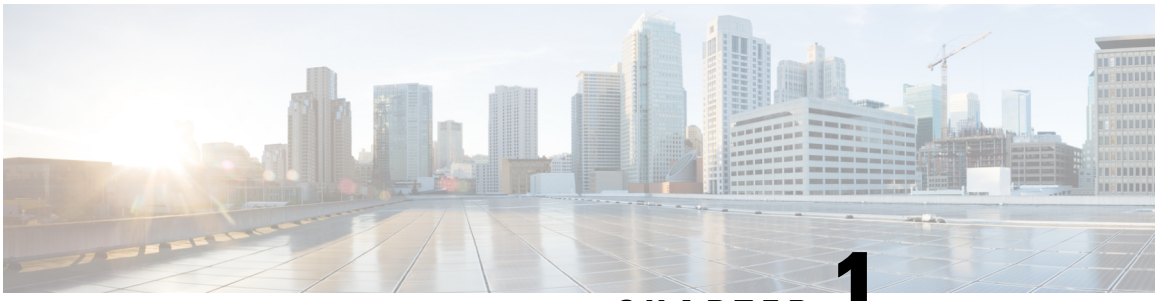
RADIUS Configuration Guide, Cisco IOS XE Gibraltar 16.12.x

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

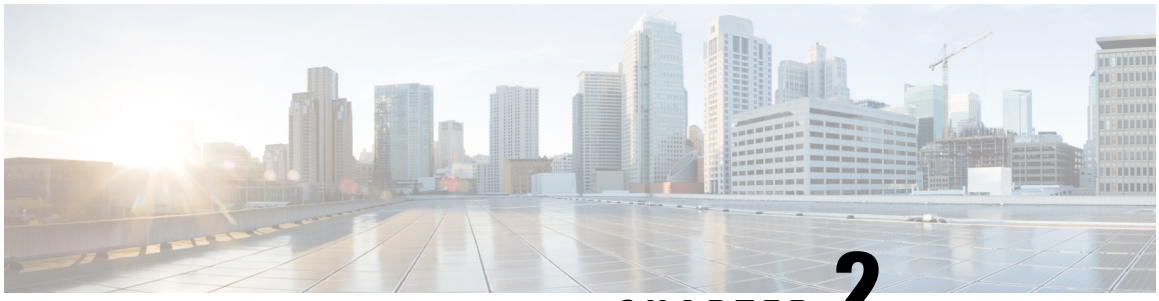
Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.



CHAPTER 2

Configuring RADIUS

The RADIUS security system is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco devices and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

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

To configure RADIUS on your Cisco device or access server, you must perform these tasks:

- Use the **aaa new-model** global configuration command to enable Authentication, Authorization, and Accounting (AAA). AAA must be configured if you plan to use RADIUS.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication.
- Use **line** and **interface** commands to enable the defined method lists to be used.

Restrictions for RadSec (RADIUS Security)

RadSec is not supported on any of the Cisco enterprise routing platforms.

Information About RADIUS

RADIUS Network Environments

Cisco supports RADIUS under its authentication, authorization, and accounting (AAA) security paradigm. RADIUS can be used with other AAA security protocols such as TACACS+, Kerberos, and local username lookup. RADIUS is supported on all Cisco platforms, but some RADIUS-supported features run only on specified platforms.

RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a smart card access control system. In one case, RADIUS has been used with Enigma's security cards to validate users and grant access to network resources.
- Networks already using RADIUS. You can add a Cisco device with RADIUS to the network. This might be the first step when you make a transition to a TACACS+ server.
- Networks in which a user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as PPP. For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using the IP address 10.2.3.4 and the defined access list is started.
- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, and bytes) used during the session. An ISP might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.
- Networks that support preauthentication. Using the RADIUS server in your network, you can configure AAA preauthentication and set up the preauthentication profiles. Preauthentication enables service providers to better manage ports using their existing RADIUS solutions, and to efficiently manage the use of shared resources to offer differing service-level agreements.

RADIUS is not suitable in these network security situations:

- Multiprotocol access environments. RADIUS does not support the following protocols:
  - AppleTalk Remote Access (ARA)

- NetBIOS Frame Control Protocol (NBFCP)
- NetWare Asynchronous Services Interface (NASI)
- X.25 Packet Assemblers/Disassemblers (PAD) connections

- Device-to-device situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires RADIUS authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

RADIUS Operation

When a user attempts to log in and authenticate to an access server using RADIUS, the following steps occur:

1. The user is prompted to enter the username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of the following responses from the RADIUS server:
   a. ACCEPT—The user is authenticated.
   b. CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
   c. CHANGE PASSWORD—A request is issued by the RADIUS server, asking the user to select a new password.
   d. REJECT—The user is not authenticated and is prompted to reenter the username and password, or access is denied.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

- Services that the user can access, including connections such as Telnet, rlogin, or local-area transport (LAT), and services such as PPP, Serial Line Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IP address, access list, and user timeouts.

RADIUS Attributes

The network access server monitors the RADIUS authorization and accounting functions defined by RADIUS attributes in each user profile:

Vendor-Proprietary RADIUS Attributes

An Internet Engineering Task Force (IETF) standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server. Some vendors, nevertheless, have extended the RADIUS attribute set in a unique way. Cisco software supports a subset of vendor-proprietary RADIUS attributes.

RADIUS Tunnel Attributes

RADIUS is a security server AAA protocol originally developed by Livingston, Inc. RADIUS uses attribute value (AV) pairs to communicate information between the security server and the network access server.

RFC 2138 and RFC 2139 describe the basic functionality of RADIUS and the original set of IETF-standard AV pairs used to send AAA information. Two IETF standards, "RADIUS Attributes for Tunnel Protocol Support" and "RADIUS Accounting Modifications for Tunnel Protocol Support," extend the IETF-defined set of AV pairs to include attributes specific to VPNs. These attributes are used to carry the tunneling information between the RADIUS server and the tunnel initiator.

RFC 2865 and RFC 2868 extend the IETF-defined set of AV pairs to include attributes specific to compulsory tunneling in VPNs by allowing the user to specify authentication names for the network access server and the RADIUS server.

Cisco devices and access servers support new RADIUS IETF-standard virtual private dialup network (VPDN) tunnel attributes.

Preauthentication on a RADIUS Server

RADIUS attributes are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. In addition to configuring preauthentication on your Cisco device, you must set up the preauthentication profiles on the RADIUS server.

RADIUS Profile for DNIS or CLID Preauthentication

To configure the RADIUS preauthentication profile, use the Dialed Number Identification Service (DNIS) or Calling Line Identification (CLID) number as the username, and use the password defined in the **dnis** or **clid** command as the password.

Note The preauthentication profile must have "outbound" as the service type because the password is predefined on the network access server (NAS). Setting up the preauthentication profile in this manner prevents users from trying to log in to the NAS with the username of the DNIS number, CLID number, or call type and an obvious password. The "outbound" service type is also included in the Access-Request packet sent to the RADIUS server.

RADIUS Profile for Call Type Preauthentication

To set up the RADIUS preauthentication profile, use the call type string as the username, and use the password defined in the **ctype** command as the password. The table below lists the call type strings that can be used in the preauthentication profile.

Table 1: Call Type Strings Used in Preauthentication

Call Type String	ISDN Bearer Capabilities
digital	Unrestricted digital, restricted digital.

Call Type String	ISDN Bearer Capabilities
speech	Speech, 3.1 kHz audio, 7 kHz audio. **Note** This is the only call type available for channel-associated signaling (CAS) .
v.110	Anything with the V.110 user information layer.
v.120	Anything with the V.120 user information layer.

Note The preauthentication profile must have “outbound” as the service type because the password is predefined on the NAS. Setting up the preauthentication profile in this manner prevents users from trying to log in to the NAS with the username of the DNIS number, CLID number, or call type and an obvious password. The “outbound” service type is also included in the Access-Request packet sent to the RADIUS server and should be a checkin item if the RADIUS server supports checkin items.

RADIUS Profile for Preauthentication Enhancements for Callback

Callback allows remote network users such as telecommuters to dial in to the NAS without being charged. When callback is required, the NAS hangs up the current call and dials the caller back. When the NAS performs the callback, only information for the outgoing connection is applied. The rest of the attributes from the preauthentication access-accept message are discarded.

Note The destination IP address is not required to be returned from the RADIUS server.

The following example shows a RADIUS profile configuration with a callback number of 555-0101 and the service type set to outbound. The cisco-avpair = “preauth:send-name=<string>” uses the string “user1” and the cisco-avpair = “preauth:send-secret=<string>” uses the password “cisco.”

```
5550101 password = “cisco”, Service-Type = Outbound
Service-Type = Callback-Framed
Framed-Protocol = PPP,
Dialback-No = “5550119”
Class = “ISP12”
cisco-avpair = “preauth:send-name=user1”
cisco-avpair = “preauth:send-secret=cisco”
```

RADIUS Profile for a Remote Hostname Used for Large-Scale Dial-Out

The following example protects against accidentally calling a valid telephone number but accessing the wrong device by providing the name of the remote device, for use in large-scale dial-out:

```
5550101 password = "PASSWORD1", Service-Type = Outbound
       Service-Type = Callback-Framed
       Framed-Protocol = PPP,
       Dialback-No = "5550190"
       Class = "ISP12"
       cisco-avpair = "preauth:send-name=user1"
```

```
cisco-avpair = "preauth:send-secret=PASSWORD1"
cisco-avpair = "preauth:remote-name=Device2"
```

RADIUS Profile for Modem Management

When DNIS, CLID, or call type preauthentication is used, the affirmative response from the RADIUS server might include a modem string for modem management in the NAS through vendor-specific attribute (VSA) 26. The modem management VSA has this syntax:

```
cisco-avpair = “preauth:modem-service=modem min-speed <
x
> max-speed <
y
>
modulation <
z
> error-correction <
a
> compression <
b
>”
```

The table below lists the modem management string elements within the VSA.

Table 2: Modem Management String

Command	Argument
min-speed	300 to 56000, any
max-speed	300 to 56000, any
modulation	K56Flex, v22bis, v32bis, v34, v90, any
error-correction	lapm, mnp4
compression	mnp5, v42bis

When the modem management string is received from the RADIUS server in the form of a VSA, the information is passed to the Cisco software and applied on a per-call basis. Modem ISDN channel aggregation (MICA) modems provide a control channel through which messages can be sent during the call setup time. Hence, this modem management feature is supported only with MICA modems. This feature is not supported with Microcom modems.

RADIUS Profile for Subsequent Authentication

If preauthentication passes, you can use vendor-proprietary RADIUS attribute 201 (Require-Auth) in the preauthentication profile to determine whether subsequent authentication is performed. If attribute 201, returned in the access-accept message, has a value of 0, subsequent authentication is not performed. If attribute 201 has a value of 1, subsequent authentication is performed as usual.

Attribute 201 has this syntax:

```
cisco-avpair = “preauth:auth-required=<
n
>”
```

where <*n*> has the same value range as attribute 201 (that is, 0 or 1).

If attribute 201 is missing in the preauthentication profile, a value of 1 is assumed, and subsequent authentication is performed.

Note Before you can perform subsequent authentication, you must set up a regular user profile in addition to a preauthentication profile.

RADIUS Profile for Subsequent Authentication Types

If you specified subsequent authentication in the preauthentication profile, you must also specify the authentication types to be used for subsequent authentication. To specify the authentication types allowed in subsequent authentication, use this VSA:

```
cisco-avpair = "preauth:auth-type=<
string
>"
```

The table below lists the allowed values for the <*string*> element.

Table 3: <string> Element Values

String	Description
chap	Requires the username and password for the Challenge-Handshake Authentication Protocol (CHAP) for PPP authentication.
ms-chap	Requires the username and password for the MS-CHAP for PPP authentication.
pap	Requires the username and password for the Password Authentication Protocol (PAP) for PPP authentication.

To specify that multiple authentication types are allowed, you can configure more than one instance of this VSA in the preauthentication profile. The sequence of the authentication type VSAs in the preauthentication profile is significant because it specifies the order of authentication types to be used in the PPP negotiation.

This VSA is a per-user attribute and replaces the authentication type list in the **ppp authentication** interface configuration command.

Note You should use this VSA only if subsequent authentication is required because it specifies the authentication type for subsequent authentication.

RADIUS Profile to Include the Username

If only preauthentication is used to authenticate a call, the NAS could be missing a username when it brings up the call. RADIUS can provide a username for the NAS to use through RADIUS attribute 1 (User-Name) or through a VSA returned in the Access-Accept packet. The VSA for specifying the username has this syntax:

```
cisco-avpair = "preauth:username=<
```

```
string
>”
```

If no username is specified, the DNIS number, CLID number, or call type is used, depending on the last preauthentication command configured (for example, if **clid** was the last preauthentication command configured, the CLID number is used as the username).

If subsequent authentication is used to authenticate a call, there might be two usernames: one provided by RADIUS and one provided by the user. In this case, the username provided by the user overrides the one contained in the RADIUS preauthentication profile. The username provided by the user is used for both authentication and accounting.

RADIUS Profile for Two-Way Authentication

In the case of two-way authentication, the calling networking device must authenticate the NAS. The PAP username and password or CHAP username and password need not be configured locally on the NAS. Instead, the username and password can be included in the Access-Accept messages for preauthentication.

Note Do not configure the **ppp authentication** command with the **radius** command.

To set up PAP, do not configure the **ppp pap sent-name password** command on the interface. The VSAs “preauth:send-name” and “preauth:send-secret” are used as the PAP username and PAP password for outbound authentication.

For CHAP, “preauth:send-name” is used not only for outbound authentication but also for inbound authentication. For a CHAP inbound case, the NAS uses the name defined in “preauth:send-name” in the challenge packet to the caller networking device. For a CHAP outbound case, both “preauth:send-name” and “preauth:send-secret” are used in the response packet.

The following example shows a configuration that specifies two-way authentication:

```
5550101 password = "PASSWORD2", Service-Type = Outbound
Service-Type = Framed-User
cisco-avpair = "preauth:auth-required=1"
cisco-avpair = "preauth:auth-type=pap"
cisco-avpair = "preauth:send-name=user1"
cisco-avpair = "preauth:send-secret=PASSWORD2"
class = "<some class>"
```

Note Two-way authentication does not work when resource pooling is enabled.

RADIUS Profile to Support Authorization

If only preauthentication is configured, subsequent authentication is bypassed. Note that because the username and password are not available, authorization is also bypassed. However, you can include authorization attributes in the preauthentication profile to apply per-user attributes and avoid having to return subsequently to RADIUS for authorization. To initiate the authorization process, you must also configure the **aaa authorization network** command on the NAS.

You can configure authorization attributes in the preauthentication profile with one exception: the service-type attribute (attribute 6). The service-type attribute must be converted to a VSA in the preauthentication profile. This VSA has this syntax:

```
cisco-avpair = "preauth:service-type=<
n
>"
```

where <*n*> is one of the standard RFC 2865 values for attribute 6.

Note If subsequent authentication is required, the authorization attributes in the preauthentication profile are not applied.

RADIUS Authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the **aaa authentication** command, specifying RADIUS as the authentication method.

RADIUS Authorization

AAA authorization lets you set parameters that restrict a user's access to the network. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, AppleTalk Remote Access (ARA), and Telnet. Because RADIUS authorization is facilitated through AAA, you must enter the **aaa authorization** command, specifying RADIUS as the authorization method.

RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing and the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must enter the **aaa accounting** command, specifying RADIUS as the accounting method.

RADIUS Login-IP-Host

To enable the network access server (NAS) to attempt more than one login host when trying to connect a dial-in user, you can enter as many as three Login-IP-Host entries in the user's profile on the RADIUS server. The following example shows that three Login-IP-Host instances are configured for the user *user1*, and that TCP-Clear is used for the connection:

```
user1 Password = xyz
        Service-Type = Login,
        Login-Service = TCP-Clear,
        Login-IP-Host = 10.0.0.0,
        Login-IP-Host = 10.2.2.2,
        Login-IP-Host = 10.255.255.255,
        Login-TCP-Port = 23
```

The order in which the hosts are entered is the order in which they are attempted. Use the **ip tcp synwait-time** command to set the number of seconds that the NAS waits before trying to connect to the next host on the list; the default is 30 seconds.

Your RADIUS server might permit more than three Login-IP-Host entries; however, the NAS supports only three hosts in Access-Accept packets.

RADIUS Prompt

To control whether user responses to Access-Challenge packets are echoed to the screen, you can configure the Prompt attribute in the user profile on the RADIUS server. This attribute is included only in Access-Challenge packets. The following example shows the Prompt attribute set to No-Echo, which prevents the user's responses from echoing:

```
user1 Password = xyz
Service-Type = Login,
Login-Service = Telnet,
Prompt = No-Echo,
Login-IP-Host = 172.31.255.255
```

To allow user responses to echo, set the attribute to Echo. If the Prompt attribute is not included in the user profile, responses are echoed by default.

This attribute overrides the behavior of the **radius-server challenge-noecho** command configured on the access server. For example, if the access server is configured to suppress echoing, but the individual user profile allows echoing, the user responses are echoed.

Note If you want to use the Prompt attribute, your RADIUS server must be configured to support Access-Challenge packets.

Vendor-Specific RADIUS Attributes

The IETF standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor ID is 9, and the supported option has vendor type 1, which is named "cisco-avpair." The value is a string with this format:

```
protocol : attribute sep value *
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization; protocols that can be used include IP, Internetwork Packet Exchange (IPX), VPDN, VoIP, Secure Shell (SSH), Resource Reservation Protocol (RSVP), Serial Interface Processor (SIP), AirNet, and Outbound. "Attribute" and "value" are an appropriate AV pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes, allowing the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes Cisco's "multiple named ip address pools" feature to be activated during IP authorization (during PPP's Internet Protocol Control Protocol (IPCP) address assignment):

```
cisco-avpair= ”ip:addr-pool=first“
```

If you insert an “*”, the AV pair “ip:addr-pool=first” becomes optional. Note that any AV pair can be made optional:

```
cisco-avpair= ”ip:addr-pool*first“
```

The following example shows how to cause a user logging in from a network access server to have immediate access to EXEC commands:

```
cisco-avpair= ”shell:priv-lvl=15“
```

Other vendors have their own unique vendor IDs, options, and associated VSAs.

Static Routes and IP Addresses on the RADIUS Server

Some vendor-proprietary implementations of RADIUS let the user define static routes and IP pool definitions on the RADIUS server instead of on each individual network access server in the network. Each network access server then queries the RADIUS server for static route and IP pool information.

To have the Cisco device or access server query the RADIUS server for static routes and IP pool definitions when the device starts up, use the **radius-server configure-nas** command.

Because the **radius-server configure-nas** command is performed when the Cisco devcie starts up, it does not take effect until you enter a **copy system:running-config nvram:startup-config** command.

How to Configure RADIUS

Configuring a Device for Vendor-Proprietary RADIUS Server Communication

Although an IETF standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco software supports a subset of vendor-proprietary RADIUS attributes.

To configure RADIUS (whether vendor-proprietary or IETF compliant), you must use the **radius-server** commands to specify the host running the RADIUS server daemon and the secret text string it shares with the Cisco device. To identify that the RADIUS server is using a vendor-proprietary implementation of RADIUS, use the **radius-server host non-standard** command. Vendor-proprietary attributes are not supported unless you use the **radius-server host non-standard** command.

Note The **radius-server host** command is deprecated from Cisco IOS Release 15.4(2)S. To configure an IPv4 or IPv6 RADIUS server, use the **radius server** *name* command. For more information about the **radius server** command, see *Cisco IOS Security Command Reference: Commands M to R*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **radius-server vsa send** [**accounting** | **authentication**]
4. **radius server** *server-name*
5. **address ipv4** *ip-address*
6. **non-standard**
7. **key** {**0** *string* | **7** *string* | *string*}
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server vsa send** [**accounting**	**authentication**] **Example:** `Device(config)# radius-server vsa send`	Enables the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26.
Step 4	**radius server** *server-name* **Example:** `Device(config)# radius server rad1`	Specifies the name for the RADIUS server. **Note** The **radius-server host** command is deprecated from Cisco IOS Release 15.4(2)S. To configure an IPv4 or IPv6 RADIUS server, use the **radius server** *name* command. For more information about the **radius server** command, see *Cisco IOS Security Command Reference: Commands M to R*.
Step 5	**address ipv4** *ip-address* **Example:** `Device(config-radius-server)# address ipv4 10.45.1.2`	Assigns an IP address to the RADIUS server.
Step 6	**non-standard** **Example:** `Device(config-radius-server)# non-standard`	Identifies that the security server is using a vendor-proprietary implementation of RADIUS.
Step 7	**key** {**0** *string*	**7** *string*	*string*} **Example:**	Specifies the shared secret text string used between the device and the vendor-proprietary RADIUS server.

	Command or Action	Purpose
	`Device(config-radius-server)# key myRaDIUSpassword`	• The device and the RADIUS server use this text string to encrypt passwords and exchange responses.
Step 8	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Configuring a Device to Expand Network Access Server Port Information

Sometimes PPP or login authentication occurs on an interface that is different from the interface on which the call itself comes in. For example, in a V.120 ISDN call, login or PPP authentication occurs on a virtual asynchronous interface "ttt", but the call itself occurs on one of the channels of the ISDN interface.

The **radius-server attribute nas-port extended** command configures RADIUS to expand the size of the NAS-Port attribute (RADIUS IETF attribute 5) field to 32 bits. The upper 16 bits of the NAS-Port attribute display the type and number of the controlling interface; the lower 16 bits indicate the interface undergoing authentication.

Note The **radius-server attribute nas-port format** command replaces the **radius-server extended-portnames** command and the **radius-server attribute nas-port extended** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server configure-nas**
4. **radius-server attribute nas-port format**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**radius-server configure-nas** **Example:** `Device(config)# radius-server configure-nas`	(Optional) Tells the Cisco device or access server to query the RADIUS server for the static routes and IP pool definitions used throughout its domain. **Note** Because the **radius-server configure-nas** command is used when the Cisco device starts up, it does not take effect until you issue a **copy system:running-config nvram:startup-config** command.
Step 4	**radius-server attribute nas-port format** **Example:** `Device(config)# radius-server attribute nas-port format`	Expands the size of the NAS-Port attribute from 16 to 32 bits to display extended interface information.
Step 5	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Replacing the NAS-Port Attribute with the RADIUS Attribute

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation does not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 appear as NAS-Port = 20101 because of the 16-bit field size limitation associated with the RADIUS IETF NAS-Port attribute. In this case, you can replace the NAS-Port attribute with a VSA (RADIUS IETF attribute 26). Cisco's vendor ID is 9, and the Cisco-NAS-Port attribute is subtype 2. VSAs can be turned on by entering the **radius-server vsa send** command. The port information in this attribute is provided and configured using the **aaa nas port extended** command.

The standard NAS-Port attribute (RADIUS IETF attribute 5) is sent. If you do not want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. After this command is configured, the standard NAS-Port attribute is no longer sent.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **aaa nas port extended**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server vsa send** [**accounting** | **authentication**] **Example:** `Device(config)# radius-server vsa send`	Enables the network access server to recognize and use vendor-specific attributes as defined by RADIUS IETF attribute 26.
Step 4	**aaa nas port extended** **Example:** `Device(config)# aaa nas port extended`	Expands the size of the VSA NAS-Port field from 16 to 32 bits to display extended interface information.
Step 5	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Monitoring and Maintaining RADIUS

SUMMARY STEPS

1. **enable**
2. **debug radius**
3. **show radius statistics**
4. **show aaa servers**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug radius** **Example:** `Device# debug radius`	Displays information associated with RADIUS.

	Command or Action	Purpose
Step 3	**show radius statistics** **Example:** `Device# show radius statistics`	Displays the RADIUS statistics for accounting and authentication packets. **Note** Few IOS processes use ephemeral source ports for RADIUS, and the port numbers may vary every time.
Step 4	**show aaa servers** **Example:** `Device# show aaa servers`	Displays the status and number of packets that are sent to and received from all public and private AAA RADIUS servers as interpreted by the AAA Server MIB.
Step 5	**exit** **Example:** `Device# exit`	Exits the device session.

Configuration Examples for RADIUS

Example: RADIUS Authentication and Authorization

The following example shows how to configure the device to authenticate and authorize using RADIUS:

```
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

- The **aaa authentication login use-radius group radius local** command configures the device to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, **use-radius** is the name of the method list, which specifies RADIUS and then local authentication.
- The **aaa authentication ppp user-radius if-needed group radius** command configures the Cisco software to use RADIUS authentication for lines using PPP with CHAP or PAP if the user has not already been authorized. If the EXEC facility has authenticated the user, RADIUS authentication is not performed. In this example, **user-radius** is the name of the method list defining RADIUS as the if-needed authentication method.
- The **aaa authorization exec default group radius** command sets the RADIUS information that is used for EXEC authorization, autocommands, and access lists.
- The **aaa authorization network default group radius** command sets RADIUS for network authorization, address assignment, and access lists.

