-Type = :3:L2TP,
    Tunnel-Medium-Type = :3:IP,
    Tunnel-Server-Endpoint = :3:"1.1.6.1",
    Tunnel-Assignment-Id = :3:"1",
    Tunnel-Preference = :3:1,
    Tunnel-Password = :3:"welcome"
```

The section [“Feature Overview”](#) describes how fail-over addresses are selected in these profiles. The section [“Related Documents”](#) lists documentation that describes how to create RADIUS tunnel profiles.

Command Reference

None

Glossary

HGW—home gateway. A gateway that terminates Layer 2 tunneling protocols such as L2TP.

home gateway—See HGW.

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.

L2TP network server—See LNS.

Layer 2 Tunnel Protocol—See L2TP.

LNS—L2TP network server. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the NAS or 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 access server. Analogous to the Layer 2 Forwarding (L2F) HGW.

NAS—network access server. Cisco platform or collection of platforms that interfaces between the packet world (the Internet, for example) and the circuit world (the public switched telephone network, for example).

network access server—See NAS.

Request for Comments—See RFCs.

RFCs—Request for Comments. A series of notes about the Internet collected by the Internet Engineering Task Force (IETF). Started in 1969, the IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture. RFCs define many aspects of computer communication, focusing on networking protocols, procedures, programs, and concepts.

virtual private dialup network—See VPDN.

VPDN—virtual private dialup network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright ©2001, 2002, 2005 Cisco Systems, Inc. All rights reserved.