# RADIUS Configuration Guide Cisco IOS XE Release 2

**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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2012 Cisco Systems, Inc. All rights reserved.

# CONTENTS

# Configuring RADIUS

This chapter describes the Remote Authentication Dial-In User Service (RADIUS) security system, defines its operation, and identifies appropriate and inappropriate network environments for using RADIUS technology.



## Finding Feature Information

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

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

## Information About RADIUS

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

RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system currently available on the market.

Cisco supports RADIUS under its 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 router with RADIUS to the network. This might be the first step when you make a transition to a Terminal Access Controller Access Control System Plus (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 Point-to-Point Protocol (PPP). For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using 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, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.
- Networks that wish to 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 the following 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 PAD connections
- Router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one router to a non-Cisco router if the non-Cisco router requires RADIUS authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

- RADIUS Operation, page 2

# 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 for and enters a 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. REJECT--The user is not authenticated and is prompted to reenter the username and password, or access is denied.

c CHALLENGE--A challenge is issued by the RADIUS server. The challenge collects additional data from the user.

d CHANGE PASSWORD--A request is issued by the RADIUS server, asking the user to select a new password.

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 Telnet, rlogin, or local-area transport (LAT) connections, and PPP, Serial Line Internet 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. For a list of supported RADIUS attributes, refer to the appendix "RADIUS Attributes."

- Vendor-Proprietary RADIUS Attributes, page 3
- RADIUS Tunnel Attributes, page 3

## Vendor-Proprietary RADIUS Attributes

An Internet Engineering Task Force (IETF) draft 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 IOS XE software supports a subset of vendor-proprietary RADIUS attributes. For a list of supported vendor-proprietary RADIUS attributes, refer to the appendix "RADIUS Attributes."

## RADIUS Tunnel Attributes

RADIUS is a security server authentication, authorization, and accounting (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 Internet Engineering Task Force (IETF)-standard AV pairs used to send AAA information. Two draft 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 virtual private networks (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 routers and access servers now support new RADIUS IETF-standard VPDN tunnel attributes. These new RADIUS IETF-standard attributes are listed in the "RADIUS Attributes" appendix.

For more information about L2TP, VPN, or VPDN, refer to the *Cisco IOS XE VPDN Configuration Guide* , Release 2.

# How to Configure RADIUS

To configure RADIUS on your Cisco router or access server, you must perform the following tasks:

- Use the **aaa new-model** global configuration command to enable AAA. AAA must be configured if you plan to use RADIUS. For more information about using the **aaa new-model** command, refer to the "AAA Overview" chapter.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication. For more information about using the **aaa authentication** command, refer to the "Configuring Authentication" chapter.
- Use **line** and **interface** commands to enable the defined method lists to be used. For more information, refer to the "Configuring Authentication" chapter.

The following configuration tasks are optional:

- You may use the **aaa group server**command to group selected RADIUS hosts for specific services. For more information about using the **aaa group server** command, refer to the Configuring AAA Server Groups section in this chapter.
- You may use the **aaa dnis map**command to select RADIUS server groups based on DNIS number. To use this command, you must define RADIUS server groups using the **aaa group server** command. For more information about using the **aaa dnis map**command, refer to the section Configuring AAA Server Group Selection Based on DNIS in this chapter.
- You may use the **aaa authorization** global command to authorize specific user functions. For more information about using the **aaa authorization** command, refer to the chapter "Configuring Authorization."
- You may use the **aaa accounting** command to enable accounting for RADIUS connections. For more information about using the **aaa accounting** command, refer to the chapter "Configuring Accounting."
- You may use the **dialer aaa**interface configuration command to create remote site profiles that contain outgoing call attributes on the AAA server. For more information about using the **dialer aaa** command, refer to the section "Configuring Suffix and Password in PADIUS Access Requests " in this chapter.

For RADIUS configuration examples using the commands in this chapter, refer to the section RADIUS Configuration Examples at the end of this chapter.