Example: RADIUS Authentication, Authorization, and Accounting

The following example shows a general configuration using RADIUS with the AAA command set:

```
radius-server host 10.45.1.2
radius-server key myRaDiUSpassWoRd
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem ri-is-cd
interface group-async 1
 encaps ppp
 ppp authentication pap dialins
```

The lines in this example RADIUS authentication, authorization, and accounting configuration are defined as follows:

- The **radius-server host** command defines the IP address of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list "dialins," which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.
- The **aaa authorization network default group radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage.
- The **aaa authentication login admins local** command defines another method list, "admins," for login authentication.
- The **login authentication admins** command applies the "admins" method list for login authentication.
- The **ppp authentication pap dialins** command applies the "dialins" method list to the lines specified.

Example: Vendor-Proprietary RADIUS Configuration

The following example shows a general configuration using vendor-proprietary RADIUS with the AAA command set:

Note The **radius-server host** command is deprecated from Cisco IOS Release 15.4(2)S. To configure an IPv4 or IPv6 RADIUS server, use the **radius server** *name* command. For more information about the **radius server** command, see *Cisco IOS Security Command Reference: Commands M to R*.

```
radius server myserver
radius server address ipv4 192.0.2.2
non-standard
key 7 any key
radius-server configure-nas
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
```

The lines in this RADIUS authentication, authorization, and accounting configuration example are defined as follows:

- The **non-standard** command defines the name of the RADIUS server host and identifies that this RADIUS host uses a vendor-proprietary version of RADIUS.
- The **key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **configure-nas** command defines that the Cisco device or access server queries the RADIUS server for static routes and IP pool definitions when the device first starts up.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list "dialins," which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.
- The **aaa authorization network default group radius local** command assigns an address and other network parameters to the RADIUS user.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage.
- The **aaa authentication login admins local** command defines another method list, "admins," for login authentication.

Example: Multiple RADIUS Server Entries for the Same Server IP Address

The following example shows how to configure the network access server to recognize several RADIUS host entries with the same IP address. Two different host entries on the same RADIUS server are configured for the same services—authentication and accounting. The second host entry configured acts as failover backup to the first one. (The RADIUS host entries are tried in the order they are configured.)

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2001
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
AAA and RADIUS commands	*Cisco IOS Security Command Reference*
RADIUS attributes	*RADIUS Attributes Configuration Guide* (part of the Securing User Services Configuration Library)
AAA	*Authentication, Authorization, and Accounting Configuration Guide* (part of the Securing User Services Configuration Library)
L2TP, VPN, or VPDN	*Dial Technologies Configuration Guide* and *VPDN Configuration Guide*
Modem configuration and management	*Dial Technologies Configuration Guide*
RADIUS port identification for PPP	*Wide-Area Networking Configuration Guide*

RFCs

RFC	Title
RFC 2138	*Remote Authentication Dial-In User Service (RADIUS)*
RFC 2139	*RADIUS Accounting*
RFC 2865	*RADIUS*
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*
RFC 2868	*RADIUS Attributes for Tunnel Protocol Support*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

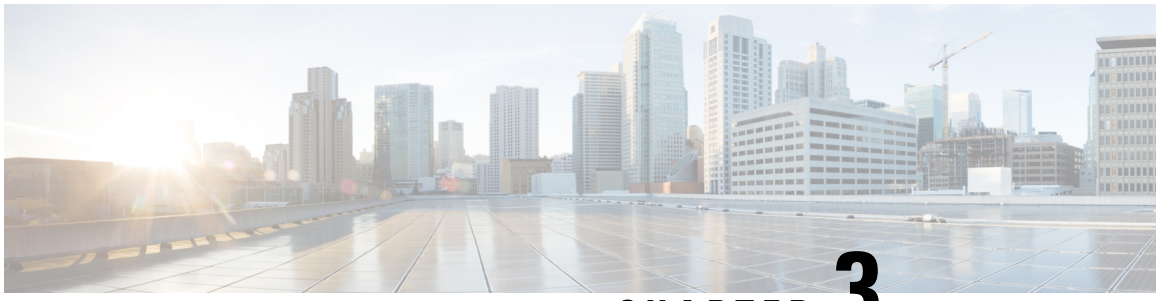
Feature Information for Configuring RADIUS

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 4: Feature Information for Configuring RADIUS

Feature Name	Releases	Feature Information
Configuring RADIUS		The RADIUS security system is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco devices and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.
RADIUS Statistics via SNMP		This feature provides statistics related to RADIUS traffic and private RADIUS servers. The following commands were introduced or modified: **show aaa servers**, **show radius statistics**.



CHAPTER 3

RADIUS for Multiple UDP Ports

RADIUS security servers are identified on the basis of their hostname or IP address, hostname and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific authentication, authorization, and accounting (AAA) service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as a failover backup to the first one. If the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services.

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 for Multiple UDP Ports

To configure RADIUS on your Cisco device or access server, you must perform these tasks:

- Use the **aaa new-model** global configuration command to enable AAA. AAA must be configured if you plan to use RADIUS.

- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication.
- Use **line** and **interface** commands to enable the defined method lists to be used.

Information About RADIUS for Multiple UDP Ports

Device-to-RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (CiscoSecure ACS), Livingston, Merit, Microsoft, or another software provider. Configuring device to RADIUS server communication can have several components:

- Hostname or IP address
- Authentication destination port
- Accounting destination port
- Timeout period
- Retransmission value
- Key string

RADIUS security servers are identified on the basis of their hostname or IP address, hostname and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as a failover backup to the first one. If the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order they are configured.)

A RADIUS server and a Cisco device use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the device.

The timeout, retransmission, and encryption key values are configurable globally for all RADIUS servers, on a per-server basis or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the device, use the three unique global commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host** command.

Note You can configure both global and per-server timeout, retransmission, and key value commands simultaneously on the same Cisco network access server. If both global and per-server functions are configured on a device, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands.

How to Configure RADIUS for Multiple UDP Ports

Configuring Device-to-RADIUS Server Communication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius server** *server-name*
4. **address ipv4** *ip-address*
5. **key** {**0** *string* | **7** *string* | *string*}
6. **retransmit** *retries*
7. **timeout** *seconds*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server rad1`	Specifies the name for the RADIUS server.
Step 4	**address ipv4** *ip-address* **Example:** `Device(config-radius-server)# address ipv4 10.45.1.2`	Assigns an IP address to the RADIUS server.
Step 5	**key** {**0** *string* | **7** *string* | *string*} **Example:** `Device(config-radius-server)# key myRaDIUSpassword`	Specifies the shared secret text string used between the device and a RADIUS server. **Note** In this step, the encryption key value is configured globally for all RADIUS servers.

	Command or Action	Purpose
		• Use the **0** *string* option to configure an unencrypted shared secret. Use the **7** *string* option to configure an encrypted shared secret.
Step 6	**retransmit** *retries* **Example:** `Device(config-radius-server)# retransmit 25`	Specifies how many times the device transmits each RADIUS request to the server before giving up (the default is 3). **Note** In this step, the retransmission value is configured globally for all RADIUS servers.
Step 7	**timeout** *seconds* **Example:** `Device(config-radius-server)# timeout 6`	Specifies for how many seconds a device waits for a reply to a RADIUS request before retransmitting the request. **Note** In this step, the timeout value is configured globally for all RADIUS servers.
Step 8	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Configuration Examples for RADIUS for Multiple UDP Ports

Example: Device-to-RADIUS Server Communication

The following example shows how to configure two RADIUS servers with specific timeout, retransmit, and key values. In this example, the **aaa new-model** command enables AAA services on the device, and specific AAA commands define the AAA services. The **retransmit** command changes the global retransmission value to 4 for all RADIUS servers. The **host** command configures specific timeout, retransmission, and key values for the RADIUS server hosts with IP addresses 172.16.1.1 and 172.29.39.46.

```
! Enable AAA services on the device and define those services.
aaa new-model
aaa authentication login default group radius
aaa authentication login console-login none
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
enable password tryit1
!
Device(config)# radius server rad1
Device(config-radius-server)# address ipv4 10.45.1.2
Device(config-radius-server)# key myRaDIUSpassword
Device(config-radius-server)# retransmit 25
Device(config-radius-server)# timeout 6
Device(config)# exit
```

Example: RADIUS Server with Server-Specific Values

The following example shows how to configure server-specific timeout, retransmit, and key values for the RADIUS server with IP address 172.31.39.46:

```
radius-server host 172.31.39.46 timeout 6 retransmit 5 key rad123
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
AAA	*Authentication, Authorization, and Accounting Configuration Guide* (part of the Securing User Services Configuration Library)

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

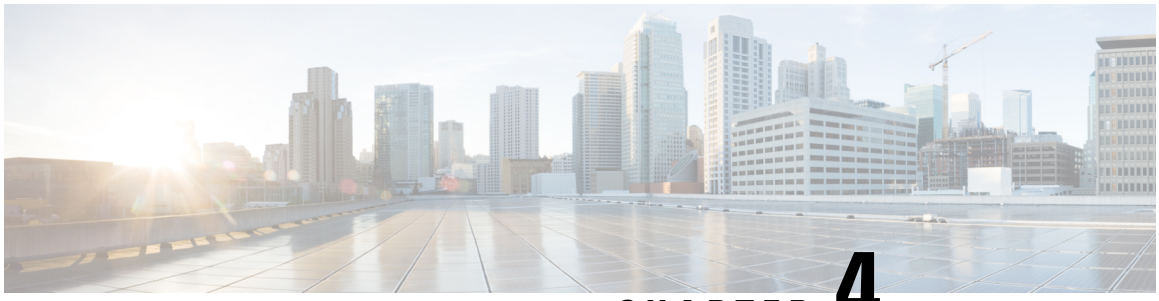
Feature Information for RADIUS for Multiple UDP Ports

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 5: Feature Information for RADIUS for Multiple UDP Ports

Feature Name	Releases	Feature Information
RADIUS for Multiple UDP Ports		RADIUS security servers are identified on the basis of their hostname or IP address, hostname and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. The following command was introduced or modified: **radius-server host**.



CHAPTER 4

AAA DNIS Map for Authorization

The AAA DNIS Map for Authorization feature allows you to assign a Dialed Number Identification Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group so that the server group can process authentication, authorization, and accounting requests for users dialing in to the network using that particular DNIS. Any phone line (a regular home phone or a commercial T1/PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you.

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 AAA DNIS Map for Authorization

- Before configuring the device to select a particular AAA server group based on the DNIS of the server group, you must configure the list of RADIUS server hosts and AAA server groups.
- Before configuring AAA preauthentication, you must configure the **aaa new-model** command and make sure that the supporting preauthentication application is running on a RADIUS server in your network.

Information About AAA DNIS Map for Authorization

AAA Server Group Selection Based on DNIS

Cisco software allows you to assign a DNIS number to a particular AAA server group so that the server group can process authentication, authorization, and accounting requests for users dialing in to the network using that particular DNIS. Any phone line (a regular home phone or a commercial T1/PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you.

For example, suppose you want to share the same phone number with several customers, but you want to know which customer is calling before you pick up the phone. You can customize how you answer the phone because DNIS allows you to know which customer is calling when you answer.

Cisco devices with either ISDN or internal modems can receive the DNIS number. This functionality allows users to assign different RADIUS server groups for different customers (that is, different RADIUS servers for different DNIS numbers). Additionally, using server groups, you can specify the same server group for AAA services or a separate server group for each AAA service.

Cisco software provides the flexibility to implement authentication and accounting services in several ways:

- Globally—AAA services are defined using global configuration access list commands and applied in general to all interfaces on a specific network access server.
- Per interface—AAA services are defined using interface configuration commands and applied specifically to the interface being configured on a specific network access server.
- DNIS mapping—You can use DNIS to specify an AAA server to supply AAA services.

Because each of these AAA configuration methods can be configured simultaneously, Cisco has established an order of precedence to determine which server or groups of servers provide AAA services. The order of precedence is as follows:

- Per DNIS—If you configure the network access server to use DNIS to identify or determine which server group provides AAA services, this method takes precedence over any additional AAA selection method.
- Per interface—If you configure the network access server per interface to use access lists to determine how a server provides AAA services, this method takes precedence over any global configuration AAA access lists.
- Globally—If you configure the network access server by using global AAA access lists to determine how the security server provides AAA services, this method has the least precedence.

AAA Preauthentication

Configuring AAA preauthentication with ISDN PRI or channel-associated signaling (CAS) allows service providers to better manage ports using their existing RADIUS solutions and efficiently manage the use of shared resources to offer differing service-level agreements. With ISDN PRI or CAS, information about an incoming call is available to the network access server (NAS) before the call is connected. The available call information includes the following:

- The DNIS number, also referred to as the called number

- The Calling Line Identification (CLID) number, also referred to as the calling number
- The call type, also referred to as the bearer capability

The AAA preauthentication feature allows a Cisco NAS to decide--on the basis of the DNIS number, the CLID number, or the call type--whether to connect an incoming call. (With ISDN PRI, it enables user authentication and authorization before a call is answered. With CAS, the call must be answered; however, the call can be dropped if preauthentication fails.)

When an incoming call arrives from the public network switch, but before it is connected, AAA preauthentication enables the NAS to send the DNIS number, CLID number, and call type to a RADIUS server for authorization. If the server authorizes the call, the NAS accepts the call. If the server does not authorize the call, the NAS sends a disconnect message to the public network switch to reject the call.

In the event that the RADIUS server application becomes unavailable or is slow to respond, a guard timer can be set in the NAS. When the timer expires, the NAS uses a configurable parameter to accept or reject the incoming call that has no authorization.

The AAA preauthentication feature supports the use of attribute 44 by the RADIUS server application and the use of RADIUS attributes that are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They can also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used.

The following restrictions apply to AAA preauthentication with ISDN PRI and CAS:

- Attribute 44 is available for CAS calls only when preauthentication or resource pooling is enabled.
- Multichassis Multilink PPP (MMP) is not available with ISDN PRI.
- AAA preauthentication is available only on some hardware platforms.
- ISDN PRI is supported only on some hardware platforms.

Guard Timer for Call Handling

Because response times for preauthentication and authentication requests can vary, the guard timer allows you to control the handling of calls. The guard timer starts when the DNIS is sent to the RADIUS server. If the NAS does not receive a response from AAA before the guard timer expires, it accepts or rejects the calls on the basis of the configuration of the timer.

How to Configure AAA DNIS Map for Authorization

Configuring AAA DNIS Preauthentication

DNIS preauthentication enables preauthentication at call setup based on the number dialed. The DNIS number is sent directly to the security server when a call is received. If the call authenticated by AAA, it is accepted.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**

4. **group** {**radius** | **tacacs+** | *server-group*}
5. **dnis** [**password** *string*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa preauthorization** **Example:** `Device(config)# aaa preauthorization`	Enters AAA preauthentication configuration mode.
Step 4	**group** {**radius**	**tacacs+**	*server-group*} **Example:** `Device(config-preauth)# group radius`	(Optional) Selects the security server to use for AAA preauthentication requests. • The default is RADIUS.
Step 5	**dnis** [**password** *string*] **Example:** `Device(config-preauth)# dnis password dnispass`	Enables preauthentication using DNIS and optionally specifies a password to use in Access-Request packets.
Step 6	**end** **Example:** `Device(config-preauth)# end`	Exits AAA preauthentication configuration mode and returns to privileged EXEC mode.

Configuring AAA Server Group Selection Based on DNIS

To configure the device to select a particular AAA server group based on the DNIS of the server group, configure DNIS mapping. To map a server group with a group name with a DNIS number, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa dnis map enable**

4. **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*
5. **aaa dnis map** *dnis-number* **authorization network group** *server-group-name*
6. **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa dnis map enable** **Example:** `Device(config)# aaa dnis map enable`	Enables DNIS mapping.
Step 4	**aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name* **Example:** `Device(config)# aaa dnis map 7777 authentication ppp group sg1`	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authentication.
Step 5	**aaa dnis map** *dnis-number* **authorization network group** *server-group-name* **Example:** `Device(config)# aaa dnis map 7777 authorization network group sg1`	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authorization.
Step 6	**aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name* **Example:** `Device(config)# aaa dnis map 8888 accounting network stop-only group sg2`	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for accounting.
Step 7	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring AAA Preauthentication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** *server-group*
5. **clid** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
6. **ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
7. **dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
8. **dnis bypass** *dnis-group-name*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa preauthorization** **Example:** `Device(config)# aaa preauthorization`	Enters AAA preauthentication configuration mode.
Step 4	**group** *server-group* **Example:** `Device(config-preauth)# group sg2`	Specifies the AAA RADIUS server group to use for preauthentication.
Step 5	**clid** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **Example:** `Device(config-preauth)# clid required`	Preauthenticates calls on the basis of the CLID number.
Step 6	**ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **Example:** `Device(config-preauth)# ctype required`	Preauthenticates calls on the basis of the call type.

	Command or Action	Purpose
Step 7	**dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **Example:** `Device(config-preauth)# dnis required`	Preauthenticates calls on the basis of the DNIS number.
Step 8	**dnis bypass** *dnis-group-name* **Example:** `Device(config-preauth)# dnis bypass group1`	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
Step 9	**end** **Example:** `Device(config-preauth)# end`	Exits preauthentication configuration mode and returns to privileged EXEC mode.

Configuring a Guard Timer

To set a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to an authentication or preauthentication request, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
5. **call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:**	Enters interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface serial 1/0/0:23`	
Step 4	**isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] **Example:** `Device(config-if)# isdn guard-timer 8000 on-expiry reject`	Sets an ISDN guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.
Step 5	**call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] **Example:** `Device(config-if)# call guard-timer 2000 on-expiry accept`	Sets a CAS guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.
Step 6	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for AAA DNIS Map for Authorization

Example: AAA Server Group Selection Based on DNIS

The following example shows how to select RADIUS server groups based on DNIS to provide specific AAA services:

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the RADIUS attributes for each server
! that will be associated with one of the defined server groups.
radius-server host 172.16.0.1 auth-port 1645 acct-port 1646 key cisco1
radius-server host 172.17.0.1 auth-port 1645 acct-port 1646 key cisco2
radius-server host 172.18.0.1 auth-port 1645 acct-port 1646 key cisco3
radius-server host 172.19.0.1 auth-port 1645 acct-port 1646 key cisco4
radius-server host 172.20.0.1 auth-port 1645 acct-port 1646 key cisco5
! The following commands define the sg1 RADIUS server group and associate servers
! with it.
aaa group server radius sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 RADIUS server group and associate a server
! with it.
aaa group server radius sg2
  server 172.18.0.1
! The following commands define the sg3 RADIUS server group and associate a server
! with it.
aaa group server radius sg3
```

```
  server 172.19.0.1
! The following commands define the default-group RADIUS server group and associate
! a server with it.
aaa group server radius default-group
  server 172.20.0.1
! The next set of commands configures default-group RADIUS server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using
! DNIS 7777 are sent to the sg1 server group. The accounting records for these
! connections (specifically, start-stop records) are handled by the sg2 server group.
! Calls with a DNIS of 8888 use server group sg3 for authentication and server group
! default-group for accounting. Calls with a DNIS of 9999 use server group
! default-group for authentication and server group sg3 for accounting records
! (stop records only). All other calls with DNIS other than the ones defined use the
! server group default-group for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

Examples: AAA Preauthentication

The following is a simple configuration that specifies that the DNIS number be used for preauthentication:

```
aaa preauthentication
 group radius
 dnis required
```

The following example shows a configuration that specifies that both the DNIS number and the CLID number be used for preauthentication. DNIS preauthentication is performed first, followed by CLID preauthentication.

```
aaa preauthentication
 group radius
 dnis required
 clid required
```

The following example specifies that preauthentication be performed on all DNIS numbers except the two DNIS numbers specified in the DNIS group called “dnis-group1”:

```
aaa preauthentication
 group radius
 dnis required
 dnis bypass dnis-group1
dialer dnis group dnis-group1
 number 12345
 number 12346
```

The following is a sample AAA configuration with DNIS preauthentication:

```
aaa new-model
aaa authentication login CONSOLE none
aaa authentication login RADIUS_LIST group radius
aaa authentication login TAC_PLUS group tacacs+ enable
aaa authentication login V.120 none
aaa authentication enable default enable group tacacs+
aaa authentication ppp RADIUS_LIST if-needed group radius
```

```
aaa authorization exec RADIUS_LIST group radius if-authenticated
aaa authorization exec V.120 none
aaa authorization network default group radius if-authenticated
aaa authorization network RADIUS_LIST if-authenticated group radius
aaa authorization network V.120 group radius if-authenticated
aaa accounting suppress null-username
aaa accounting exec default start-stop group radius
aaa accounting commands 0 default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting connection default start-stop group radius
aaa accounting system default start-stop group radius
aaa preauthentication
 dnis password Cisco-DNIS
aaa nas port extended
!
radius-server configure-nas
radius-server host 10.0.0.0 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.255.255.255 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 2
radius-server deadtime 1
radius-server attribute nas-port format c
radius-server unique-ident 18
radius-server key MyKey
```

Note To configure preauthentication, you must also set up preauthentication profiles on the RADIUS server.

Examples: Guard Timer for ISDN and CAS

The following example shows an ISDN guard timer that is set at 8000 milliseconds. A call is rejected if the RADIUS server does not respond to a preauthentication request when the timer expires.

```
interface serial 1/0/0:23
 isdn guard-timer 8000 on-expiry reject
aaa preauthentication
 group radius
 dnis required
```

The following example shows a CAS guard timer that is set at 20,000 milliseconds. A call is accepted if the RADIUS server does not respond to a preauthentication request when the timer expires.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
 call guard-timer 20000 on-expiry accept
aaa preauthentication
group radius
dnis required
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
AAA	*Authentication, Authorization, and Accounting Configuration Guide* (part of the Securing User Services Configuration Library)

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

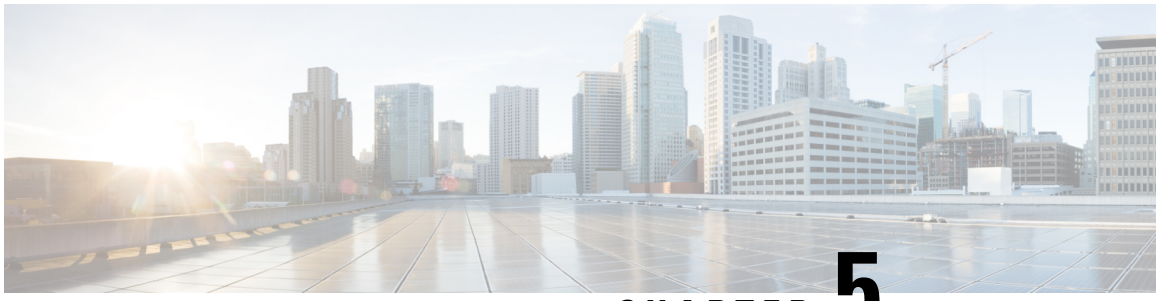
Feature Information for AAA DNIS Map for Authorization

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 6: Feature Information for AAA DNIS Map for Authorization

Feature Name	Releases	Feature Information
AAA DNIS Map for Authorization	12.1(1)T 12.2(2)T 12.2(27)SBA Cisco IOS XE Release 2.3	The AAA DNIS Map for Authorization feature allows you to assign a Dialed Number Identification Service (DNIS) number to a particular AAA server group so that the server group can process authentication, authorization, and accounting requests for users dialing in to the network using that particular DNIS. Any phone line (a regular home phone or a commercial T1/ PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you. The following commands were introduced or modified: **aaa dnis enable**, **aaa dnis map authentication group**, **aaa dnis map authorization network group**, and **aaa dnis map accounting network**.



CHAPTER 5

AAA Server Groups

Configuring a device to use authentication, authorization, and accounting (AAA) server groups provides a way to group existing server hosts. Grouping existing server hosts allows you to select a subset of the configured server hosts and use them for a particular service. Configuring deadtime within a server group allows you to direct AAA traffic to separate groups of servers that have different operational characteristics. This feature module describes how to configure AAA server groups and the deadtimer.

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.

Information About AAA Server Groups

AAA Server Groups

Configuring the device to use AAA server groups provides a way to group existing server hosts. Grouping existing server hosts allows you to select a subset of the configured server hosts and use them for a particular service. A server group is used with a global server-host list. The server group lists the IP addresses of the selected server hosts.

Server groups can also include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique

identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry that is configured acts as a failover backup to the first one. If the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order in which they are configured.)

AAA Server Groups with a Deadtimer

After you configure a server host with a server name, you can use the **deadtime** command to configure each server per server group. Configuring deadtime within a server group allows you to direct AAA traffic to separate groups of servers that have different operational characteristics.

Configuring deadtime is not limited to a global configuration. A separate timer is attached to each server host in every server group. Therefore, when a server is found to be unresponsive after numerous retransmissions and timeouts, the server is assumed to be dead. The timers attached to each server host in all server groups are triggered. In essence, the timers are checked and subsequent requests to a server (once it is assumed to be dead) are directed to alternate timers, if configured. When the network access server receives a reply from the server, it checks and stops all configured timers (if running) for that server in all server groups.

If the timer has expired, the server to which the timer is attached is assumed to be alive. This becomes the only server that can be tried for later AAA requests using the server groups to which the timer belongs.

Note Because one server has different timers and might have different deadtime values configured in the server groups, the same server might, in the future, have different states (dead and alive) at the same time.

Note To change the state of a server, you must start and stop all configured timers in all server groups.

The size of the server group will be slightly increased because of the addition of new timers and the deadtime attribute. The overall impact of the structure depends on the number and size of the server groups and how the servers are shared among server groups in a specific configuration.

How to Configure AAA Server Groups

Configuring AAA Server Groups

To define a server host with a server group name, enter the following commands in global configuration mode. The listed server must exist in global configuration mode.

Before you begin

Each server in the group must be defined previously using the **radius-server host** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius server** *server-name*
4. **aaa group server** {**radius** | **tacacs+**} *group-name*
5. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server rad1`	Specifies the name for the RADIUS server.
Step 4	**aaa group server** {**radius**	**tacacs+**} *group-name* **Example:** `Device(config)# aaa group server radius group1`	Defines the AAA server group with a group name. • All members of a group must be the same type, that is, RADIUS or TACACS+. This command puts the device in server group RADIUS configuration mode.
Step 5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Device(config-sg-radius)# server 172.16.1.1 acct-port 1616`	Associates a particular RADIUS server with the defined server group. • Each security server is identified by its IP address and UDP port number. • Repeat this step for each RADIUS server in the AAA server group.
Step 6	**end** **Example:** `Device(config-sg-radius)# end`	Exits server group RADIUS configuration mode and returns to privileged EXEC mode.

Configuring AAA Server Groups with a Deadtimer

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group*
4. **deadtime** *minutes*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa group server radius** *group* **Example:** `Device(config)# aaa group server radius group1`	Defines a RADIUS type server group and enters server group RADIUS configuration mode.
Step 4	**deadtime** *minutes* **Example:** `Device(config-sg-radius)# deadtime 1`	Configures and defines a deadtime value in minutes. **Note** Local server group deadtime overrides the global configuration. If the deadtime vlaue is omitted from the local server group configuration, it is inherited from the primary list.
Step 5	**end** **Example:** `Device(config-sg-radius)# end`	Exits the server group RADIUS configuration mode and returns to the privileged EXEC mode.

Configuration Examples for AAA Server Groups

Examples: AAA Server Groups

The following example shows how to create server group radgroup1 with three different RADIUS server members, each using the default authentication port (1645) and accounting port (1646):

```
aaa group server radius radgroup1
 server 172.16.1.11
 server 172.17.1.21
 server 172.18.1.31
```

The following example shows how to create server group radgroup2 with three RADIUS server members, each with the same IP address but with unique authentication and accounting ports:

```
aaa group server radius radgroup2
 server 172.16.1.1 auth-port 1000 acct-port 1001
 server 172.16.1.1 auth-port 2000 acct-port 2001
 server 172.16.1.1 auth-port 3000 acct-port 3001
```

Example: Multiple RADIUS Server Entries Using AAA Server Groups

The following example shows how to configure the network access server to recognize two different RADIUS server groups. One of these groups, group1, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as failover backup to the first one. Each group is individually configured for the deadtime; the deadtime for group 1 is one minute, and the deadtime for group 2 is two minutes.

Note In cases where both global commands and **server** commands are used, the **server** command takes precedence over the global command.

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS server group and associate servers
! with it and configures a deadtime of one minute.
aaa group server radius group1
 server 10.1.1.1 auth-port 1645 acct-port 1646
 server 10.2.2.2 auth-port 2000 acct-port 2001
 deadtime 1
! The following commands define the group2 RADIUS server group and associate servers
! with it and configures a deadtime of two minutes.
aaa group server radius group2
 server 10.2.2.2 auth-port 2000 acct-port 2001
 server 10.3.3.3 auth-port 1645 acct-port 1646
 deadtime 2
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined server groups.
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server host 10.2.2.2 auth-port 2000 acct-port 2001
radius-server host 10.3.3.3 auth-port 1645 acct-port 1646
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
AAA and RADIUS commands	*Cisco IOS Security Command Reference*
RADIUS attributes	*RADIUS Attributes Configuration Guide* (part of the Securing User Services Configuration Library)
AAA	*Authentication, Authorization, and Accounting Configuration Guide* (part of the Securing User Services Configuration Library)
L2TP, VPN, or VPDN	*Dial Technologies Configuration Guide* and *VPDN Configuration Guide*
Modem configuration and management	*Dial Technologies Configuration Guide*
RADIUS port identification for PPP	*Wide-Area Networking Configuration Guide*

RFCs

RFC	Title
RFC 2138	*Remote Authentication Dial-In User Service (RADIUS)*
RFC 2139	*RADIUS Accounting*
RFC 2865	*RADIUS*
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*
RFC 2868	*RADIUS Attributes for Tunnel Protocol Support*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

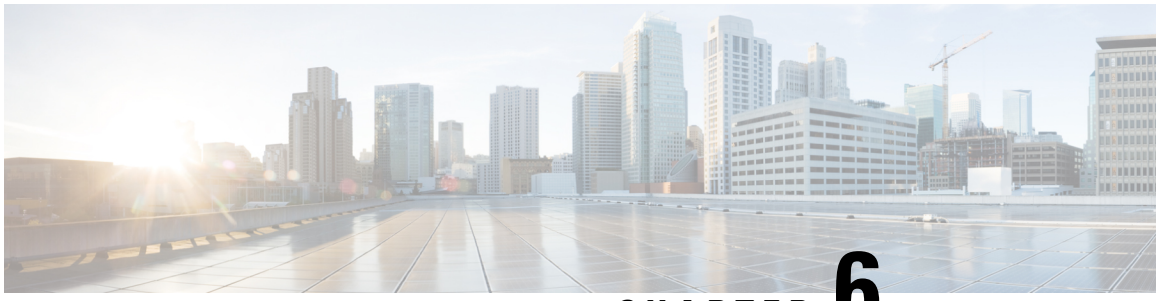
Feature Information for AAA Server Groups

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 7: Feature Information for AAA Server Groups

Feature Name	Releases	Feature Information
AAA Server Group		Configuring the device to use AAA server groups provides a way to group existing server hosts. This allows you to select a subset of the configured server hosts and use them for a particular service. A server group is used with a global server-host list. The server group lists the IP addresses of the selected server hosts. The following commands were introduced or modified: **aaa group server radius**, **aaa group server tacacs+**, and **server** (RADIUS).
AAA Server Group Enhancements		AAA Server Group Enhancements enables the full configuration of a server in a server group.
AAA Server Group Deadtimer		Configuring deadtime within a server group allows you to direct AAA traffic to separate groups of servers that have different operational characteristics. The following commands were introduced or modified: **deadtime**.



CHAPTER 6

Framed-Route in RADIUS Accounting

The Framed-Route in RADIUS Accounting feature provides for the presence of Framed-Route (RADIUS attribute 22) information in RADIUS Accounting-Request accounting records. The Framed-Route information is returned to the RADIUS server in the Accounting-Request packets. The Framed-Route information can be used to verify that a per-user route or routes have been applied for a particular static IP customer on the network access server (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 Framed-Route in RADIUS Accounting

Be familiar with configuring authentication, authorization, and accounting (AAA), RADIUS servers, and RADIUS attribute screening.

Information About Framed-Route in RADIUS Accounting

Framed-Route Attribute 22

Framed-Route, attribute 22 as defined in Internet Engineering Task Force (IETF) standard RFC 2865, provides for routing information to be configured for the user on the NAS. The Framed-Route attribute information is usually sent from the RADIUS server to the NAS in Access-Accept packets. The attribute can appear multiple times.

Framed-Route in RADIUS Accounting Packets

The Framed-Route attribute information in RADIUS accounting packets shows per-user routes that have been applied for a particular static IP customer on the NAS. The Framed-Route attribute information is currently sent in Access-Accept packets. The Framed-Route attribute information is also sent in Accounting-Request packets if it was provided in the Access-Accept packets and was applied successfully. Zero or more instances of the Framed-Route attribute may be present in the Accounting-Request packets.

Note If there is more than one Framed-Route attribute in an Access-Accept packet, there can also be more than one Framed-Route attribute in the Accounting-Request packet.

The Framed-Route information is returned in Stop and Interim accounting records and in Start accounting records when accounting Delay-Start is configured.

No configuration is required to have the Frame-Route attribute information returned in the RADIUS accounting packets.

How to Monitor Framed-Route in RADIUS Accounting

Use the **debug radius** command to monitor whether Framed-Route (attribute 22) information is being sent in RADIUS Accounting-Request packets.

ConfigurationExamplesforFramed-RouteinRADIUSAccounting

debug radius Command Output Example

In the following example, the **debug radius** command is used to verify that Framed-Route (attribute 22) information is being sent in the Accounting-Request packets (see the line 00:06:23: RADIUS: Framed-Route [22] 26 "10.80.0.1 255.255.255.255 10.60.0.1 100").

```
Router# debug radius
00:06:23: RADIUS:  Send to unknown id 0 10.1.0.2:1645, Access-Request, len 126
00:06:23: RADIUS:  authenticator 40 28 A8 BC 76 D4 AA 88 - 5A E9 C5 55 0E 50 84 37
00:06:23: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
```

```
00:06:23: RADIUS:  User-Name           [1]   14  "nari@trw1001"
00:06:23: RADIUS:  CHAP-Password       [3]   19  *
00:06:23: RADIUS:  NAS-Port            [5]   6   1
00:06:23: RADIUS:  Vendor, Cisco       [26]  33
00:06:23: RADIUS:  Cisco AVpair        [1]   27  "interface=Virtual-Access1"
00:06:23: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
00:06:23: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:06:23: RADIUS:  NAS-IP-Address      [4]   6   12.1.0.1
00:06:23: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
00:06:23: RADIUS:  Received from id 0 10.1.0.2:1645, Access-Accept, len 103
00:06:23: RADIUS:  authenticator 5D 2D 9F 25 11 15 45 B2 - 54 BB 7F EB CE 79 20 3B
00:06:23: RADIUS:  Vendor, Cisco       [26]  33
00:06:23: RADIUS:  Cisco AVpair        [1]   27  "interface=Virtual-Access1"
00:06:23: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:06:23: RADIUS:  Framed-Protocol     [7]   6   PPP                      [1]
00:06:23: RADIUS:  Framed-IP-Netmask   [9]   6   255.255.255.255
00:06:23: RADIUS:  Framed-IP-Address   [8]   6   10.60.0.1
00:06:23: RADIUS:  Framed-Route        [22]  26  "10.80.0.1 255.255.255.255 10.60.0.1 100"
        <=======
00:06:23: RADIUS:  Received from id 2
00:06:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state
to up
00:06:25: AAA/AUTHOR:  Processing PerUser AV route
00:06:25: Vi1 AAA/PERUSER/ROUTE: route string: IP route  10.80.0.1 255.255.255.255 10.60.0.1
 100
00:06:25: RADIUS/ENCODE(00000002): Unsupported AAA attribute timezone
00:06:25: RADIUS(00000002): sending
00:06:25: RADIUS:  Send to unknown id 1 10.1.0.2:1646, Accounting-Request, len 278
00:06:25: RADIUS:  authenticator E0 CC 99 EB 49 18 B9 78 - 4A 09 60 0F 4E 92 24 C6
00:06:25: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
00:06:25: RADIUS:  Tunnel-Server-Endpoi[67]  12  00:"10.1.1.1"
00:06:25: RADIUS:  Tunnel-Client-Endpoi[66]  12  00:"10.1.1.2"
00:06:25: RADIUS:  Tunnel-Assignment-Id[82]  15  00:"from_isdn101"
00:06:25: RADIUS:  Tunnel-Type         [64]  6   00:L2TP                  [3]
00:06:25: RADIUS:  Acct-Tunnel-Connecti[68]  12  "2056100083"
00:06:25: RADIUS:  Tunnel-Client-Auth-I[90]  10  00:"isdn101"
00:06:25: RADIUS:  Tunnel-Server-Auth-I[91]  6   00:"lns"
00:06:25: RADIUS:  Framed-Protocol     [7]   6   PPP                      [1]
00:06:25: RADIUS:  Framed-Route        [22]  39  "10.80.0.1 255.255.255.255 10.60.0.1 100"
         <========
00:06:25: RADIUS:  Framed-IP-Address   [8]   6   10.60.0.1
00:06:25: RADIUS:  Vendor, Cisco       [26]  35
00:06:25: RADIUS:  Cisco AVpair        [1]   29  "connect-progress=LAN Ses Up"
00:06:25: RADIUS:  Authentic           [45]  6   RADIUS                    [1]
00:06:25: RADIUS:  User-Name           [1]   14  "username1@example.com"
00:06:25: RADIUS:  Acct-Status-Type    [40]  6   Start                    [1]
00:06:25: RADIUS:  NAS-Port            [5]   6   1
00:06:25: RADIUS:  Vendor, Cisco       [26]  33
00:06:25: RADIUS:  Cisco AVpair        [1]   27  "interface=Virtual-Access1"
00:06:25: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
00:06:25: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:06:25: RADIUS:  NAS-IP-Address      [4]   6   10.1.0.1
00:06:25: RADIUS:  Acct-Delay-Time     [41]  6   0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*
RADIUS	"Configuring RADIUS" feature module.

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
None.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 3575	IANA Considerations for RADIUS (Remote Authentication Dial In User Service)

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/cisco/web/support/index.html

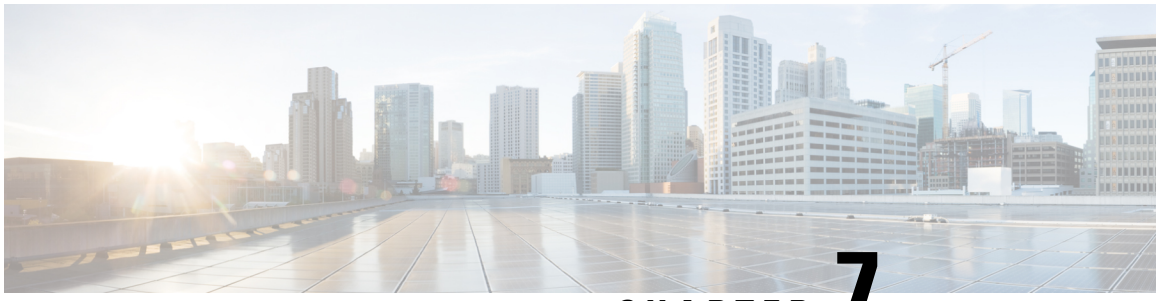
Feature Information for Framed-Route in RADIUS Accounting

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 8: Feature Information for Framed-Route in RADIUS Accounting

Feature Name	Releases	Feature Information
Framed-Route in RADIUS Accounting	Cisco IOS XE Release 2.1	The Framed-Route in RADIUS Accounting feature provides for the presence of Framed-Route (RADIUS attribute 22) information in RADIUS Accounting-Request accounting records. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 7

RFC-2867 RADIUS Tunnel Accounting

The RFC-2867 RADIUS Tunnel Accounting introduces six new RADIUS accounting types that are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40), which indicates whether an accounting request marks the beginning of user service (start) or the end (stop).

This feature also introduces two new virtual private virtual private dialup network (VPDN) commands that help users better troubleshoot VPDN session events.

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.

Restrictions for RFC-2867 RADIUS Tunnel Accounting

RADIUS tunnel accounting works only with L2TP tunnel support.

Information About RFC-2867 RADIUS Tunnel Accounting

Benefits of RFC-2867 RADIUS Tunnel Accounting

Without RADIUS tunnel accounting support, VPDN with network accounting, which allows users to determine tunnel-link status changes, did not report all possible attributes to the accounting record file. Now that all possible attributes can be displayed, users can better verify accounting records with their Internet Service Providers (ISPs).

RADIUS Attributes Support for RADIUS Tunnel Accounting

The table below outlines the new RADIUS accounting types that are designed to support the provision of compulsory tunneling in dialup networks; that is, these attribute types allow you to better track tunnel status changes.

Note The accounting types are divided into two separate tunnel types so users can decide if they want tunnel type, tunnel-link type, or both types of accounting.