# Configuring Router 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 router to RADIUS server communication can have several components:

- Host name 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 host name or IP address, host name 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. In other words, 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 fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

A RADIUS server and a Cisco router 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 router.

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 router, 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 router, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands.

To configure per-server RADIUS server communication, use the following command in global configuration mode:

| Command | Purpose |
|---|---|
| `Router(config)#` **radius-server host** {*hostname* \| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* \| *ip address*}] | Specifies the IP address or host name of the remote RADIUS server host and assign authentication and accounting destination port numbers. Use the **auth-port** *port-number* option to configure a specific UDP port on this RADIUS server to be used solely for authentication. Use the **acct-port** *port-number* option to configure a specific UDP port on this RADIUS server to be used solely for accounting. Use the **alias** keyword to configure up to eight multiple IP addresses for use when referring to RADIUS servers.<br><br>To configure the network access server to recognize more than one host entry associated with a single IP address, simply repeat this command as many times as necessary, making sure that each UDP port number is different. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.<br><br>If no timeout is set, the global value is used; otherwise, enter a value in the range 1 to 1000. If no retransmit value is set, the global value is used; otherwise enter a value in the range 1 to 1000. If no key string is specified, the global value is used.<br><br>**Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host**command syntax because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key. |

- Configuring Global Communications Between the Router and a RADIUS Server, page 6

## Configuring Global Communications Between the Router and a RADIUS Server

To configure global communication settings between the router and a RADIUS server, use the following **radius-server** commands in global configuration mode:

### SUMMARY STEPS

1. Router(config)# **radius-server key** {**0** *string*|**7** *string*| *string*}
2. Router(config)# **radius-server retransmit** *retries*
3. Router(config)# **radius-server timeout** *seconds*
4. Router(config)# **radius-server deadtime** *minutes*

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **radius-server key** {**0** *string*\|**7** *string*\| *string*} | Specifies the shared secret text string used between the router and a RADIUS server. Use the **0** line option to configure an unencrypted shared secret. Use the **7** line option to configure an encrypted shared secret. |
| **Step 2** | Router(config)# **radius-server retransmit** *retries* | Specifies how many times the router transmits each RADIUS request to the server before giving up (the default is 3). |
| **Step 3** | Router(config)# **radius-server timeout** *seconds* | Specifies for how many seconds a router waits for a reply to a RADIUS request before retransmitting the request. |
| **Step 4** | Router(config)# **radius-server deadtime** *minutes* | Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication. |

# Configuring Router to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft 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 of the following 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, IPX, VPDN, VOIP, SHELL, RSVP, SIP, AIRNET, OUTBOUND. "Attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes. This allows 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 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. For more information about vendor-IDs and VSAs, refer to RFC 2138, Remote Authentication Dial-In User Service (RADIUS).

To configure the network access server to recognize and use VSAs, use the following command in global configuration mode:

| Command | Purpose |
|---|---|
| `Router(config)#` **radius-server vsa send** [**accounting** \| **authentication**] | Enables the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26. |

For a complete list of RADIUS attributes or more information about vendor-specific attribute 26, refer to the appendix "RADIUS Attributes."

# Configuring Router for Vendor-Proprietary RADIUS Server Communication

Although an Internet Engineering Task Force (IETF) draft 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 IOS XE software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the Cisco device. You specify the RADIUS host and secret text string by using the **radius-server** commands. 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 will not be supported unless you use the **radius-server host non-standard**command.

To specify a vendor-proprietary RADIUS server host and a shared secret text string, use the following commands in global configuration mode:

### SUMMARY STEPS

1. Router(config)# **radius-server host**
2. Router(config)# **radius-server key** {**0** *string*|**7** *string*| *string*}

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **radius-server host**<br><br>**Example:**<br><br>{*hostname* \| *ip-address*} **non-standard** | Specifies the IP address or host name of the remote RADIUS server host and identifies that it is using a vendor-proprietary implementation of RADIUS. |
| **Step 2** | Router(config)# **radius-server key** {**0** *string*\| **7** *string*\| *string*} | Specifies the shared secret text string used between the router and the vendor-proprietary RADIUS server. The router and the RADIUS server use this text string to encrypt passwords and exchange responses. |

# Configuring Router to Query RADIUS Server for Static Routes and IP Addresses

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.