Table 9: RADIUS Accounting Types for the Acct-Status-Type Attribute

Type-Name	Number	Description	Additional Attributes[1]
Tunnel-Start	9	Marks the beginning of a tunnel setup with another node.	• User-Name (1)--from client • NAS-IP-Address (4)--from AAA • Acct-Delay-Time (41)--from AAA • Event-Timestamp (55)--from AAA • Tunnel-Type (64)--from client • Tunnel-Medium-Type (65)--from client • Tunnel-Client-Endpoint (66)--from client • Tunnel-Server-Endpoint (67)--from client • Acct-Tunnel-Connection (68)--from client

Type-Name	Number	Description	Additional Attributes[1]
Tunnel-Stop	10	Marks the end of a tunnel connection to or from another node.	• User-Name (1)--from client • NAS-IP-Address (4)--from AAA • Acct-Delay-Time (41)--from AAA • Acct-Input-Octets (42)--from AAA • Acct-Output-Octets (43)--from AAA • Acct-Session-Id (44)--from AAA • Acct-Session-Time (46)--from AAA • Acct-Input-Packets (47)--from AAA • Acct-Output-Packets (48)--from AAA • Acct-Terminate-Cause (49)--from AAA • Acct-Multi-Session-Id (51)--from AAA • Event-Timestamp (55)--from AAA • Tunnel-Type (64)--from client • Tunnel-Medium-Type (65)--from client • Tunnel-Client-Endpoint (66)--from client • Tunnel-Server-Endpoint (67)--from client • Acct-Tunnel-Connection (68)--from client • Acct-Tunnel-Packets-Lost (86)--from client

Type-Name	Number	Description	Additional Attributes[1]
Tunnel-Reject	11	Marks the rejection of a tunnel setup with another node.	• User-Name (1)--from client • NAS-IP-Address (4)--from AAA • Acct-Delay-Time (41)--from AAA • Acct-Terminate-Cause (49)--from client • Event-Timestamp (55)--from AAA • Tunnel-Type (64)--from client • Tunnel-Medium-Type (65)--from client • Tunnel-Client-Endpoint (66)--from client • Tunnel-Server-Endpoint (67)--from client • Acct-Tunnel-Connection (68)--from client
Tunnel-Link-Start	12	Marks the creation of a tunnel link. Only some tunnel types (Layer 2 Transport Protocol [L2TP]) support the multiple links per tunnel; this value should be included only in accounting packets for tunnel types that support multiple links per tunnel.	• User-Name (1)--from client • NAS-IP-Address (4)--from AAA • NAS-Port (5)--from AAA • Acct-Delay-Time (41)--from AAA • Event-Timestamp (55)--from AAA • Tunnel-Type (64)--from client • Tunnel-Medium-Type (65)--from client • Tunnel-Client-Endpoint (66)--from client • Tunnel-Server-Endpoint (67)--from client • Acct-Tunnel-Connection (68)--from client

Type-Name	Number	Description	Additional Attributes[1]
Tunnel-Link-Stop	13	Marks the end of a tunnel link. Only some tunnel types (L2TP) support the multiple links per tunnel; this value should be included only in accounting packets for tunnel types that support multiple links per tunnel.	• User-Name (1)--from client • NAS-IP-Address (4)--from AAA • NAS-Port (5)--from AAA • Acct-Delay-Time (41)--from AAA • Acct-Input-Octets (42)--from AAA • Acct-Output-Octets (43)--from AAA • Acct-Session-Id (44)--from AAA • Acct-Session-Time (46)--from AAA • Acct-Input-Packets (47)--from AAA • Acct-Output-Packets (48)--from AAA • Acct-Terminate-Cause (49)--from AAA • Acct-Multi-Session-Id (51)--from AAA • Event-Timestamp (55)--from AAA • NAS-Port-Type (61)--from AAA • Tunnel-Type (64)--from client • Tunnel-Medium-Type (65)--from client • Tunnel-Client-Endpoint (66)--from client • Tunnel-Server-Endpoint (67)--from client • Acct-Tunnel-Connection (68)--from client • Acct-Tunnel-Packets-Lost (86)--from client

Type-Name	Number	Description	Additional Attributes[1]
Tunnel-Link-Reject	14	Marks the rejection of a tunnel setup for a new link in an existing tunnel. Only some tunnel types (L2TP) support the multiple links per tunnel; this value should be included only in accounting packets for tunnel types that support multiple links per tunnel.	• User-Name (1)--from client • NAS-IP-Address (4)--from AAA • Acct-Delay-Time (41)--from AAA • Acct-Terminate-Cause (49)--from AAA • Event-Timestamp (55)--from AAA • Tunnel-Type (64)--from client • Tunnel-Medium-Type (65)--from client • Tunnel-Client-Endpoint (66)--from client • Tunnel-Server-Endpoint (67)--from client • Acct-Tunnel-Connection (68)--from client

[1] If the specified tunnel type is used, these attributes should also be included in the accounting request packet.

How to Configure RADIUS Tunnel Accounting

Enabling Tunnel Type Accounting Records

Use this task to configure your LAC to send tunnel and tunnel-link accounting records to be sent to the RADIUS server.

Two new command line interfaces (CLIs)--vpdn session accounting network(tunnel-link-type records)and vpdn tunnel accounting network(tunnel-type records) --are supported to help identify the following events:

- A VPDN tunnel is brought up or destroyed
- A request to create a VPDN tunnel is rejected
- A user session within a VPDN tunnel is brought up or brought down
- A user session create request is rejected

Note The first two events are tunnel-type accounting records: authentication, authorization, and accounting (AAA) sends Tunnel-Start, Tunnel-Stop, or Tunnel-Reject accounting records to the RADIUS server. The next two events are tunnel-link-type accounting records: AAA sends Tunnel-Link-Start, Tunnel-Link-Stop, or Tunnel-Link-Reject accounting records to the RADIUS server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa accounting network default** *list-name*} {**start-stop** | **stop-only** | **wait-start** | **none group** *groupname*
4. Router(config)# **vpdn enable**
5. Router(config)# **vpdn tunnel accounting network** *list-name*
6. Router(config)# **vpdn session accounting network** *list-name*

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	Router(config)# **aaa accounting network default** *list-name*} {**start-stop**	**stop-only**	**wait-start**	**none group** *groupname* **Example:** **Example:** **Example:** **Example:** **Example:** **Example:** **Example:** **Example:** **Example:**	Enables network accounting. • **default** --If the default network accounting method-list is configured and no additional accounting configurations are enabled on the interface, network accounting is enabled by default. If either the **vpdn session accounting network** command or the **vpdn tunnel accounting network** command is linked to the **default** method-list, all tunnel and tunnel-link accounting records are enabled for those sessions. • *list-name* --The *list-name*defined in the **aaa accounting**command must be the same as the *list-name* defined in the VPDN command; otherwise, accounting will not occur.

	Command or Action	Purpose
	Example: **Example:** `Router(config)# aaa accounting network m1 start-stop group radius`	
Step 4	Router(config)# **vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (if applicable).
Step 5	Router(config)# **vpdn tunnel accounting network** *list-name* **Example:** `Router(config)# vpdn tunnel accounting network m1`	Enables Tunnel-Start, Tunnel-Stop, and Tunnel-Reject accounting records. • *list-name* --The *list-name* must match the *list-name* defined in the **aaa accounting**command; otherwise, network accounting will not occur.
Step 6	Router(config)# **vpdn session accounting network** *list-name* **Example:** `Router(config)# vpdn session accounting network m1`	Enables Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject accounting records. • *list-name* --The *list-name* must match the *list-name* defined in the **aaa accounting**command; otherwise, network accounting will not occur.

What To Do Next

After you have enabled RADIUS tunnel accounting, you can verify your configuration via the following optional task Verifying RADIUS Tunnel Accounting.

Verifying RADIUS Tunnel Accounting

Use either one or both of the following optional steps to verify your RADIUS tunnel accounting configuration.

SUMMARY STEPS

1. **enable**
2. Router# **show accounting**
3. Router# **show vpdn** [**session**] [**tunnel**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	Router# **show accounting** **Example:** `Router# show accounting`	Displays the active accountable events on the network and helps collect information in the event of a data loss on the accounting server.
Step 3	Router# **show vpdn** [**session**] [**tunnel**] **Example:** **Example:** **Example:** **Example:** `Router# show vpdn session`	Displays information about active L2TP tunnel and message identifiers in a VPDN. • **session** --Displays a summary of the status of all active tunnels. • **tunnel** --Displays information about all active L2TP tunnels in summary-style format.

Configuration Examples for RADIUS Tunnel Accounting

Configuring RADIUS Tunnel Accounting on LAC Example

The following example shows how to configure your L2TP access concentrator (LAC) to send tunnel and tunnel-link accounting records to the RADIUS server:

```
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$IDjH$iL7puCja1RMlyOM.JAeuf/
enable password lab
!
username ISP_LAC password 0 tunnelpass
!
!
resource-pool disable
!
!
ip subnet-zero
ip cef
no ip domain-lookup
ip host dirt 172.16.1.129
!
vpdn enable
```

```
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.1.26.71
 local name ISP_LAC
!
mta receive maximum-recipients 0
!
interface GigabitEthernet0/0/0
 ip address 10.1.27.74 255.255.255.0
 no ip mroute-cache
 duplex half
 speed auto
 no cdp enable
!
interface FastEthernet0/0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip default-gateway 10.1.27.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.27.254
no ip http server
ip pim bidir-enable
!
no cdp run
!
!
radius-server host 172.19.192.26 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
!
```

Configuring RADIUS Tunnel Accounting on LNS Example

The following example shows how to configure your L2TP network server (LNS) to send tunnel and tunnel-link accounting records to the RADIUS server:

```
aaa new-model
!
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnelpass
username user1@cisco.com password 0 lab
username user2@cisco.com password 0 lab
spe 1/0 1/7
 firmware location system:/ucode/mica_port_firmware
spe 2/0 2/9
 firmware location system:/ucode/mica_port_firmware
```

```
!
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 172.24.80.28 10.47.0.0
ip host dirt 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname ISP_LAC
 local name ENT_LNS
!
mta receive maximum-recipients 0
!
interface Loopback0
 ip address 192.168.70.101 255.255.255.0
!
interface Loopback1
 ip address 192.168.80.101 255.255.255.0
!
interface FastEthernet0/0/0
 ip address 10.1.26.71 255.255.255.0
 no ip mroute-cache
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool vpdn-pool1
 ppp authentication chap
!
interface Virtual-Template2
 ip unnumbered Loopback1
 peer default ip address pool vpdn-pool2
 ppp authentication chap
!
interface FastEthernet0/0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip local pool vpdn-pool1 192.168.70.1 192.168.70.100
ip local pool vpdn-pool2 192.168.80.1 192.168.80.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 10.90.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
no cdp run
!
radius-server host 172.19.192.80 auth-port 1645 acct-port 1646 key rad123
```

```
radius-server retransmit 3
call rsvp-sync
```

Additional References

The following sections provide references related to RFC-2867 RADIUS Tunnel Accounting.

Related Documents

Related Topic	Document Title
RADIUS attributes	"RADIUS Attributes Overview and RADIUS IETF Attributes" in the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2
VPDN	*Cisco IOS XE VPDN Configuration Guide* , Release 2
Network accounting	"Configuring Accounting" in the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2
Commands	• *Cisco IOS Security Command Reference* • *Cisco IOS VPDN Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing standards 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

RFCs	Title
RFC 2867	*RADIUS Accounting Modifications 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

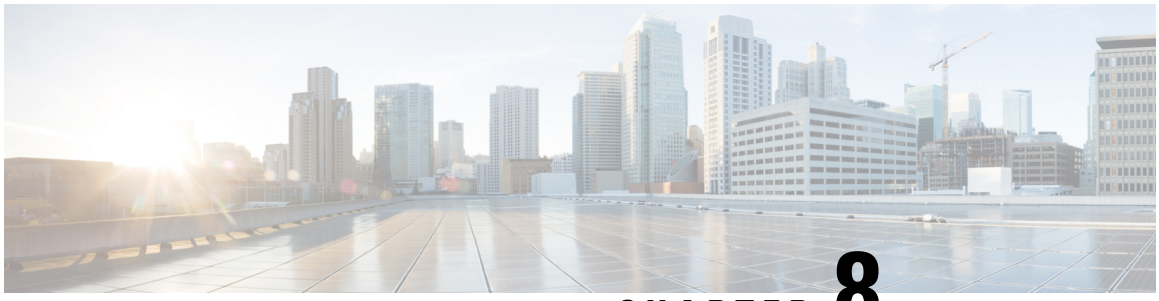
Feature Information for RFC-2867 RADIUS Tunnel Accounting

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 10: Feature Information for RFC-2867 RADIUS Tunnel Accounting

Feature Name	Releases	Feature Information
RFC-2867 RADIUS Tunnel Accounting	Cisco IOS XE Release 2.1	The RFC-2867 RADIUS Tunnel Accounting introduces six new RADIUS accounting types that are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40), which indicates whether an accounting request marks the beginning of user service (start) or the end (stop). This feature also introduces two new virtual private virtual private dialup network (VPDN) commands that help users better troubleshoot VPDN session events. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **aaa accounting**, **vpdn session accounting network**, **vpdn tunnel accounting network**.



CHAPTER 8

RADIUS Logical Line ID

The RADIUS Logical Line ID feature, also known as the Logical Line Identification (LLID) Blocking feature enables administrators to track their customers on the basis of the physical lines on which customer calls originate. Administrators use a virtual port that does not change as customers move from one physical line to another. This virtual port facilitates the maintenance of the administrator's customer profile database and allows the administrator to do additional security checks on customers.

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 Logical Line ID

Although this feature can be used with any RADIUS server, some RADIUS servers may require modifications to their dictionary files to allow the Calling-Station-ID attribute to be returned in Access-Accept messages. For example, the Merit RADIUS server does not support LLID downloading unless you modify its dictionary as follows: "ATTRIBUTE Calling-Station-Id 31 string (*, *)"

Restrictions for RADIUS Logical Line ID

The RADIUS Logical Line ID feature supports RADIUS only. TACACS+ is not supported.

This feature can be applied only toward PPP over Ethernet over ATM (PPPoEoATM) and PPP over Ethernet over VLAN (PPPoEoVLAN) (Dot1Q) calls; no other calls, such as ISDN, can be used.

Information About RADIUS Logical Line ID

Preauthorization

LLID is an alphanumeric string (which must be a minimum of one character and a maximum of 253 characters) that is a logical identification of a subscriber line. LLID is maintained in a customer profile database on a RADIUS server. When the customer profile database receives a preauthorization request from the access router, the RADIUS server sends the LLID to the router as the Calling-Station-ID attribute (attribute 31).

The Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) sends a preauthorization request to the customer profile database when the LAC is configured for preauthorization. Configure the LAC for preauthorization using the **subscriber access** command.

Note Downloading the LLID is referred to as “preauthorization” because it occurs before either service (domain) authorization or user authentication and authorization occur.

The customer profile database on the RADIUS server consists of user profiles for each physical network access server (NAS) port that is connected to the router. Each user profile contains a profile matched to a username (attribute 1) representing the physical port on the router. When the router is configured for preauthorization, it queries the customer profile database using a username representative of the physical NAS port making the connection to the router. When a match is found in the customer profile database, the customer profile database returns an Access-Accept message containing the LLID in the user profile. The LLID is defined in the Access-Accept record as the Calling-Station-ID attribute.

The preauthorization process can also provide the real username being used for authentication to the RADIUS server. Because the physical NAS port information is being used as the username (attribute 1), RADIUS attribute 77 (Connect-Info) can be configured to contain the authentication username. This configuration allows the RADIUS server to provide additional validation on the authorization request if it chooses, such as analyzing the username for privacy rules, before returning an LLID back to the router.

How to Configure RADIUS Logical Line ID

Configuring Preauthorization

To download the LLID and configure the LAC for preauthorization, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *interface-name*
4. **subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id** [**default** | *list-name*] [**send username**]

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	**ip radius source-interface** *interface-name* **Example:** **Example:** `Router (config)# ip radius source-interface Loopback1`	Specifies the IP address portion of the username for the preauthorization request.
Step 4	**subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id** [**default** | *list-name*] [**send username**] **Example:** **Example:** `Router (config)# subscriber access pppoe pre-authorize nas-port-id mlist_llid send username`	Enables the LLID to be downloaded so the router can be configured for preauthorization. The **send username** option specifies that you include the authentication username of the session inside the Connect-Info (attribute 77) in the Access-Request message.

Configuring the LLID in a RADIUS User Profile

To configure the user profile for preauthorization, add a NAS port user to the customer profile database and add RADIUS Internet Engineering Task Force (IETF) attribute 31 (Calling-Station-ID) to the user profile.

SUMMARY STEPS

1. UserName=nas_port: ip-address:slot/module/port/vpi.vci
2. User-Name=nas-port: ip-address:slot/module/port/vlan-id
3. Calling-Station-Id = “string (*,*)”

DETAILED STEPS

	Command or Action	Purpose
Step 1	UserName=nas_port: ip-address:slot/module/port/vpi.vci	(Optional) Adds a PPPoE over ATM NAS port user.
Step 2	User-Name=nas-port: ip-address:slot/module/port/vlan-id	(Optional) Adds a PPPoE over VLAN NAS port user.
Step 3	Calling-Station-Id = “string (*,*)”	Adds attribute 31 to the user profile. • String--One or more octets, containing the phone number from which the user placed the call.

Verifying Logical Line ID

To verify feature functionality, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug radius** **Example:** `Router# debug radius`	Checks to see that RADIUS attribute 31 is the LLID in the Accounting-Request on LAC and in the Access-Request and Accounting-Request on the LNS.

Configuration Examples for RADIUS Logical Line ID

LAC for Preauthorization Configuration Example

The following example shows how to configure your LAC for preauthorization by downloading the LLID:

```
aaa new-model
aaa group server radius sg_llid
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg_water
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization confg-commands
aaa authorization network default group sg_water
aaa authorization network mlist_llid group sg_llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg_water password 0 lab
vpdn enable
!
vpdn-group 2
 request-dialin
 protocol l2tp
 domain example.com
 domain example.com#184
 initiate-to ip 10.1.1.1
 local name s7200_2
 l2tp attribute clid mask-method right * 255 match #184
!
vpdn-group 3
 accept dialin
  protocol pppoe
  virtual-template 1
!
!
Enable the LLID to be downloaded.
subscriber access pppoe pre-authorize nas-port-id mlist_llid send username
!
interface Loopback0
 ip address 10.1.1.2 255.255.255.0
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet1/0/0
 ip address 10.1.1.8 255.255.255.0 secondary
 ip address 10.0.58.111 255.255.255.0
 no cdp enable
!
interface ATM4/0/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0/0.1 point-to-point
 pvc 1/100
  encapsulation aa15snap
  protocol pppoe
!
interface virtual-template1
 no ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap
!
radius-server host 172.31.164.120 auth-port 1645 acct-port 1646 key rad123
radius-server host 172.31.164.106 auth-port 1645 acct-port 1646 key rad123
ip radius source-interface Loopback1
```

RADIUS User Profile for LLID Example

The following example shows how to configure the user profile for LLID querying for PPPoEoVLAN and PPPoEoATM and how to add attribute 31:

```
pppoeovlan
----------
nas-port:10.1.0.3:6/0/0/0    Password = "password1",
    Service-Type = Outbound,
    Calling-Station-ID = "cat-example"
pppoeoa
--------
nas-port:10.1.0.3:6/0/0/1.100    Password = "password1",
    Service-Type = Outbound,
    Calling-Station-ID = "cat-example"
```

Additional References

The following sections provide references related to RADIUS EAP Support feature.

Related Documents

Related Topic	Document Title
Configuring PPP Authentication Using AAA	" Configuring Authentication " module.
Configuring RADIUS	" Configuring RADIUS " module.
PPP Configuration	" Configuring Asynchronous SLIP and PPP " module.
Dial Technologies commands	*Cisco IOS Dial Technologies Command Reference*
Security Commands	*Cisco IOS Security Command Reference*

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 2284	*PPP Extensible Authentication Protocol (EAP)*
RFC 1938	*A One-Time Password System*
RFC 2869	*RADIUS Extensions*

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 Logical Line ID

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 11: Feature Information for RADIUS Logical Line ID

Feature Name	Releases	Feature Information
RADIUS Logical Line ID	Cisco IOS XE Release 2.1	The RADIUS Logical Line ID feature, also known as the Logical Line Identification (LLID) Blocking feature enables administrators to track their customers on the basis of the physical lines on which customer calls originate. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following command was introduced or modified by this feature: **subscriber access**.
Calling Station ID Attribute 31	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Feature Name	Releases	Feature Information
LLID Blocking	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Glossary

attribute --A RADIUS Internet Engineering Task Force (IETF) attribute is one of the original set of 255 standard attributes that are used to communicate authentication, authorization, and accounting (AAA) information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers that exchange AAA information through IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

CHAP --Challenge Handshake Authentication Protocol. Security feature that is supported on lines using PPP encapsulation and prevents unauthorized access. CHAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines whether that user is allowed access.

EAP --Extensible Authentication Protocol. A PPP authentication protocol that supports multiple authentication mechanisms that are negotiated during the authentication phase (instead of the Link Control Protocol [LCP] phase). EAP allows a third-party authentication server to interact with the PPP implementation through a generic interface.

LCP --link control protocol. Protocol that establishes, configures, and tests data-link connections for use by PPP.

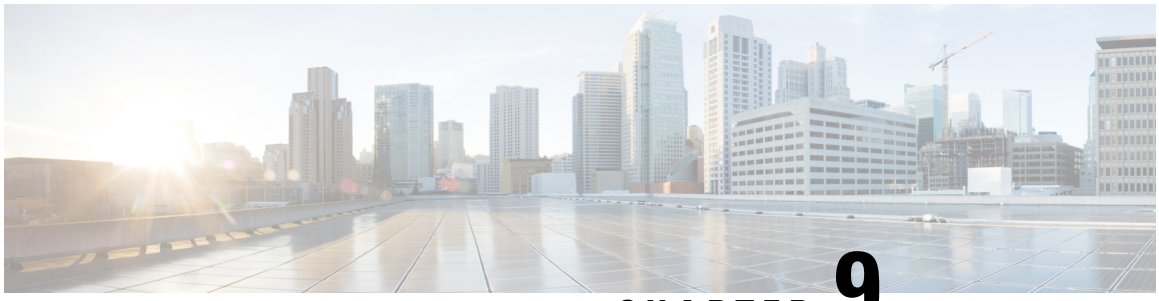
MD5 (HMAC variant) --Message Digest 5. A hash algorithm used to authenticate packet data. HMAC is a key hashing for message authentication.

NAS --network access server. A device providing local network access to users across a remote access network such as the public switched telephone network (PSTN).

PAP --Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines.

PPP --Point-to-Point Protocol. A protocol that encapsulates network layer protocol information over point-to-point links. PPP is defined in RFC 1661.

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



CHAPTER 9

RADIUS Route Download

The RADIUS Route Download feature allows users to configure their network access server (NAS) to direct RADIUS authorization.

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 Route Download

AAA network security must be enabled before you perform the tasks in this feature.

Information About RADIUS Route Download

The RADIUS Route Download feature allows users to configure their network access server (NAS) to direct RADIUS authorization. Users configure a separate named method list (in addition to the default method list) for static route download requests sent by their NAS to authorization, authentication, and accounting (AAA) servers.

Before this feature, RADIUS authorization for static route download requests was sent only to AAA servers specified by the default method list.

This feature extends the functionality of the **aaa route download** command to allow users to specify the name of the method list that will be used to direct static route download requests to the AAA servers. The **aaa route download**commandmay be used to specify a separate method list for downloading static routes. This method list can be added by using the **aaa authorization configuration** command.

How to Configure RADIUS Route Download

Configuring RADIUS Route Download

To configure the NAS to send static route download requests to the servers specified by a named method list, use the following commands in global configuration mode:

SUMMARY STEPS

1. Router(config)# **aaa authorization configuration** *method-name* **[radius | tacacs+ | group** *group-name* **]**
2. Router(config)# **aaa route download** [*time*] [**authorization** *method-list*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **aaa authorization configuration** *method-name* **[radius	tacacs+	group** *group-name* **]**	Downloads static route configuration information from the AAA server using RADIUS.
Step 2	Router(config)# **aaa route download** [*time*] [**authorization** *method-list*]	Enables the static route download feature. Use the **authorization** *method-list* attributes to specify a named method list to which RADIUS authorization requests for static route downloads are sent.

Verifying RADIUS Route Download

To verify the routes that are installed, use the **show ip route** command in EXEC mode.

To display information that is associated with RADIUS, use the **debug radius** command in privileged EXEC mode.

Configuration Examples for RADIUS Route Download

RADIUS Route Download Configuration Example

The following example shows how to configure the NAS to send static route download requests to the servers specified by the method list named “list1”:

```
aaa new-model
aaa group server radius rad1
```

```
server 10.2.2.2 auth-port 1645 acct-port 1646
!
aaa group server tacacs+ tac1
server 172.17.3.3
!
aaa authorization configuration default group radius
aaa authorization configuration list1 group rad1 group tac1
aaa route download 1 authorization list1
tacacs-server host 172.17.3.3
tacacs-server key cisco
tacacs-server administration
!
radius-server host 10.2.2.2 auth-port 1645 acct-port 1646
radius-server key cisco
```

Additional References

The following sections provide references related to RADIUS Route Download.

Related Documents

Related Topic	Document Title
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

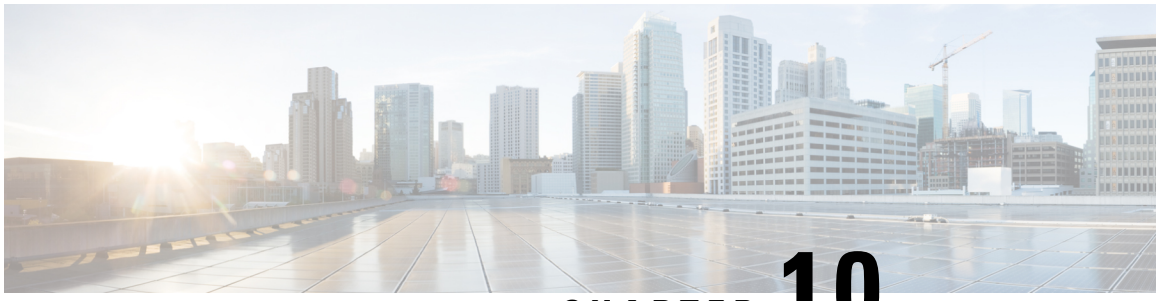
Feature Information for RADIUS Route Download

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 12: Feature Information for RADIUS Route Download

Feature Name	Releases	Feature Information
RADIUS Route Download	Cisco IOS XE Release 2.1	The RADIUS Route Download feature allows users to configure their network access server (NAS) to direct RADIUS authorization. Users configure a separate named method list (in addition to the default method list) for static route download requests sent by their NAS to authorization, authentication, and accounting (AAA) servers. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced: **aaa route download**



CHAPTER 10

RADIUS Server Load Balancing

The RADIUS Server Load Balancing feature distributes authentication, authorization, and accounting (AAA) authentication and accounting transactions across RADIUS servers in a server group. These servers can share the AAA transaction load and thereby respond faster to incoming requests.

This module describes the RADIUS Server Load Balancing feature.

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 Server Load Balancing

- Authentication, authorization, and accounting (AAA) must be configured on the RADIUS server.
- AAA RADIUS server groups must be configured.
- RADIUS must be configured for functions such as authentication, accounting, or static route download.

Restrictions for RADIUS Server Load Balancing

- Incoming RADIUS requests, such as Packet of Disconnect (POD) requests, are not supported.

Information About RADIUS Server Load Balancing

RADIUS Server Load Balancing Overview

Load balancing distributes batches of transactions to RADIUS servers within a server group. Load balancing assigns each batch of transactions to the server with the lowest number of outstanding transactions in its queue. The process of assigning a batch of transactions is as follows:

1. The first transaction is received for a new batch.
2. All server transaction queues are checked.
3. The server with the lowest number of outstanding transactions is identified.
4. The identified server is assigned the next batch of transactions.

The batch size is a user-configured parameter. Changes in the batch size may impact CPU load and network throughput. As batch size increases, CPU load decreases and network throughput increases. However, if a large batch size is used, all available server resources may not be fully utilized. As batch size decreases, CPU load increases and network throughput decreases.

Note There is no set number for large or small batch sizes. A batch with more than 50 transactions is considered large and a batch with fewer than 25 transactions is considered small.

Note If a server group contains ten or more servers, we recommend that you set a high batch size to reduce CPU load.

Transaction Load Balancing Across RADIUS Server Groups

You can configure load balancing either per-named RADIUS server group or for the global RADIUS server group. The load balancing server group must be referred to as “radius” in the authentication, authorization, and accounting (AAA) method lists. All public servers that are part of the RADIUS server group are then load balanced.

You can configure authentication and accounting to use the same RADIUS server or different servers. In some cases, the same server can be used for preauthentication, authentication, or accounting transactions for a session. The preferred server, which is an internal setting and is set as the default, informs AAA to use the same server for the start and stop record for a session regardless of the server cost. When using the preferred server setting, ensure that the server that is used for the initial transaction (for example, authentication), the

preferred server, is part of any other server group that is used for a subsequent transaction (for example, accounting).

The preferred server is not used if one of the following criteria is true:

- The **load-balance method least-outstanding ignore-preferred-server** command is used.
- The preferred server is dead.
- The preferred server is in quarantine.
- The want server flag has been set, overriding the preferred server setting.

The want server flag, an internal setting, is used when the same server must be used for all stages of a multistage transaction regardless of the server cost. If the want server is not available, the transaction fails.

You can use the **load-balance method least-outstanding ignore-preferred-server** command if you have either of the following configurations:

- Dedicated authentication server and a separate dedicated accounting server
- Network where you can track all call record statistics and call record details, including start and stop records and records that are stored on separate servers

If you have a configuration where authentication servers are a superset of accounting servers, the preferred server is not used.

RADIUS Server Status and Automated Testing

The RADIUS Server Load Balancing feature considers the server status when assigning batches. Transaction batches are sent only to live servers. We recommend that you test the status of all RADIUS load-balanced servers, including low usage servers (for example, backup servers).

Transactions are not sent to a server that is marked dead. A server is marked dead until its timer expires, at which time it moves to quarantine state. A server is in quarantine until it is verified alive by the RADIUS automated tester functionality.

To determine if a server is alive and available to process transactions, the RADIUS automated tester sends a request periodically to the server for a test user ID. If the server returns an Access-Reject message, the server is alive; otherwise the server is either dead or quarantined.

A transaction sent to an unresponsive server is failed over to the next available server before the unresponsive server is marked dead. We recommend that you use the retry reorder mode for failed transactions.

When using the RADIUS automated tester, verify that the authentication, authorization, and accounting (AAA) servers are responding to the test packets that are sent by the network access server (NAS). If the servers are not configured correctly, packets may be dropped and the server erroneously marked dead.

Caution We recommend that you use a test user that is not defined on the RADIUS server for the RADIUS server automated testing to protect against security issues that may arise if the test user is not correctly configured.

Note Use the **test aaa group** command to check load-balancing transactions.

How to Configure RADIUS Server Load Balancing

Enabling Load Balancing for a Named RADIUS Server Group

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group-name*
4. **server ip-address [auth-port port-number] [acct-port port-number]**
5. **load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa group server radius** *group-name* **Example:** `Device(config)# aaa group server radius rad-sg`	Enters server group configuration mode.
Step 4	**server ip-address [auth-port port-number] [acct-port port-number]** **Example:** `Device (config-sg-radius)server 192.0.2.238 auth-port 2095 acct-port 2096`	Configures the IP address of the RADIUS server for the group server.
Step 5	**load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] **Example:** `Device(config-sg-radius)# load-balance method least-outstanding batch-size 30`	Enables the least-outstanding load balancing for a named server group.
Step 6	**end** **Example:** `Device(config-sg)# end`	Exits server group configuration mode and enters privileged EXEC mode.

Enabling Load Balancing for a Global RADIUS Server Group

The global RADIUS server group is referred to as "radius" in the authentication, authorization, and accounting (AAA) method lists.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**test username** *name*] [**auth-port** *number*] [**ignore-auth-port**] [**acct-port** *number*] [**ignore-acct-port**] [**idle-time** *seconds*]
4. **radius-server load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]
5. **load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server host** {*hostname* | *ip-address*} [**test username** *name*] [**auth-port** *number*] [**ignore-auth-port**] [**acct-port** *number*] [**ignore-acct-port**] [**idle-time** *seconds*] **Example:** `Device(config)# radius-server host 192.0.2.1 test username test1 idle-time 1`	Enables RADIUS automated testing.
Step 4	**radius-server load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] **Example:** `Device(config)# radius-server load-balance method least-outstanding`	Enables the least-outstanding load balancing for the global RADIUS server group and enters server group configuration mode. • The default batch size is 25. The batch size range is from 1 to 2147483647.
Step 5	**load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] **Example:** `Device(config-sg)# load-balance method least-outstanding batch-size 5`	Enables least-outstanding load balancing for a global named server group.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-sg)# end`	Exits server group configuration mode and enters privileged EXEC mode.

Troubleshooting RADIUS Server Load Balancing

After configuring the RADIUS Server Load Balancing feature, you can monitor the idle timer, dead timer, and load balancing server selection or verify the server status by using a manual test command.

SUMMARY STEPS

1. Use the **debug aaa test** command to determine when an idle timer or dead timer has expired, when test packets are sent, the status of the server, or to verify the server state.
2. Use the **debug aaa sg-server selection** command to determine the server that is selected for load balancing.
3. Use the **test aaa group** command to manually verify the RADIUS load-balanced server status.

DETAILED STEPS

Step 1 Use the **debug aaa test** command to determine when an idle timer or dead timer has expired, when test packets are sent, the status of the server, or to verify the server state.

The idle timer is used to check the server status and is updated with or without any incoming requests. Monitoring the idle timer helps to determine if there are nonresponsive servers and to keep the RADIUS server status updated to efficiently utilize available resources. For instance, an updated idle timer would help ensure that incoming requests are sent to servers that are alive.

The dead timer is used either to determine that a server is dead or to update a dead server's status appropriately.

Monitoring server selection helps to determine how often the server selection changes. Server selection is effective in analyzing if there are any bottlenecks, a large number of queued requests, or if only specific servers are processing incoming requests.

The following sample output from the **debug aaa test** command shows when the idle timer expired:

Example:

```
Device# debug aaa test

Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) quarantined.
Jul 16 00:07:01: AAA/SG/TEST: Sending test request(s) to server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Sending 1 Access-Requests, 1 Accounting-Requests in current batch.
Jul 16 00:07:01: AAA/SG/TEST(Req#: 1): Sending test AAA Access-Request.
Jul 16 00:07:01: AAA/SG/TEST(Req#: 1): Sending test AAA Accounting-Request.
Jul 16 00:07:01: AAA/SG/TEST: Obtained Test response from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Obtained Test response from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Necessary responses received from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) marked ALIVE. Idle timer set for 60
sec(s).
Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) removed from quarantine.
```

Step 2 Use the **debug aaa sg-server selection** command to determine the server that is selected for load balancing.

The following sample output from the **debug aaa sg-server selection** command shows five access requests being sent to a server group with a batch size of three:

Example:

```
Device# debug aaa sg-server selection

Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [3] transactions remaining in batch. Reusing server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [2] transactions remaining in batch. Reusing server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [1] transactions remaining in batch. Reusing server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: No more transactions in batch. Obtaining a new server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining a new least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[0] load: 3
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[1] load: 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[2] load: 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Selected Server[1] with load 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [3] transactions remaining in batch.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [2] transactions remaining in batch. Reusing server.
```

Step 3 Use the **test aaa group** command to manually verify the RADIUS load-balanced server status.

The following sample output shows the response from a load-balanced RADIUS server that is alive when the username “test” does not match a user profile. The server is verified alive when it issues an Access-Reject response to an authentication, authorization, and accounting (AAA) packet generated using the **test aaa group** command.

Example:

```
Device# test aaa group SG1 test lab new-code

00:06:07: RADIUS/ENCODE(00000000):Orig. component type = INVALID
00:06:07: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6 on-for-login-auth"
 is off
00:06:07: RADIUS(00000000): Config NAS IP: 192.0.2.4
00:06:07: RADIUS(00000000): sending
00:06:07: RADIUS/ENCODE: Best Local IP-Address 192.0.2.141 for Radius-Server 192.0.2.176
00:06:07: RADIUS(00000000): Send Access-Request to 192.0.2.176:1645 id 1645/1, len 50
00:06:07: RADIUS:  authenticator CA DB F4 9B 7B 66 C8 A9 - D1 99 4E 8E A4 46 99 B4
00:06:07: RADIUS:  User-Password       [2]   18  *
00:06:07: RADIUS:  User-Name           [1]   6   "test"
00:06:07: RADIUS:  NAS-IP-Address      [4]   6   192.0.2.141
00:06:07: RADIUS: Received from id 1645/1 192.0.2.176:1645, Access-Reject, len 44
00:06:07: RADIUS:  authenticator 2F 69 84 3E F0 4E F1 62 - AB B8 75 5B 38 82 49 C3
00:06:07: RADIUS:  Reply-Message       [18]  24
00:06:07: RADIUS:   41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66  [Authentication f]
00:06:07: RADIUS:   61 69 6C 75 72 65                               [failure]
00:06:07: RADIUS(00000000): Received from id 1645/1
00:06:07: RADIUS/DECODE: Reply-Message fragments, 22, total 22 bytes
```

Configuration Examples for RADIUS Server Load Balancing

Example: Enabling Load Balancing for a Global RADIUS Server Group

The following examples show how to enable load balancing for global RADIUS server groups. These examples are shown in three parts: the current configuration of the RADIUS command output, debug output, and authentication, authorization, and accounting (AAA) server status information. You can use delimiting characters to display relevant parts of the configuration.

The following example shows the relevant RADIUS configuration:

```
Device# show running-config | include radius

aaa authentication ppp default group radius
aaa accounting network default start-stop group radius
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

Lines in the current configuration of the preceding RADIUS command output are defined as follows:

- The **aaa authentication ppp** command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables the sending of all accounting requests to an AAA server when the client is authenticated and then disconnected through use of the **start-stop** keyword.
- The **radius-server host** command defines the IP address of the RADIUS server host with the authorization and accounting ports specified and the authentication and encryption keys identified.
- The **radius-server load-balance** command enables load balancing for global RADIUS server groups with the batch size specified.

The **show debug** sample output below shows the selection of the preferred server and the processing of requests for the configuration:

```
Device# show debug

General OS:
  AAA server group server selection debugging is on
#
<sending 10 pppoe requests>
Device#
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):Server (192.0.2.238:2095,2096) now being
```

```
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):Server (192.0.2.238:2015,2016) now being
 used as preferred server.
```

The following sample output from the **show aaa servers** command shows the AAA server status for the global RADIUS server group configuration:

The sample output shows the status of two RADIUS servers. Both servers are up and successfully processed in the last 2 minutes:

- Five out of six authentication requests
- Five out of five accounting requests

```
Device# show aaa servers

RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1841ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3303ms
             Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1955ms
             Transaction:success 5, failure 0
```

```
Author:request 0, timeouts 0
        Response:unexpected 0, server error 0, incorrect 0, time 0ms
        Transaction:success 0, failure 0
Account:request 5, timeouts 0
        Response:unexpected 0, server error 0, incorrect 0, time 3247ms
        Transaction:success 5, failure 0
Elapsed time since counters last cleared:2m
```

Example: Server Configuration and Enabling Load Balancing for Global RADIUS Server Group

The following example shows the relevant RADIUS configuration:

```
Device# show running-config | include radius

aaa authentication ppp default group radius
aaa accounting network default start-stop group radius
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

Lines in the current configuration of the RADIUS command output above are defined as follows:

- The **aaa authentication ppp** command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables the sending of all accounting requests to an authentication, authorization, and accounting (AAA) server when the client is authenticated and then disconnected by using the **start-stop** keyword .
- The **radius-server host** command defines the IP address of the RADIUS server host with the authorization and accounting ports specified and the authentication and encryption keys identified.
- The **radius-server load-balance** command enables load balancing for global RADIUS server groups with the batch size specified.

Example: Debug Output for Global RADIUS Server Group

The **debug** command output below shows the selection of the preferred server and the processing of requests for the configuration.

```
Device# show debug

General OS:
  AAA server group server selection debugging is on
#
<sending 10 pppoe requests>
Device#
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):Server (192.0.2.238:2095,2096) now being
```

```
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):Server (192.0.2.238:2015,2016) now being
 used as preferred server.
```

Example: Server Status Information for Global RADIUS Server Group

The following sample output from the **show aaa server** command shows the AAA server status for the global RADIUS server group configuration:

```
Device# show aaa server

RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1841ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3303ms
             Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1955ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3247ms
```

```
            Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
```

The sample output shows the status of two RADIUS servers. Both servers are up and successfully processed in the last 2 minutes:

- 5 out of 6 authentication requests
- 5 out of 5 accounting requests

Example: Enabling Load Balancing for a Named RADIUS Server Group

The following examples show load balancing enabled for a named RADIUS server group. These examples are shown in three parts: the current configuration of the RADIUS command output, debug output, and authentication, authorization, and accounting (AAA) server status information.

The following sample output shows the relevant RADIUS configuration:

```
Device# show running-config
.
.
.
aaa group server radius server-group1
 server 192.0.2.238 auth-port 2095 acct-port 2096
 server 192.0.2.238 auth-port 2015 acct-port 2016
 load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
.
.
Device(config-sg-radius)# load-balance method least-outstanding batch-size 30
```

The lines in the current configuration of the preceding RADIUS command output are defined as follows:

- The **aaa group server radius** command shows the configuration of a server group with two member servers.
- The **load-balance** command enables load balancing for global RADIUS server groups with the batch size specified.
- The **aaa authentication ppp** command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables sending of all accounting requests to the AAA server when the client is authenticated and then disconnected using the **start-stop** keyword.

The show debug sample output below shows the selection of the preferred server and the processing of requests for the preceding configuration:

```
Device# show debug

*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
```

```
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.
```

The following sample output from the **show aaa servers** command shows the AAA server status for the named RADIUS server group configuration:

The sample output shows the status of two RADIUS servers. Both servers are alive, and no requests have been processed since the counters were cleared 0 minutes ago.

```
Device# show aaa servers

RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
```

```
            Response:unexpected 0, server error 0, incorrect 0, time 0ms
            Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
            Response:unexpected 0, server error 0, incorrect 0, time 0ms
            Transaction:success 0, failure 0
     Author:request 0, timeouts 0
            Response:unexpected 0, server error 0, incorrect 0, time 0ms
            Transaction:success 0, failure 0
     Account:request 0, timeouts 0
            Response:unexpected 0, server error 0, incorrect 0, time 0ms
            Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
```

Example: Server Configuration and Enabling Load Balancing for Named RADIUS Server Group

The following sample output shows the relevant RADIUS configuration:

```
Device# show running-config
.
.
.
aaa group server radius server-group1
 server 192.0.2.238 auth-port 2095 acct-port 2096
 server 192.0.2.238 auth-port 2015 acct-port 2016
 load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
.
.
```

The lines in the current configuration of the RADIUS command output above are defined as follows:

- The **aaa group server radius** command shows the configuration of a server group with two member servers.
- The **load-balance** command enables load balancing for global RADIUS server groups with the batch size specified.
- The **aaa authentication ppp** command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables sending of all accounting requests to the AAA server when the client is authenticated and then disconnected using the **start-stop** keyword.

Example: Debug Output for Named RADIUS Server Group

The debug sample output below shows the selection of preferred server and processing of requests for the configuration above.

```
Device# show debug

*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
```

```
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.
```

Example: Server Status Information for Named RADIUS Server Group

The following sample output from the **show aaa servers** command shows the AAA server status for the named RADIUS server group configuration:

```
Device# show aaa servers

RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
```

```
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
```

The sample output shows the status of two RADIUS servers. Both servers are alive, and no requests have been processed since the counters were cleared 0 minutes ago.

Example: Monitoring Idle Timer

The following example shows idle timer and related server state for load balancing enabled for a named RADIUS server group. The current configuration of the RADIUS command output and debug command output are also displayed.

The following sample output shows the relevant RADIUS configuration:

```
Device# show running-config | include radius

aaa group server radius server-group1
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 test username junk1 idle-time
 1 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 test username junk1 idle-time
 1 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

The lines in the current configuration of the preceding RADIUS command output are defined as follows:

- The **aaa group server radius** command shows the configuration of a server group.
- The **radius-server host** command defines the IP address of the RADIUS server host with authorization and accounting ports specified and the authentication and encryption key identified.
- The **radius-server load-balance** command enables load balancing for the RADIUS server with the batch size specified.

The **show debug** sample output below shows test requests being sent to servers. The response to the test request sent to the server is received, the server is removed from quarantine as appropriate, the server is marked alive, and then the idle timer is reset.

```
Device# show debug

*Feb 28 13:52:20.835:AAA/SG/TEST:Server (192.0.2.238:2015,2016) quarantined.
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending test request(s) to server (192.0.2.238:2015,2016)
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending 1 Access-Requests, 1 Accounting-Requests in current
```

```
 batch.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Access-Request.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Accounting-Request.
*Feb 28 13:52:21.087:AAA/SG/TEST:Obtained Test response from server (192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Obtained Test response from server (192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Necessary responses received from server
(192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) marked ALIVE. Idle timer
set for 60 secs(s).
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) removed from quarantine.
.
.
.
```

Example: Server Configuration and Enabling Load Balancing for Idle Timer Monitoring

The following sample output shows the relevant RADIUS configuration:

```
Device# show running-config | include radius

aaa group server radius server-group1
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 test username junk1 idle-time
 1 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 test username junk1 idle-time
 1 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

The lines in the current configuration of the RADIUS command output above are defined as follows:

- The **aaa group server radius** command shows the configuration of a server group.
- The **radius-server host** command defines the IP address of the RADIUS server host with authorization and accounting ports specified and the authentication and encryption key identified.
- The **radius-server load-balance** command enables load balancing for the RADIUS server with the batch size specified.