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

To have the Cisco router or access server query the RADIUS server for static routes and IP pool definitions when the device first starts up, use the following command in global configuration mode:

| Command | Purpose |
|---|---|
| `Router(config)#` **radius-server configure-nas** | Tells the Cisco router or access server to query the RADIUS server for the static routes and IP pool definitions used throughout its domain. |

# Configuring Router to Expand Network Access Server Port Information

There are some situations when PPP or login authentication occurs on an interface 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.

To display expanded interface information in the NAS-Port attribute field, use the following command in global configuration mode:

| Command | Purpose |
|---|---|
| `Router(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. |

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

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation will not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI interface is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 will appear as NAS-Port = 20101.

Once again, this is because of the 16-bit field size limitation associated with RADIUS IETF NAS-Port attribute. In this case, the solution is to replace the NAS-Port attribute with a vendor-specific attribute (RADIUS IETF attribute 26). Cisco's vendor-ID is 9, and the Cisco-NAS-Port attribute is subtype 2. Vendor-specific attributes (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.

# Configuring the Router to Replace the NAS-Port Attribute

To replace the NAS-Port attribute with RADIUS IETF attribute 26 and to display extended field information, use the following commands in global configuration mode:

### SUMMARY STEPS

1. Router(config)# **radius-server vsa send**
2. Router(config)# **aaa nas port extended**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **radius-server vsa send**<br><br>**Example:**<br><br>[**accounting** \| **authentication**] | Enables the network access server to recognize and use vendor-specific attributes as defined by RADIUS IETF attribute 26. |
| **Step 2** | Router(config)# **aaa nas port extended** | Expands the size of the VSA NAS-Port field from 16 to 32 bits to display extended interface information. |

The standard NAS-Port attribute (RADIUS IETF attribute 5) will continue to be 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. When this command is configured, the standard NAS-Port attribute will no longer be sent.

For a complete list of RADIUS attributes, refer to the "RADIUS Attributes" section of the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2.

For information about configuring RADIUS port identification for PPP, see the Cisco IOS XE Wide-Area Networking Configuration Guide, Release 2.

# Configuring AAA Server Groups

Configuring the router 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 in conjunction with a global server-host list. The server group lists the IP addresses of the selected server hosts.

Server groups also can 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. In other words, 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 configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order in which they are configured.)

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:

### SUMMARY STEPS

1. Router(config)# **radius-server host**
2. Router(config-if)# **aaa group server**
3. Router(config-sg)# **server** *ip-address*

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **radius-server host**<br><br>**Example:**<br><br>{*hostname* \| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* \| *ip address*}] | Specifies and defines the IP address of the server host before configuring the AAA server-group. Refer to the section Configuring Router to RADIUS Server Communication, page 5 of this chapter for more information on the **radius-server host** command. |
| **Step 2** | Router(config-if)# **aaa group server**<br><br>**Example:**<br><br>{**radius** \| **tacacs+**} *group-name* | 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 router in server group subconfiguration mode. |
| **Step 3** | Router(config-sg)# **server** *ip-address*<br><br>**Example:**<br><br>[**auth-port** *port-number*] [**acct-port** *port-number*] | Associates a particular RADIUS server with the defined server group. Each security server is identified by its IP address and UDP port number.<br><br>Repeat this step for each RADIUS server in the AAA server group.<br><br>**Note** Each server in the group must be defined previously using the **radius-server host** command. |

# Configuring AAA Server Groups with Deadtime

After you have configured 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 no longer limited to a global configuration. A separate timer has been 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, only 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** Since one server has different timers and may have different deadtime values configured in the server groups, the same server may 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.