Example: Debug Output for Idle Timer Monitoring

The **debug** command output below shows test requests being sent to servers. The response to the test request sent to the server is received, the server is removed from quarantine as appropriate, marked alive, and then the idle timer is reset.

```
Device# show debug
*Feb 28 13:52:20.835:AAA/SG/TEST:Server (192.0.2.238:2015,2016) quarantined.
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending test request(s) to server (192.0.2.238:2015,2016)
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending 1 Access-Requests, 1 Accounting-Requests in current
 batch.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Access-Request.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Accounting-Request.
*Feb 28 13:52:21.087:AAA/SG/TEST:Obtained Test response from server (192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Obtained Test response from server (192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Necessary responses received from server
(192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) marked ALIVE. Idle timer
set for 60 secs(s).
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) removed from quarantine.
.
.
.
```

Example: Configuring the Preferred Server with the Same Authentication and Authorization Server

The following example shows an authentication server group and an authorization server group that use the same servers 209.165.200.225 and 209.165.200.226. Both server groups have the preferred server flag enabled.

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
aaa group server radius accounting-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
```

When a preferred server is selected for a session, all transactions for that session will continue to use the original preferred server. The servers 209.165.200.225 and 209.165.200.226 are load balanced based on sessions rather than transactions.

Example: Configuring the Preferred Server with Different Authentication and Authorization Servers

The following example shows an authentication server group that uses servers 209.165.200.225 and 209.165.200.226 and an authorization server group that uses servers 209.165.201.1 and 209.165.201.2. Both server groups have the preferred server flag enabled.

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
aaa group server radius accounting-group
   server 209.165.201.1 key radkey3
   server 209.165.201.2 key radkey4
```

The authentication server group and the accounting server group do not share any common servers. A preferred server is never found for accounting transactions; therefore, authentication and accounting servers are load-balanced based on transactions. Start and stop records are sent to the same server for a session.

Example: Configuring the Preferred Server with Overlapping Authentication and Authorization Servers

The following example shows an authentication server group that uses servers 209.165.200.225, 209.165.200.226, and 209.165.201.1 and an accounting server group that uses servers 209.165.201.1 and 209.165.201.2. Both server groups have the preferred server flag enabled.

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
   server 209.165.201.1 key radkey3
aaa group server radius accounting-group
   server 209.165.201.1 key radkey3
   server 209.165.201.2 key radkey4
```

If all servers have equal transaction processing capability, one-third of all authentication transactions are directed toward the server 209.165.201.1. Therefore, one-third of all accounting transactions are also directed toward the server 209.165.201.1. The remaining two-third of accounting transactions are load balanced equally between servers 209.165.201.1 and 209.165.201.2. The server 209.165.201.1 receives fewer authentication transactions because the server 209.165.201.1 has outstanding accounting transactions.

Example: Configuring the Preferred Server with Authentication Servers As a Subset of Authorization Servers

The following example shows an authentication server group that uses servers 209.165.200.225 and 209.165.200.226 and an authorization server group that uses servers 209.165.200.225, 209.165.200.226, and 209.165.201.1. Both server groups have the preferred server flag enabled.

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
aaa group server radius accounting-group
  server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
   server 209.165.201.1 key radkey3
```

One-half of all authentication transactions are sent to the server 209.165.200.225 and the other half to the server 209.165.200.226. Servers 209.165.200.225 and 209.165.200.226 are preferred servers for authentication and accounting transaction. Therefore, there is an equal distribution of authentication and accounting transactions across servers 209.165.200.225 and 209.165.200.226. The server 209.165.201.1 is relatively unused.

Example: Configuring the Preferred Server with Authentication Servers As a Superset of Authorization Servers

The following example shows an authentication server group that uses servers 209.165.200.225, 209.165.200.226, and 209.165.201.1 and an authorization server group that uses servers 209.165.200.225 and 209.165.200.226. Both server groups have the preferred server flag enabled.

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
   server 209.165.201.1 key radkey3
aaa group server radius accounting-group
  server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
```

Initially, one-third of authentication transactions are assigned to each server in the authorization server group. As accounting transactions are generated for more sessions, accounting transactions are sent to servers 209.165.200.225 and 209.165.200.226 because the preferred server flag is on. As servers 209.165.200.225 and 209.165.200.226 begin to process more transactions, authentication transactions will start to be sent to server 209.165.201.1. Transaction requests authenticated by server 209.165.201.1 do not have any preferred server setting and are split between servers 209.165.200.225 and 209.165.200.226, which negates the use of the preferred server flag. This configuration should be used cautiously.

Additional References for RADIUS Server Load Balancing

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z
AAA and RADIUS	*Authentication, Authorization, and Accounting Configuration Guide*
AAA server groups and RADIUS configuration	"Configuring RADIUS" module in the *RADIUS Configuration Guide*
Failover retry reorder mode	"RADIUS Server Reorder on Failure" module in the *RADIUS Configuration Guide*

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

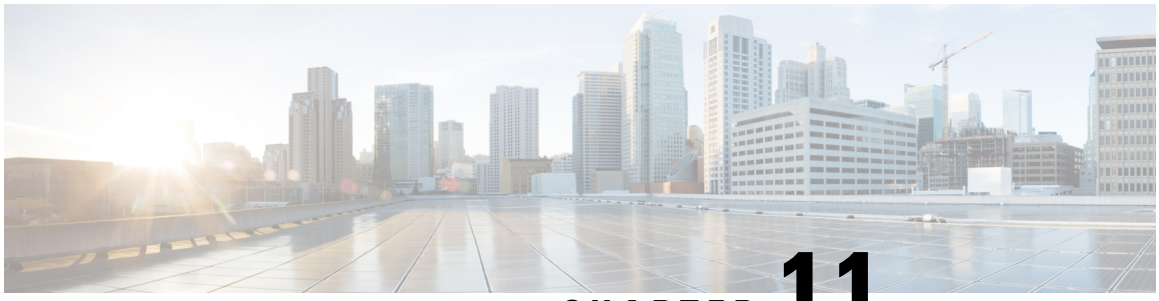
Feature Information for RADIUS Server Load Balancing

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 13: Feature Information for RADIUS Server Load Balancing

Feature Name	Releases	Feature Information
RADIUS Server Load Balancing	12.2(28)SB 12.4(11)T 12.2(33)SRC	The RADIUS Server Load Balancing feature distributes authentication, authorization, and accounting (AAA) authentication and accounting transactions across servers in a server group. These servers can then share the transaction load, resulting in faster responses to incoming requests by optimally using available servers. This feature was integrated into Cisco IOS Release 12.2(28)SB. This feature was integrated into Cisco IOS Release 12.4(11)T. This feature was integrated into Cisco IOS Release 12.2(33)SRC. The following commands were introduced or modified: **debug aaa sg-server selection**, **debug aaa test**, **load-balance (server-group)**, **radius-server host**, **radius-server load-balance**, **test aaa group.**
RADIUS Server Load Balancing porting	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 series routers.



CHAPTER 11

RADIUS Server Reorder on Failure

The RADIUS Server Reorder on Failure feature provides for failover to another server in the server group during periods of high load or when server failure occurs. Subsequent to the failure, all RADIUS traffic is directed to the new server. Traffic is switched from the new server to another server in the server group only if the new server also fails. Traffic is not automatically switched back to the first server.

By spreading the RADIUS transactions across multiple servers, authentication and accounting requests are serviced more quickly.

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 Server Reorder on Failure

- Before you can configure your RADIUS server to perform reorder on failure, you must enable authentication, authorization, and accounting (AAA) by using the **aaa new-model**command.
- You must also have RADIUS configured, for functions such as authentication, accounting, or static route download.

Restrictions for RADIUS Server Reorder on Failure

- An additional 4 bytes of memory is required per server group. However, because most server configurations have only a small number of server groups configured, the additional 4 bytes should have a minimal impact on performance.
- Some RADIUS features within the software set may not be capable of using this feature. If a RADIUS feature cannot use the RADIUS Server Reorder on Failure feature, your server behaves as though the reorder feature is not configured.

Information About RADIUS Server Reorder on Failure

RADIUS Server Failure

If the RADIUS Server Reorder on Failure feature is not configured and server failure occurs:

1. A new RADIUS transaction has to be performed.
2. A RADIUS packet for the transaction is sent to the first server in the group that is not marked dead (as per the configured deadtime) and is retransmitted for the configured number of retransmissions.
3. If all of those retransmits time out (as per the configured timeout), the router transmits the packet to the next nondead server in the list for the configured number of retransmissions.
4. Step 3 is repeated until the specified maximum number of transmissions per transaction have been made. If the end of the list is reached before the maximum number of transmissions has been reached, the router goes back to the beginning of the list and continue from there.

If at any time during this process, a server meets the dead-server detection criteria (not configurable; it varies depending on the version of software being used), the server is marked as dead for the configured deadtime.

How the RADIUS Server Reorder on Failure Feature Works

If you have configured the RADIUS Server Reorder on Failure feature, the decision about which RADIUS server to use as the initial server is as follows:

- The network access server (NAS) maintains the status of “flagged” server, which is the first server to which a transmission is sent.
- After the transmission is sent to the flagged server, the transmission is sent to the flagged server again for the configured number of retransmissions.
- The NAS then sequentially sends the transmission through the list of nondead servers in the server group, starting with the one listed after the flagged server, until the configured transaction maximum tries is reached or until a response is received.
- At boot time, the flagged server is the first server in the server group list as was established using the **radius-server host** command.

- If the flagged server is marked as dead (even if the dead time is zero), the first nondead server listed after the flagged server becomes the flagged server.
- If the flagged server is the last server in the list, and it is marked as dead, the flagged server becomes the first server in the list that is not marked as dead.
- If all servers are marked as dead, the transaction fails, and no change is made to the flagged server.
- If the flagged server is marked as dead, and the dead timer expires, nothing happens.

Note Some types of transmissions (for example, Challenge Handshake Authentication Protocol [CHAP], Microsoft CHAP [MS-CHAP], and Extensible Authentication Protocol [EAP]) require multiple roundtrips to a single server. For these special transactions, the entire sequence of roundtrips to the server are treated as though they were one transmission.

When RADIUS Servers Are Dead

A server can be marked as dead if the criteria in 1 and 2 are met:

1. The server has not responded to at least the configured number of retransmissions as specified by the **radius-server transaction max-tries** command.
2. The server has not responded to any request for at least the configured timeout. The server is marked dead only if both criteria (this and the one listed above) are met. The marking of a server as dead, even if the dead time is zero, is significant for the RADIUS server retry method reorder system.

How to Configure RADIUS Server Reorder on Failure

Configuring a RADIUS Server to Reorder on Failure

Perform this task to configure a server in a server group to direct traffic to another server in the server group when the first server fails.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server retry method reorder**
5. **radius-server retransmit** {*retries*}
6. **radius-server transaction max-tries {** *number* **}**
7. **radius-server host { ***hostname* **|** *ip-address* **} [key** *string* **]**
8. **radius-server host { ***hostname* **|** *ip-address* **} [key** *string* **]**

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 new-model** **Example:** `Router (config)# aaa new-model`	Enables the AAA access control model.
Step 4	**radius-server retry method reorder** **Example:** **Example:** `Router (config)# radius-server retry method reorder`	Specifies the reordering of RADIUS traffic retries among a server group.
Step 5	**radius-server retransmit** {*retries*} **Example:** `Router (config)# radius-server retransmit 1`	Specifies the number of times the Cisco IOS XE software searches the list of RADIUS server hosts before giving up. The *retries* argument is the maximum number of retransmission attempts. The default is 3 attempts.
Step 6	**radius-server transaction max-tries {** *number* **}** **Example:** `Router (config)# radius-server transaction max-tries 3`	Specifies the maximum number of transmissions per transaction that may be retried on a RADIUS server. The *number* argument is the total number of transmissions per transaction. If this command is not configured, the default is eight transmissions. **Note** This command is global across all RADIUS servers for a given transaction.
Step 7	**radius-server host {** *hostname* **|** *ip-address* **} [key** *string* **]** **Example:** `Router (config)# radius-server host 10.2.3.4 key radi23`	Specifies a RADIUS server host. **Note** You can also configure a global key for all RADIUS servers that do not have a per-server key configured by issuing the **radius-server key** command.
Step 8	**radius-server host {** *hostname* **|** *ip-address* **} [key** *string* **]**	Specifies a RADIUS server host. **Note** At least two servers must be configured.

	Command or Action	Purpose
	Example: `Router (config)# radius-server host 10.5.6.7 key rad234`	

Monitoring RADIUS Server Reorder on Failure

To monitor the server-reorder-on-failure process on your router, use the following commands:

SUMMARY STEPS

1. **enable**
2. **debug aaa sg-server selection**
3. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug aaa sg-server selection** **Example:** `Router# debug aaa sg-server selection`	Displays information about why the RADIUS and TACAC+ server group system in the router is choosing a particular server.
Step 3	**debug radius** **Example:** `Router# debug radius`	Displays information about why the router is choosing a particular RADIUS server.

Example

Debug 1

Debug 2

The following two debug outputs display the behavior of the RADIUS Server Reorder on Failure feature:

In the following sample output, the RADIUS Server Reorder on Failure feature is configured. The server retransmits are set to 0 (so each server is tried just one time before failover to the next configured server), and the transmissions per transaction are set to 4 (the transmissions stop on the

third failover). The third server in the server group (10.107.164.118) has accepted the transaction on the third transmission (second failover).

```
00:38:35: %SYS-5-CONFIG-I: Configured from console by console
00:38:53: RADIUS/ENCODE(OOOOOOOF) : ask "Username: "
00:38:53: RADIUS/ENCODE (0000000F) : send packet; GET-USER
00:38:58: RADIUS/ENCODE (0000000F) : ask "Password: "
00:38:58: RADIUS/ENCODE(0000000F) : send packet; GET-PASSWORD
00:38:59: RADIUS: AAA Unsupported [152] 4
00:38:59: RADIUS: 7474 [tt]
00:38:59: RADIUS (0000000F) : Storing nasport 2 in rad-db
00:38:59: RADIUS/ENCODE(0000000F) : dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:38:59: RADIUS (0000000F) : Config NAS IP: 0.0.0.0
00:38:59: RADIUS/ENCODE (0000000F) : acct-session-id: 15
00:38:59: RADIUS (0000000F) : sending
00:38:59: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 192.1.1.1
00:38:59: RAPIUS(0000000F) : Send Access-Request to 10.10.10.10:1645 id 21645/11, len 78
00:38:59: RADIUS:: authenticator 4481 E6 65 2D 5F 6F OA -lE F5 81 8F 4E 1478 9C
00:38:59: RADIUS: User-Name [1] 7 "username1"
00:38:59: RADIUS: User-Password [2] 18 *
00:38:59: RADIUS: NAS-Port fSl 6 2
00:~8:59: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
00:38:59: RADIUS: Calling-Station-Id [31] 15 "10.19.192.23"
00:39:00: RADIUS: NAS-IP-Address [4] 6 10.0.1.130
00:39:02: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/11
00:39:02: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 192.2.2.2
00:39:04: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/11
00:39:04: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 128.107.164.118
00:39:05: RADIUS: Received from id 21645/11 10.107.164.118:1645, Access-Accept, len 26
00:39:05: RADIUS: authenticator 5609 56 F9 64 4E DF 19- F3 A2 DD 73 EE 3F 9826
00:39:05: RADIUS: Service-Type [6] 6 Login [1]
```

In the following sample output, the RADIUS Server Reorder on Failure feature is configured. The server retransmits are set to 0, and the transmissions per transaction are set to 8. In this transaction, the transmission to server 10.10.10.0 has failed on the eighth transmission.

```
00:42:30: RADIUS(00000011): Received from id 21645/13
00:43:34: RADIUS/ENCODE(00000012) : ask "Username: "
00:43:34: RADIUS/ENCODE(00000012) : send packet; GET-USER
00:43:39: RADIUS/ENCODE(00000012) : ask "Password: "
00:43:39: RADIUS/ENCODE(00000012) : send packet; GET-PASSWORD
00:43:40: RADIUS: AAA Unsupported [152] 4
00:43:40: RADIUS: 7474 [tt]
00:43:40: RADIUS(00000012) : Storing nasport 2 in rad-db
00:43:40: RADIUS/ENCODE(00000012): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:43:40: RADIUS(00000012) : Co~fig NAS IP: 0.0.0.0
00:43:40: RADIUS/ENCODE(00000012) : acct-session-id: 18
00:43:40: RADIUS(00000012) : sending
00:43:40: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
 00:43:40: RADIUS(00000012) : Send Access-Request to 10.107.164.118:1645 id 21645/14, len
78 00:43:40: RADIUS: authenticator B8 OA 51 3A AF A6 0018 -B3 2E 94 5E 07 OB 2A IF 00:43:40:
 RADIUS: User-Name [1] 7 "username1" 00:43:40: RADIUS: User-Password [2] 18 * 00:43:40:
RADIUS: NAS-Port [5] 6 2
00:43:40: RADIUS: NAS-Port-Type [61] 6 Virtual [5] 00:43:40: RADIUS: Calling-Station-]d
[31] 15 "172.19.192.23" 00:43:40: RADIUS: NAS-IP-Address [4] 6 10.0.1.130
00:43:42: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:42: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1 00:43:44:
 RADius: Fail-over to (10.2.2.2:1645,1646) for id 21645/14
00:43:44: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.2.2.2 00:43:46:
 RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/14
```

```
00:43:46: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
 00:43:48: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:48: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1 00:43:50:
 RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/14
00:43:50: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.2.2.2 00:43:52:
 RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/14
00:43:52: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
 00:43:54: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:54: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1 00:43:56:
 RADIUS: No response from (10.10.10.10:1645,1646) for id 21645/14 00:43:56: RADIUS/DECODE:
 parse response no app start; FAIL 00:43:56: RADIUS/DECODE: parse response; FAIL
```

Configuration Examples for RADIUS Server Reorder on Failure

Configuring a RADIUS Server to Reorder on Failure Example

The following configuration example shows that a RADIUS server is configured to reorder on failure. The maximum number of transmissions per transaction that may be retried on the RADIUS server is six.

```
aaa new-model

radius-server retry method reorder

radius-server retransmit 0

radius-server transaction max-tries 6

radius-server host 10.2.3.4 key rad123

radius-server host 10.5.6.7 key rad123
```

Determining Transmission Order When RADIUS Servers Are Dead

If at boot time you have configured the following:

```
Router(config)# aaa new-model
Router(config)# radius-server retry method reorder
Router(config)# radius-server retransmit 0
Router(config)# radius-server transaction max-tries 6
Router(config)# radius-server host 10.2.3.4
Router(config)# radius-server host 10.5.6.7
```

and both servers are down, but not yet marked dead, for the first transaction you would see the transmissions as follows:

```
10.2.3.4
10.5.6.7
10.2.3.4
10.5.6.7
10.2.3.4
10.5.6.7
```

If you configure the reorder as follows:

```
Router(config)# aaa new-model
Router(config)# radius-server retry method reorder
Router(config)# radius-server retransmit 1
Router(config)# radius-server transaction max-tries 3
Router(config)# radius-server host 10.2.3.4
Router(config)# radius-server host 10.4.5.6
```

and both RADIUS servers are not responding to RADIUS packets but are not yet marked dead (as after the NAS boots), the transmissions for the first transaction are as follows:

```
10.2.3.4
10.2.3.4
10.4.5.6
```

Subsequent transactions may be transmitted according to a different pattern. The transmissions depend on whether the criteria for marking one (or both) servers as dead have been met, and as per the server flagging pattern already described.

If you configure the reorder as follows:

```
Router(config)# aaa new-model
Router(config)# radius-server retry method reorder
Router(config)# radius-server retransmit 1
Router(config)# radius-server max-tries-per-transaction 8
Router(config)# radius-server host 10.1.1.1
Router(config)# radius-server host 10.2.2.2
Router(config)# radius-server host 10.3.3.3
Router(config)# radius-server timeout 3
```

And the RADIUS server 10.1.1.1 is not responding to RADIUS packets but is not yet marked as dead, and the remaining two RADIUS servers are live, you see the following:

For the first transaction:

```
10.1.1.1
10.1.1.1
10.2.2.2
```

For any additional transaction initiated for any transmissions before the server is marked as dead:

```
10.1.1.1
10.1.1.1
10.2.2.2
```

For transactions initiated thereafter:

```
10.2.2.2
```

If servers 10.2.2.2 and 10.3.3.3 then go down as well, you see the following transmissions until servers 10.2.2.2 and 10.3.3.3 meet the criteria for being marked as dead:

```
10.2.2.2
10.2.2.2
10.3.3.3
10.3.3.3
10.1.1.1
10.1.1.1
```

```
10.2.2.2
10.2.2.2
```

The above is followed by the failure of the transmission and by the next method in the method list being used (if any).

If servers 10.2.2.2 and 10.3.3.3 go down but server 10.1.1.1 comes up at the same time, you see the following:

```
10.2.2.2
10.2.2.2
10.3.3.3
10.3.3.3
10.1.1.1
```

When servers 10.2.2.2 and 10.3.3.3 are then marked as dead, you see the following:

```
10.1.1.1
```

Additional References

Related Documents

Related Topic	Document Title
RADIUS	"Configuring RADIUS" in the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2
AAA and RADIUS commands	*Cisco IOS Security Command Reference*
Enabling AAA	Authentication, Authorization, and Accounting (AAA) section of the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2.
Security commands	*Cisco IOS Security Command Reference*

Standards

Standards	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

RFCs	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

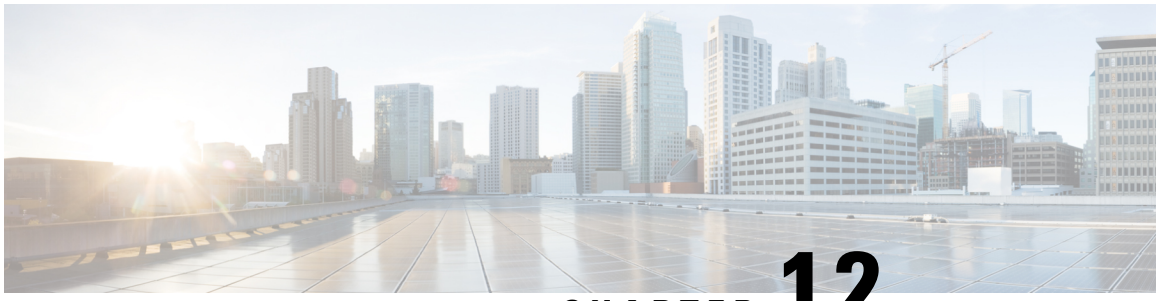
Feature Information for RADIUS Server Reorder on Failure

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 14: Feature Information for RADIUS Server Reorder on Failure

Feature Name	Releases	Feature Information
RADIUS Server Reorder on Failure	Cisco IOS XE Release 2.1	The RADIUS Server Reorder on Failure feature provides for failover to another server in the server group during periods of high load or when server failure occurs. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified by this feature: **debug aaa sg-server selection, radius-server retry method reorder, radius-server transaction max-tries.**



CHAPTER 12

RADIUS Separate Retransmit Counter for Accounting

The RADIUS: Separate Retransmit Counter for Accounting feature allows users to configure an exponential backoff retransmit. That is, after the normally configured retransmission retries have been used, the router will keep on trying with an interval that doubles on each retransmission failure until a configured maximum interval is reached. This functionality allows users to retransmit accounting requests for many hours without overloading the RADIUS server when it does come back up.

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.

Restrictions for RADIUS Separate Retransmit Counter for Accounting

The following tasks will result in excessive memory consumption on the router:

- Configuring this feature on a router with a high call rate.

- Configuring the **aaa accounting send stop-record authentication failure** command: an accounting record and a RADIUS packet will be generated for each user that fails to authenticate while the RADIUS server is down.
- Configuring interim accounting: new accounting records are generated and stored on the router.

Information About RADIUS Separate Retransmit Counter for Accounting

How Retransmission of Accounting Requests Works

In many environments, a single RADIUS server is used for authentication and accounting. Whenever this server is down for approximately 24 hours, the accounting records of users already on the router are lost after authentication, authorization, and accounting (AAA) does all the retransmissions. Before the introduction of this feature, the retransmissions could be configured for a maximum of 100 retries and the timeout could be configured for 1,000 seconds. Although these configurations keep the accounting records on the router for 24 hours, a timeout of 1,000 seconds is unreasonable, causing problems when the RADIUS server cannot be reached due to network congestion.

The RADIUS: Separate Retransmit Counter for Accounting feature allows users to configure an exponential backoff retransmit. That is, after the normally configured retransmission retries have been used, the router will keep on trying with an interval that doubles on each retransmission failure until a configured maximum interval is reached. This functionality allows users to retransmit accounting requests for many hours without overloading the RADIUS server when it does come back up.

This feature can be configured globally (via the **radius-server backoff exponential** command), per server (via the **radius-server host** command), or per group (via the **backoff exponential** command).

Benefits

With this feature, users can extend the time in which the RADIUS client (the router) sends accounting requests to the RADIUS server in the event that the RADIUS server or the connection to the server is down and there is no accounting response confirmation. This functionality enables accounting records to remain on the router for up to 24 hours.

How to Configure RADIUS Separate Retransmit Counter for Accounting

Configuring a Retransmit Counter for Accounting Globally or per RADIUS Host

To configure exponential backoffs of RADIUS retransmits over an extended period of time on a global basis and per RADIUS host, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router(config)# **radius-server backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *retransmits*
4. Router(config)# **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*] [**backoff exponential** {**backoff-retry** *number-of-retransmits* | **key** *encryption-key* | **max-delay** *minutes*}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Router(config)# **radius-server backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *retransmits* **Example:** `Router (config)# radius-server backoff exponential max-delay 60 backoff-retry 32`	Configures the router for exponential backoff retransmit of accounting requests.
Step 4	Router(config)# **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*] [**backoff exponential** {**backoff-retry** *number-of-retransmits* | **key** *encryption-key* | **max-delay** *minutes*}] **Example:** `Router (config)# radius-server host 192.0.2.1 test username test1 auth-port 1645 acct-port 1646`	Specifies a RADIUS server host and configures that RADIUS server host for exponential backoff retransmit of accounting requests.

Configuring a Retransmit Counter for Accounting per RADIUS Server Group

To configure exponential backoffs of RADIUS retransmits over an extended period of time per RADIUS server group, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa group server radius** *group-name*
4. Router(config -sg-radius)# **backoff exponential max-delay** *minutes*] [**backoff-retry** *retransmits*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router (config)# configure terminal`	Enters global configuration mode.
Step 3	Router(config)# **aaa group server radius** *group-name*	Groups different RADIUS server hosts into distinct lists and distinct methods and enters server-group RADIUS configuration mode.
Step 4	Router(config -sg-radius)# **backoff exponential max-delay** *minutes*] [**backoff-retry** *retransmits*	Configures the router for exponential backoff retransmit of accounting requests per RADIUS server group.

Verifying Retransmit Configurations

To verify feature functionality, use any of the following EXEC commands:

SUMMARY STEPS

1. **enable**
2. **debug radius**
3. **show accounting**
4. **show radius statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug radius** **Example:**	Displays information associated with RADIUS.

	Command or Action	Purpose
	`Router# debug radius`	
Step 3	**show accounting** **Example:** `Router# show accounting`	Displays all active sessions and prints all the accounting records for actively accounted functions.
Step 4	**show radius statistics** **Example:** `Router# show radius statistics`	Displays the RADIUS statistics for accounting packets.

Configuration Examples for RADIUS Separate Retransmit Counter for Accounting

This section provides the following configuration examples:

Retransmit Counter for Accounting Comprehensive Configuration Example

The following example shows how to configure your router for exponential backoff retransmit of accounting requests. In this example, an exponential backoff is configured globally (via the **radius-server backoff exponential** command) and for the RADIUS server host "172.107.164.206" (via the **radius-server host** command).

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization exec default group radius
aaa authorization network default group radius
aaa accounting send stop-record authentication failure
aaa accounting update periodic 1
aaa accounting network default start-stop group radius
!
radius-server host 172.107.164.206 auth-port 1645 acct-port 1646 backoff exponential max-delay
 60 backoff-retry 32
radius-server backoff exponential max-delay 60 backoff-retry 32
radius-server retransmit 3
radius-server key rad123
end
```

Per-Server Configuration Example

The following example shows how to enable exponential backoff retransmits on a per-server basis. In this example, assume that the retransmit is configured for 3 retries and the timeout is configured for 5 seconds; that is, the RADIUS request will be transmitted 3 times with a delay of 5 seconds. Thereafter, the router will continue to retransmit RADIUS requests with a delayed interval that doubles each time until 32 retries have

been achieved. The router will stop doubling the retransmit intervals after the interval surpasses the configured 60 minutes; it will transmit every 60 minutes.

```
radius-server host foo.xyz.com backoff exponential max-delay 60 backoff-retry 32
```

After enabling this command, the retransmits will be sent as follows ("t" equals seconds):

```
t = 0 req sent
t = 5 retrans 1
t = 10 retrans 2
t = 15 retrans 3
t = 25 retrans 4
t = 45 retrans 5
t = 85 retrans 6
t = 165 retrans 7
t = 325 retrans 8
t = 645 retrans 9
t = 1285 retrans 10
t= 2565 retrans 11
t = 5125 retrans 12
t = 8725 retrans 13 (The interval has stabilized to 60 minutes here).
t = 12325 retrans 14 till retransmit 35
```

After all the retransmits are sent, the RADIUS request follows the same path that it would when all the normal retransmits are done.

Additional References

The following sections provide references related to the RADIUS: Separate Retransmit Counter for Accounting.

Related Documents

Related Topic	Document Title
RADIUS and AAA accounting configuration tasks and commands	• The chapters "Configuring RADIUS" and "Configuring Accounting" in th e *Cisco IOS XE Security Configuration Guide: Configuring User Services* , Release 2 • 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

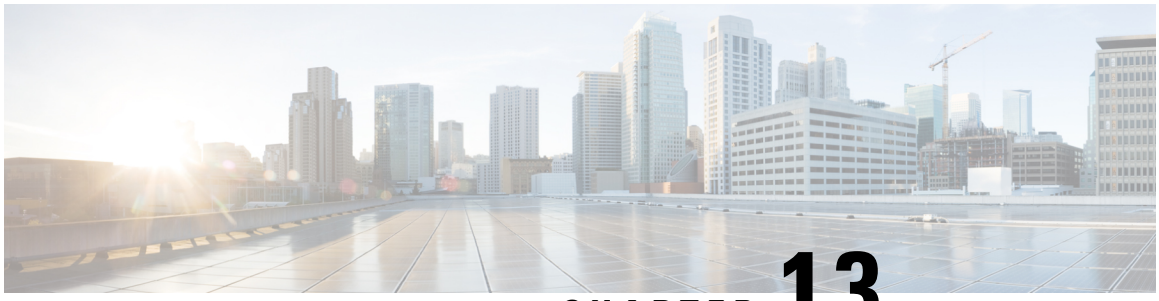
Feature Information for RADIUS Separate Retransmit Counter for Accounting

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 15: Feature Information for RADIUS: Separate Retransmit Counter for Accounting

Feature Name	Releases	Feature Information
RADIUS: Separate Retransmit Counter for Accounting	Cisco IOS XE Release 2.1	The RADIUS: Separate Retransmit Counter for Accounting feature allows users to configure an exponential backoff retransmit. That is, after the normally configured retransmission retries have been used, the router will keep on trying with an interval that doubles on each retransmission failure until a configured maximum interval is reached. This functionality allows users to retransmit accounting requests for many hours without overloading the RADIUS server when it does come back up. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **backoff exponential**, **radius-server host**, **radius-server backoff exponential**.



CHAPTER 13

RADIUS VC Logging

RADIUS Virtual Circuit (VC) Logging allows the Cisco IOS XE to accurately record the virtual path interface (VPI) and virtual circuit interface (VCI) of an incoming subscriber session.

With RADIUS VC Logging enabled, the RADIUS network access server (NAS)-port field is extended and modified to carry VPI/VCI information. This information is logged in the RADIUS accounting record that was created at session startup.

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.

How to Configure RADIUS VC logging

Configuring the NME Interface IP Address on the NSP

The NAS-IP-Address field in the RADIUS accounting packet contains the IP address of the Network Management Ethernet (NME) port on the Network Service provider (NSP), even if the NME is shut down. If your Network Route Processor (NRP) does not use a DHCP server to obtain an IP address, you must configure a static IP address. Perform the following steps to configure a static combined NME IP address.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface BVI** *bridge-group*
4. **ip address** *address subnet*
5. **exit**

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	**interface BVI** *bridge-group* **Example:** `Router(config)# interface BVI1`	Selects the combined Bridge-Group Virtual Interface (BVI) NME interface and enters interface configuration mode.
Step 4	**ip address** *address subnet* **Example:** `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	Configures a static IP and subnetwork address.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits interface configuration mode.

Configuring the NME IP address

You can use the Gigabit Ethernet port as a separate NME interface instead of the combined NME interface. Perform the following steps to configure the NME IP address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface GigabitEthernet** *number*
4. **ip address** *address mask*
5. **exit**

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	**interface GigabitEthernet** *number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Selects the NME interface.
Step 4	**ip address** *address mask* **Example:** `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	Configures a static IP and subnetwork address. **Note** You must configure the NME IP address before configuring PVCs on the NRP. Otherwise the NAS-IP-Address field in the RADIUS accounting packet will contain an incorrect IP address.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.

Configuring RADIUS VC Logging on the NRP

Perform the following steps to configure RADIUS VC logging.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute nas-port format d**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute nas-port format d** **Example:** `Router(config)# radius-server attribute nas-port format d`	Selects the ATM VC (virtual circuit) extended format for the NAS port field.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits interface configuration mode.

Verifying the NME Interface IP Address

To verify the NME IP address, enter the **show interface bvi1** or **show interface e0/0/0**EXEC command on the NSP. Check the Internet address statement (indicated with an arrow).

```
Router# show interface bvi1BVI1 is up, line protocol is up
  Hardware is BVI, address is 0010.7ba9.c783 (bia 0000.0000.0000)
    MTU 1500 bytes, BW 10000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1540 packets input, 302775 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     545 packets output, 35694 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Verifying RADIUS VC Logging on the NRP

To verify RADIUS VC logging on the RADIUS server, examine a RADIUS accounting packet. If RADIUS VC logging is enabled on the Cisco IOS XE software, the RADIUS accounting packet will appear similar to the following example:

```
Wed Jun 16 13:57:31 1999
NAS-IP-Address = 192.168.100.192
```

```
NAS-Port = 268566560
NAS-Port-Type = Virtual
User-Name = "cisco"
Acct-Status-Type = Start
Service-Type = Framed
Acct-Session-Id = "1/0/0/2.32_00000009"
Framed-Protocol = PPP
Framed-IP-Address = 172.16.7.254
Acct-Delay-Time = 0
```

The NAS-Port field shows that RADIUS VC logging is enabled. If this line does not appear in the display, then RADIUS VC logging is not enabled on the Cisco IOS XE software.

The Acct-Session-Id field should also identify the incoming NSP interface and VPI/VCI information, in this format:

```
Acct-Session-Id = "slot/subslot/port/VPI.VCI_acct-session-id"
```

Configuration Examples for RADIUS VC Logging

Example Configuring the NME Interface IP Address on the NSP

The following example shows how to configure a static IP and subnetwork address for the Bridge-Group Virtual Interface:

```
Router> enable
Router# configure terminal
Router(config)# interface BVI1
ip address 209.165.200.225 255.255.255.224
Router(config)# exit
```

Example Configuring the NME IP address

The following example shows how to configure the GigabitEthernet interface:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 209.165.200.225 255.255.255.224
Router(config)# exit
```

Example Configuring RADIUS VC Logging on the NRP

The following example shows how to configure the RADIUS VC logging on the NRP:

```
Router> enable
Router# configure terminal
Router(config)# radius-server attribute nas-port format d
Router(config)# exit
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Security Commands List, All Releases*

MIBs

MIB	MIBs Link
None	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

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/cisco/web/support/index.html

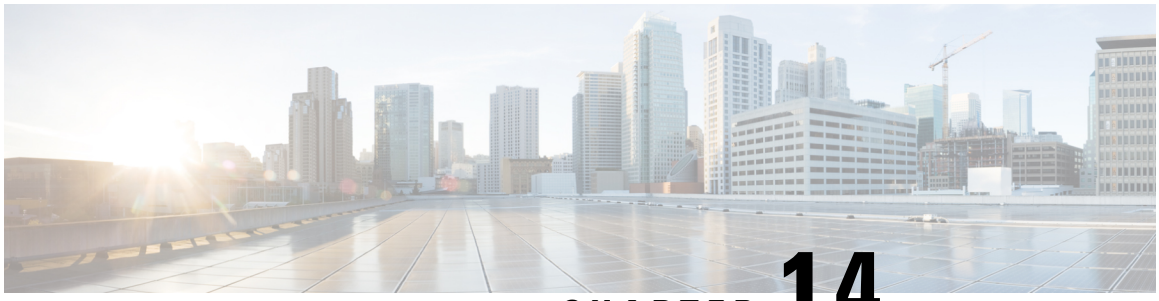
Feature Information for RADIUS VC Logging

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 16: Feature Information for Zone-Based Policy Firewall

Feature Name	Releases	Feature Configuration Information
RADIUS VC Logging	Cisco IOS XE Release 3.1S	RADIUS Virtual Circuit (VC) Logging allows the Cisco IOS XE software to accurately record the virtual path interface (VPI) and virtual circuit interface (VCI) of an incoming subscriber session.



CHAPTER 14

RADIUS Centralized Filter Management

The RADIUS Centralized Filter Management feature introduces a filter-server to simplify ACL configuration and management. This filter-server serves as a centralized RADIUS repository and administration point, which users can centrally manage and configure access control list (ACL) filters.

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 Centralized Filter Management

- You may need to add a dictionary file to your server if it does not support the new RADIUS VSAs. For a sample dictionary and vendors file, see the section “RADIUS Dictionary and Vendors File Example” later in this document.

If you need to add a dictionary file, ensure that your RADIUS server is nonstandard and that it can send the newly introduced VSAs.

- You want to set up RADIUS network authentication so a remote user can dial in and get IP connectivity.

Restrictions for RADIUS Centralized Filter Management

Multiple method lists are not supported in this feature; only a single global filter method list can be configured.

Information About RADIUS Centralized Filter Management

Before the RADIUS Centralized Filter Management feature, wholesale providers (who provide premium charges for customer services such as access control lists [ACLs]) were unable to prevent customers from applying exhaustive ACLs, which could impact router performance and other customers. This feature introduces a centralized administration point--a filter server--for ACL management. The filter server acts as a centralized RADIUS repository for ACL configuration.

Whether or not the RADIUS server that is used as the filter server is the same server that is used for access authentication, the network access server (NAS) will initiate a second access request to the filter server. If configured, the NAS will use the filter-ID name as the authentication username and the filter server password for the second access request. The RADIUS server will attempt to authenticate the filter-ID name, returning any required filtering configuration in the access-accept response.

Because downloading ACLs is time consuming, a local cache is maintained on the NAS. If an ACL name exists on the local cache, that configuration will be used without consulting the filter server.

Note An appropriately configured cache should minimize delays; however, the first dialin user to require a filter will always experience a longer delay because the ACL configuration is retrieved for the first time.

Cache Management

A global filter cache is maintained on the NAS of recently downloaded ACLs; thus, users no longer have to repeatedly request the same ACL configuration information from a potentially overloaded RADIUS server. Users are required to flush the cache when the following criteria have been met:

- After an entry becomes associated with a newly active call, the idle timer that is associated with that entry will be reset, if configured to do so.
- After the idle-time stamp of an entry expires, the entry will be removed.
- After the global cache of entries reaches a specified maximum number, the entry whose idle-timer is closest to the idle time limit will be removed.

A single timer is responsible for managing all cache entries. The timer is started after the first cache entry is created, and it runs periodically until reboot. The period of the timer will correspond to the minimum granularity offered when configuring cache idle timers, which is one expiration per minute. A single timer prevents users from having to manage individual timers per cache entry.

Note The single timer introduces a lack of precision in timer expiration. There is an average error of approximately 50 percent of the timer granularity. Although decreasing the timer granularity will decrease the average error, the decreased timer granularity will negatively impact performance. Because precise timing is not required for cache management, the error delay should be acceptable.

New Vendor-Specific Attribute Support

This feature introduces support for three new vendor-specific attributes (VSAs), which can be divided into the following two categories:

- User profile extensions
  - Filter-Required (50)--Specifies whether the call should be permitted if the specified filter is not found. If present, this attribute will be applied after any authentication, authorization, and accounting (AAA) filter method-list.
- Pseudo-user profile extensions
  - Cache-Refresh (56)--Specifies whether cache entries should be refreshed each time an entry is referenced by a new session. This attribute corresponds to the **cache refresh** command.
  - Cache-Time (57)--Specifies the idle time out, in minutes, for cache entries. This attribute corresponds to the **cache clear age** command.

Note All RADIUS attributes will override any command-line interface (CLI) configurations.

How to Configure Centralized Filter Management for RADIUS

Configuring the RADIUS ACL Filter Server

To enable the RADIUS ACL filter server, use the following command in global configuration mode:

Command	Purpose
`Router(config)# aaa authorization cache filterserver default methodlist[methodlist2...]`	Enables AAA authorization caches and the downloading of an ACL configuration from a RADIUS filter server. • **default** --The default authorization list. • *methodlist* [*methodlist2...*]--One of the keywords listed on the **password** command page.

Configuring the Filter Cache

Follow the steps in this section to configure the AAA filter cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa cache filter**
4. Router(config-aaa-filter)# **password 0 7**} *password*
5. Router(config-aaa-filter)# **cache disable**
6. Router(config-aaa-filter)# **cache clear age** *minutes*
7. Router(config-aaa-filter)# **cache refresh**
8. Router(config-aaa-filter)# **cache max** *number*

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	Router(config)# **aaa cache filter**	Enables filter cache configuration and enters AAA filter configuration mode.
Step 4	Router(config-aaa-filter)# **password 0 7**} *password*	(Optional) Specifies the optional password that is to be used for filter server authentication requests. **0** --Specifies that an unencrypted password will follow. **7** --Specifies that a hidden password will follow. *password* --The unencrypted (clear text) password. **Note** If a password is not specified, the default password ("cisco") is enabled.
Step 5	Router(config-aaa-filter)# **cache disable**	(Optional) Disables the cache.
Step 6	Router(config-aaa-filter)# **cache clear age** *minutes*	(Optional) Specifies, in minutes, when cache entries expire and the cache is cleared. *minutes* --Any value between 0 to 4294967295. **Note** If a time is not specified, the default (1400 minutes [1 day]) is enabled.
Step 7	Router(config-aaa-filter)# **cache refresh**	(Optional) Refreshes a cache entry when a new session begins. This command is enabled by default. To disable this functionality, use the **no cache refresh**command.

	Command or Action	Purpose
Step 8	Router(config-aaa-filter)# **cache max** *number*	(Optional) Limits the absolute number of entries the cache can maintain for a particular server. *number* --The maximum number of entries the cache can contain. Any value between 0 to 4294967295. **Note** If a number is not specified, the default (100 entries) is enabled.

Verifying the Filter Cache

To display the cache status, use the **show aaa cache filterserver** EXEC command. The following is sample output for the **show aaa cache filterserver** command:

```
Router# show aaa cache filterserver
Filter     Server          Age Expires Refresh Access-Control-Lists
-------------------------------------------------------------------------------
aol        10.2.3.4          0    1440     100 ip in icmp drop
                                               ip out icmp drop
                                               ip out forward tcp dstip 1.2.3...
msn        10.3.3.4        N/A   Never       2 ip in tcp drop
msn2       10.4.3.4        N/A   Never       2 ip in tcp drop
vone       10.5.3.4        N/A   Never       0 ip in tcp drop
```

Note The **show aaa cache filterserver** command shows how many times a particular filter has been referenced or refreshed. This function may be used in administration to determine which filters are actually being used.

Troubleshooting Tips

To help troubleshoot your filter cache configurations, use the privileged EXEC **debug aaa cache filterserver** command. To view sample output for the **debug aaa cache filterserver** command, refer to the section "Debug Output Example" later in this document.

Monitoring and Maintaining the Filter Cache

To monitor and maintain filter caches, use at least one of the following EXEC commands:

Command	Purpose
Router# **clear aaa cache filterserver acl** [*filter-name*]	Clears the cache status for a particular filter or all filters.
Router# **show aaa cache filterserver**	Displays the cache status.

Configuration Examples for RADIUS Centralized Filter Management

NAS Configuration Example

The following example shows how to configure the NAS for cache filtering. In this example, the server group "mygroup" in contacted first. If there is no response, the default RADIUS server will then be contacted. If there still is no response, the local filters care contacted. Finally, the call is accepted if the filter cannot be resolved.

```
aaa authorization cache filterserver group mygroup group radius local none
!
aaa group server radius mygroup
 server 10.2.3.4
 server 10.2.3.5
!
radius-server host 10.1.3.4
!
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
!
```

RADIUS Server Configuration Example

The following example is a sample RADIUS configuration that is for a remote user "user1" dialing into the NAS:

```
myfilter Password = "cisco"
Service-Type = Outbound,
Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32 icmp",
Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32 tcp dstport =
 telnet",
Ascend:Ascend-Cache-Refresh = Refresh-No,
Ascend:Ascend-Cache-Time = 15
user1 Password = "cisco"
Service-Type = Framed,
Filter-Id = "myfilter",
Ascend:Ascend-Filter-Required = Filter-Required-Yes,
```

RADIUS Dictionary and Vendors File Example

The following example is a sample RADIUS dictionary file for the new VSAs. In this example, the dictionary file is for a Merit server.

```
dictionary file:
Ascend.attr Ascend-Filter-Required 50 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Refresh   56 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Time      57 integer (*, 0, NOENCAPS)
Ascend.value Ascend-Cache-Refresh Refresh-No  0
```

```
Ascend.value Ascend-Cache-Refresh Refresh-Yes 1
Ascend.value Ascend-Filter-Required  Filter-Required-No  0
Ascend.value Ascend-Filter-Required  Filter-Required-Yes 1
vendors file:
50     50
56     56
57     57
```

Debug Output Example

The following is sample output from the **debug aaa cache filterserver** command:

```
Router# debug aaa cache filterserver

AAA/FLTSV: need "myfilter" (fetch), call 0x612DAC64
AAA/FLTSV: send req, call 0x612DAC50
AAA/FLTSV: method SERVER_GROUP myradius
AAA/FLTSV: recv reply, call 0x612DAC50 (PASS)
AAA/FLTSV: create cache
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: skip attr "filter-cache-refresh"
AAA/FLTSV: skip attr "filter-cache-time"
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" refresh? no
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" cachetime 15
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: PASS call 0x612DAC64
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (1 entry)
AAA/CACHE: destroy "AAA filtserv cache" entry "myfilter"
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
```

Additional References

The following sections provide references related to RADIUS Centralized Filter Management.

Related Documents

Related Topic	Document Title
Configuring Authorization	“ Configuring Authorization ” feature module.
Configuring RADIUS	“ Configuring RADIUS ” feature module
Authorization Commands	*Cisco IOS Security Command Reference*

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
None	--

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

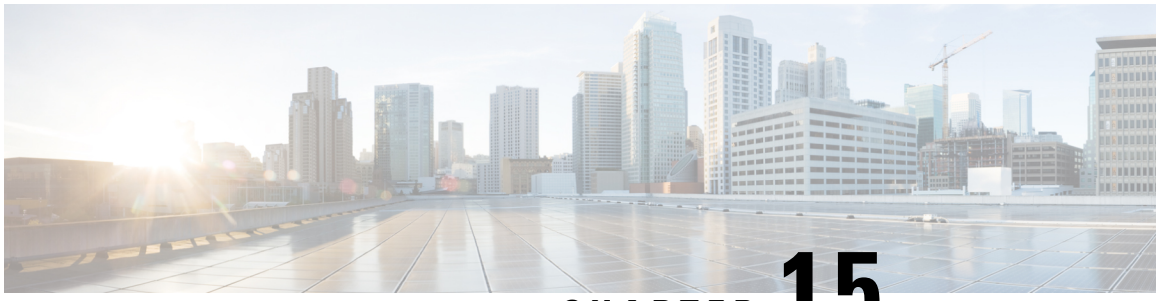
Feature Information for RADIUS Centralized Filter Management

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 17: Feature Information for RADIUS Centralized Filter Management

Feature Name	Releases	Feature Information
RADIUS Centralized Filter Management	Cisco IOS XE Release 3.9S	The RADIUS Centralized Filter Management feature introduces a filter-server to simplify ACL configuration and management. This filter-server serves as a centralized RADIUS repository and administration point, which users can centrally manage and configure access control list (ACL) filters. The following commands were introduced or modified by this feature: **aaa authorization cache filterserver**, **aaa cache filter, cache clear age, cache disable, cache refresh**,**clear aaa cache filterserver acl**, **debug aaa cache filterserver**, **password**, **show aaa cache filterserver.**



CHAPTER 15

RADIUS EAP Support

The RADIUS EAP Support feature makes it possible for users to apply the client authentication methods within PPP (including proprietary authentication), which may not be supported by the network access server (NAS); to be accomplished through the Extensible Authentication Protocol (EAP). Before this feature was introduced, support for various authentication methods for PPP connections required custom vendor-specific configuration and changes to the client and NAS. RADIUS EAP support allows authentication schemes, such as token cards and public key, to strengthen end-user and device authenticated access to their networks.

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 EAP Support

Before enabling EAP RADIUS on the client, you must perform the following tasks:

- Configure an interface type and enter interface configuration mode by using the **interface** command.
- Configure the interface for PPP encapsulation by using the **encapsulation** command.

For more information on completing these tasks, refer to the " Configuring Asynchronous SLIP and PPP " module.

Restrictions for RADIUS EAP Support

When EAP is running in proxy mode, there may be a significant increase in the authentication time because every packet from the peer must be sent to the RADIUS server and every EAP packet from the RADIUS server must be sent back to the client. Although this extra processing causes delays, you can increase the default authentication timeout value by using the **ppp timeout authentication** command.

Information About RADIUS EAP Support

EAP is an authentication protocol for PPP that supports multiple authentication mechanisms that are negotiated during the authentication phase (instead of the link control protocol [LCP] phase). EAP allows a third-party authentication server to interact with a PPP implementation through a generic interface.

How EAP Works

By default, EAP runs in proxy mode. This means that EAP allows the entire authentication process to be negotiated by the NAS to a back-end server that may reside on or be accessed through a RADIUS server. After EAP is negotiated between the client and the NAS during LCP exchange, all further authentication messages are transparently transmitted between the client and the back-end server. The NAS is no longer directly involved in the authentication process; that is, the NAS works as a proxy, sending EAP messages between the remote peers.

Note EAP can also run in a local mode; the session is authenticated using the Message Digest 5 (MD5) algorithm and obeys the same authentication rules as Challenge Handshake Authentication Protocol (CHAP). To disable proxy mode and authenticate locally, you must use the **ppp eap local** command.

Newly Supported Attributes

The RADIUS EAP Support feature introduces support for the following RADIUS attributes:

Number	IETF Attribute	Description
79	EAP-Message	Encapsulates one fragment of an EAP message, which includes the PPP type, request-id, length, and EAP-type fields.
80	Message Authenticator	Ensures source integrity of the message; all messages that are received with invalid checksums are silently discarded by either end. This attribute contains an HMAC-MD5 checksum of the entire RADIUS request or response message and uses the RADIUS server secret as the key.

How to Configure RADIUS EAP Support

Configuring EAP

Perform this task to configure EAP on an interface configured for PPP encapsulation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ppp authentication eap**
4. **ppp eap identity** *string*
5. **ppp eap password** [*number*] *string*
6. **ppp eap local**
7. **ppp eap wait**
8. **ppp eap refuse** [**callin**]

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	**ppp authentication eap** **Example:** `Router(config-if)# ppp authentication eap`	Enables EAP as the authentication protocol.
Step 4	**ppp eap identity** *string* **Example:** `Router(config-if)# ppp eap identity user`	(Optional) Specifies the EAP identity when requested by the peer.
Step 5	**ppp eap password** [*number*] *string* **Example:** `Router(config-if)# ppp eap password 7 141B1309`	(Optional) Sets the EAP password for peer authentication. This command should only be configured on the client.

	Command or Action	Purpose
Step 6	**ppp eap local** **Example:** `Router(config-if)# ppp eap local`	(Optional) Authenticates locally instead of using a RADIUS back-end server, which is the default. **Note** This command should only be configured on the NAS.
Step 7	**ppp eap wait** **Example:** `Router(config-if)# ppp eap wait`	(Optional) Waits for the caller to authenticate itself first. By default, the client always authenticates itself before the caller does. **Note** This command should only be configured on the NAS.
Step 8	**ppp eap refuse** [**callin**] **Example:** `Router(config-if)# ppp eap refuse`	(Optional) Refuses to authenticate using EAP. If the **callin** keyword is enabled, only incoming calls are not authenticated. **Note** This command should only be configured on the NAS.

Verifying EAP

To verify EAP configurations on your client or NAS, use at least one of the following commands in privileged EXEC configuration mode:

Command	Purpose
`Router# show users`	Displays information about the active lines on the router.
`Router# show interfaces`	Displays statistics for all interfaces configured on the router or access server.
`Router# show running-config`	Ensures that your configurations appear as part of the running configuration.

Configuration Examples

EAP Local Configuration on Client Example

The following example is a sample configuration for a client configured for EAP:

```
interface Ethernet0/0
 ip address 10.1.1.202 255.255.255.0
 no ip mroute-cache
 half-duplex
!
interface BRI0/0
```

```
 ip address 192.168.101.100 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 dialer map ip 192.168.101.101 56167
 dialer-group 1
 isdn switch-type basic-5ess
 ppp eap identity user
 ppp eap password 7 141B1309
!
!
ip default-gateway 10.1.1.1
ip classless
ip route 192.168.101.101 255.255.255.255 BRI0/0
no ip http server
!
dialer-list 1 protocol ip permit
```

EAP Proxy Configuration for NAS Example

The following example is a sample configuration for a NAS configured to use EAP proxy:

```
aaa authentication login default group radius
aaa authentication login NOAUTH none
aaa authentication ppp default if-needed group radius
aaa session-id common
enable secret 5 $1$x5D0$cfTL/D8Be.34PgTbdGdgl/
!
username dtw5 password 0 lab
username user password 0 lab
ip subnet-zero
no ip domain-lookup
ip host lab24-boot 172.19.192.254
ip host lb 172.19.192.254
!
isdn switch-type primary-5ess
!
controller T1 3
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
interface Ethernet0
 ip address 10.1.1.108 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface Serial3:23
 ip address 192.168.101.101 255.255.255.0
 encapsulation ppp
 dialer map ip 192.168.101.100 60213
 dialer-group 1
 isdn switch-type primary-5ess
 isdn T321 0
 ppp authentication eap
 ppp eap password 7 011F0706
!
!
ip default-gateway 10.0.190.1
ip classless
ip route 192.168.101.0 255.255.255.0 Serial3:23
no ip http server
!
```

```
dialer-list 1 protocol ip permit
!
radius-server host 10.1.1.201 auth-port 1645 acct-port 1646 key lab
radius-server retransmit 3
call rsvp-sync
!
mgcp profile default
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 login authentication NOAUTH
line 1 48
line aux 0
ine vty 0 4
lpassword lab
```

Additional References

The following sections provide references related to RADIUS EAP Support feature.

Related Documents

Related Topic	Document Title
Configuring PPP Authentication Using AAA	“ Configuring Authentication ” module.
Configuring RADIUS	“ Configuring RADIUS ” module.
PPP Configuration	“ Configuring Asynchronous SLIP and PPP ” module.
Dial Technologies commands	*Cisco IOS Dial Technologies Command Reference*
Security Commands	*Cisco IOS Security Command Reference*

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 2284	*PPP Extensible Authentication Protocol (EAP)*
RFC 1938	*A One-Time Password System*
RFC 2869	*RADIUS Extensions*

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 EAP Support

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 18: Feature Information for RADIUS EAP Support

Feature Name	Releases	Feature Information
RADIUS EAP Support	Cisco IOS XE Release 3.9S	The RADIUS EAP Support feature makes it possible for users to apply the client authentication methods within PPP (including proprietary authentication), which may not be supported by the network access server (NAS); to be accomplished through the Extensible Authentication Protocol (EAP). Before this feature was introduced, support for various authentication methods for PPP connections required custom vendor-specific configuration and changes to the client and NAS. RADIUS EAP support allows authentication schemes, such as token cards and public key, to strengthen end-user and device authenticated access to their networks. The following commands were introduced or modified: **ppp authentication**, **ppp eap identity, ppp eap local**, **ppp eap password**, **ppp eap refuse**, **ppp eap wait**.

Glossary

attribute --A RADIUS Internet Engineering Task Force (IETF) attribute is one of the original set of 255 standard attributes that are used to communicate authentication, authorization, and accounting (AAA) information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers that exchange AAA information through IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

CHAP --Challenge Handshake Authentication Protocol. Security feature that is supported on lines using PPP encapsulation and prevents unauthorized access. CHAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines whether that user is allowed access.

EAP --Extensible Authentication Protocol. A PPP authentication protocol that supports multiple authentication mechanisms that are negotiated during the authentication phase (instead of the Link Control Protocol [LCP] phase). EAP allows a third-party authentication server to interact with the PPP implementation through a generic interface.

LCP --link control protocol. Protocol that establishes, configures, and tests data-link connections for use by PPP.

MD5 (HMAC variant) --Message Digest 5. A hash algorithm used to authenticate packet data. HMAC is a key hashing for message authentication.

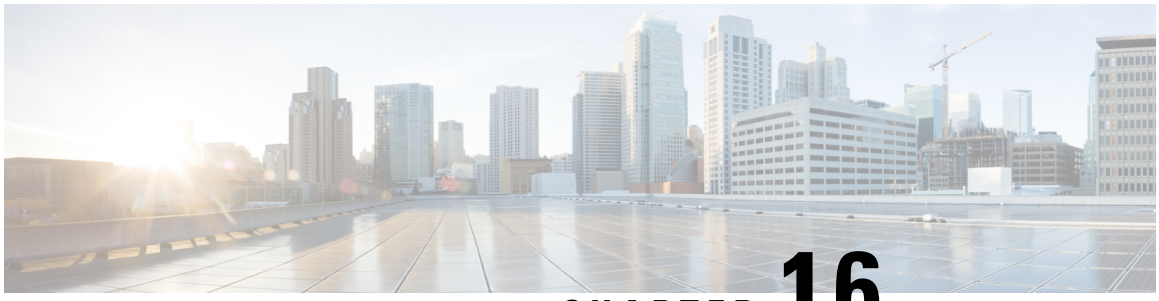
NAS --network access server. A device providing local network access to users across a remote access network such as the public switched telephone network (PSTN).

PAP --Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines.

PPP --Point-to-Point Protocol. A protocol that encapsulates network layer protocol information over point-to-point links. PPP is defined in RFC 1661.

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



CHAPTER 16

RADIUS Interim Update at Call Connect

The RADIUS Interim Update at Call Connect feature generates an additional accounting record that provides the call connection timestamp for the billing server.

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.

Information About RADIUS Interim Update at Call Connect

When the RADIUS Interim Update at Call Connect feature enabled, Cisco IOS software generates and sends an additional updated interim accounting record to the accounting server when a call leg is connected. A call leg is a distinct segment of a call connection in a voice over IP (VOIP) network that is a logical connection between the router and either a telephony endpoint over a bearer channel, or another endpoint using a session protocol. All attributes (for example, h323-connect-time and backward-call-indicators) available at the time of call connection are sent through this interim updated accounting record.

How to Enable RADIUS Interim Update at Call Connect Feature

Perform the following task to enable the Cisco IOS to generate and send an additional updated interim accounting record to the accounting server when a call leg is connected.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **gw-accounting aaa**
5. **aaa accounting update newinfo**

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 new-model** **Example:** `Router(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA).
Step 4	**gw-accounting aaa** **Example:** `Router(config)# gw-accounting aaa`	Enables an accounting through the AAA system and sends call detail records (CDRs) to the RADIUS server in the form of vendor-specific attributes (VSAs).
Step 5	**aaa accounting update newinfo** **Example:** `Router(config)# aaa accounting update newinfo`	Enables periodic interim accounting records to be sent to the accounting server whenever there is new accounting information to report relating to the user in question.

Additional References

The following sections provide references related to the RADIUS Interim Update at Call Connect feature.

Related Documents

Related Topic	Document Title
Authentication, Authorization, and Accounting (AAA)	Configuring Authentication , Configuring Authorization , and Configuring Accounting modules.
RADIUS Vendor-Specific Attributes	RADIUS Vendor-Proprietary Attributes module.

Related Topic	Document Title
Configuring Dynamic Prompts, Customizing Accounting Templates, and Directing AAA Requests for Voice Gateways	*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T and *Cisco IOS VPDN Configuration Guide* , Release 12.4T.

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 2138	*Remote Authentication Dial In User Service (RADIUS)*
RFC 2139	*RADIUS Accounting*

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

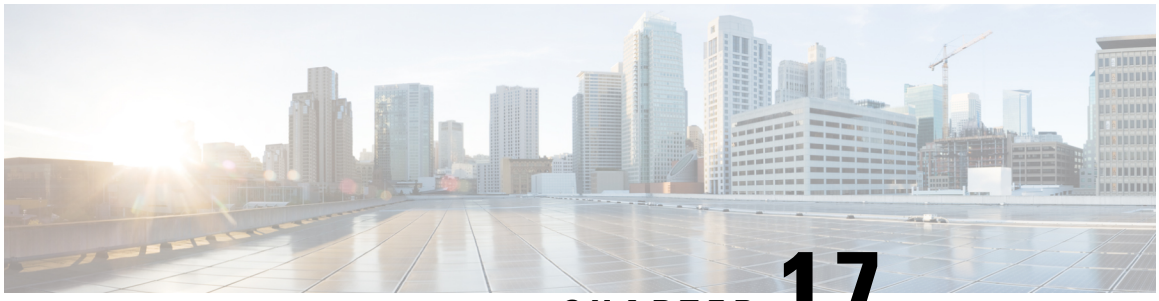
Feature Information for RADIUS Interim Update at Call Connect

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 19: Feature Information for RADIUS Interim Update at Call Connect

Feature Name	Releases	Feature Information
RADIUS Interim Update at Call Connect	Cisco IOS XE Release 3.9S	The RADIUS Interim Update at Call Connect feature generates an additional accounting record that provides the call connection timestamp for the billing server. The following commands were introduced or modified: **gw-accounting aaa** and **aaa accounting update**



CHAPTER 17

RADIUS Tunnel Preference for Load Balancing and Fail-Over

The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature provides industry-standard load balancing and fail-over functionality for an Layer 2 Tunnel Protocol network server (LNS), rather than requiring the use of a Cisco proprietary Vendor Specific Attribute (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 network access servers (NASs) manufactured by different vendors.

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

Configuring VPDNs and HGW groups is beyond the scope of this document. See the Related Document section for more information.

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.

Information About RADIUS Tunnel Preference for Load Balancing and Fail-Over

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 LNS was provided by the Cisco proprietary VSA. In a multivendor network environment, using VSA on a RADIUS server can cause interoperability issues among 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.

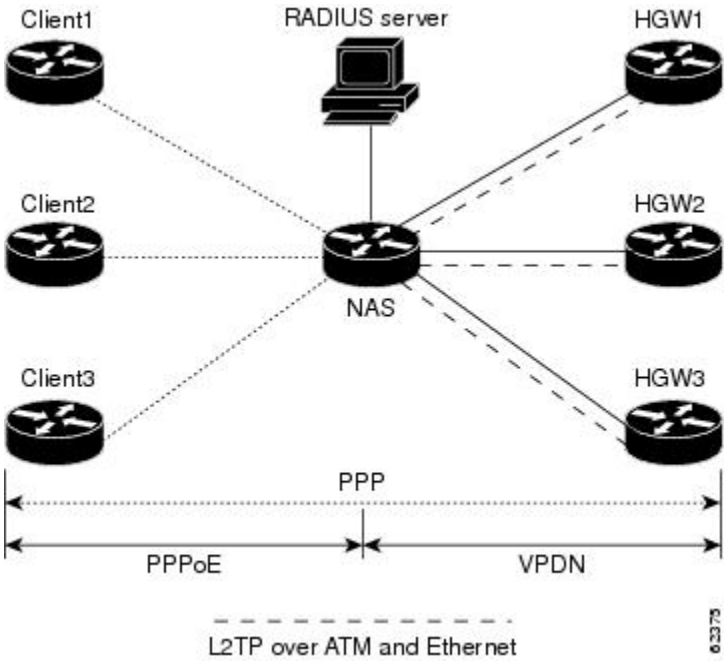
Until Cisco IOS Release 12.2(4)T, a specially formatted string would be transported within a Cisco VSA “vpdn:ip-addresses” string to a NAS for the purpose of HGW load balancing and fail-over. For example, 10.0.0.1 10.0.0.2 10.0.0.3/2.0.0.1 2.0.0.2 would be interpreted as IP addresses 10.0.0.1, 10.0.0.2, 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 RADIUS Tunnel Preference for Load Balancing and Fail-Over, on page 156 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 the figure below.

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



In the configuration shown in the figure above, 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.

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

How RADIUS Tunnel Preference for Load Balancing and Fail-Over is Configured

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 for RADIUS Tunnel Preference for Load Balancing and Fail-Over

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"
```

See Information About RADIUS Tunnel Preference for Load Balancing and Fail-Over, on page 154 for more information on how fail-over addresses are selected in these profiles.

Additional References

The following sections provide references related to RADIUS Tunnel Preference for Load Balancing and Fail-Over feature.

Related Documents

Related Topic	Document Title
RADIUS	" Configuring RADIUS " module.
RADIUS Attributes	" RADIUS Attributes Overview and RADIUS IETF Attributes " module.
Virtual private dialup networks (VPDN) roadmap	*Cisco IOS VPDN Configuration Guide* , Release 15.0.
Dial Technologies	*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T
Broadband Access: PPP and Routed Bridge Encapsulation	*Cisco IOS Broadband Access Aggregation and DSL Configuration Guide* , Release 12.4T

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

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

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 20: Feature Information for RADIUS Tunnel Preference for Load Balancing and Fail-Over

Feature Name	Releases	Feature Information
RADIUS Tunnel Preference for Load Balancing and Fail-Over	Cisco IOS XE Release 3.9S	The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature provides industry-standard load balancing and fail-over functionality for an Layer 2 Tunnel Protocol network server (LNS), rather than requiring the use of a Cisco proprietary Vendor Specific Attribute (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 network access servers (NASs) manufactured by different vendors.

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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.