To configure deadtime within a server group, use the following commands beginning in global configuration mode:

### SUMMARY STEPS

1. Router(config)# **aaa group server radius** *group1*
2. Router(config-sg)# deadtime 1
3. Router(config-sg)# **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **aaa group server radius** *group1* | Defines a RADIUS type server group. |
| **Step 2** | Router(config-sg)# deadtime 1 | Configures and defines deadtime value in minutes.<br>**Note** Local server group deadtime will override the global configuration. If omitted from the local server group configuration, the value will be inherited from the master list. |
| **Step 3** | Router(config-sg)# **exit** | Exits server group configuration mode. |

# Configuring AAA DNIS Authentication

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 authenticated by AAA, the call is accepted.

To configure DNIS authentication, perform the following tasks in global configuration mode:

### SUMMARY STEPS

1. Router# **config term**
2. Router (config)# **aaa preauth**
3. Router (config-preauth)# **group** {**radius** | **tacacs+** | *server-group*}
4. Router (config-preauth)# **dnis** [**password** *string*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router# **config term** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | Router (config)# **aaa preauth** | Enters AAA preauthentication mode. |
| **Step 3** | Router (config-preauth)# **group** {**radius** \| **tacacs+** \| *server-group*} | (Optional) Selects the security server to use for AAA preauthentication requests. The default is RADIUS. |
| **Step 4** | Router (config-preauth)# **dnis** [**password** *string*] | Enables preauthentication using DNIS and optionally specifies a password to use in Access-Request packets. |

# Configuring AAA Server Group Selection Based on DNIS

Cisco IOS XE software 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.

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 routers 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 IOS XE 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/determine which server group provides AAA services, then 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.

**Note** Prior to configuring AAA Server Group Selection Based on DNIS, you must configure the list of RADIUS server hosts and configure the AAA server groups. See the sections Configuring Router to RADIUS Server Communication, page 5 and Configuring AAA Server Groups, page 10 of this chapter.

To configure the router 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 DNIS number, use the following commands in global configuration mode:

### SUMMARY STEPS

1. Router(config)# **aaa dnis map enable**
2. Router(config)# **aaa dnis map** *dnis-number* **authentication ppp group** server-*group-name*
3. Router(config)# **aaa dnis map** dnis-number
4. Router(config)# **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **aaa dnis map enable** | Enables DNIS mapping. |
| **Step 2** | Router(config)# **aaa dnis map** *dnis-number* **authentication ppp group** server-*group-name* | Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authentication. |
| **Step 3** | Router(config)# **aaa dnis map** dnis-number<br><br>**Example:**<br><br>**authorization network group** `server-group-name` | Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authorization. |
| **Step 4** | Router(config)# **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name* | Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for accounting. |

# Configuring AAA Preauthentication

Configuring AAA preauthentication with channel-associated signalling (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 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 Dialed Number Identification Service (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

This 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 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, then the NAS accepts the call. If the server does not authorize the call, then 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.

This 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 may 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 CAS:

- Attribute 44 is available for CAS calls only when preauthentication or resource pooling is enabled.

**Note** Prior to configuring AAA preauthentication, you must enable the **aaa new-model** command and make sure the supporting preauthentication application is running on a RADIUS server in your network.

To configure AAA preauthentication, use the following commands beginning in global configuration mode:

### SUMMARY STEPS

1. Router(config)# **aaa preauth**
2. Router(config-preauth)# **group** *server-group*
3. Router(config-preauth)# **clid** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
4. Router(config-preauth)# **ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
5. Router(config-preauth)# **dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
6. Router(config-preauth)# **dnis bypass** {*dnis-group-name*}

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **aaa preauth** | Enters AAA preauthentication configuration mode. |
| **Step 2** | Router(config-preauth)# **group** *server-group* | Specifies the AAA RADIUS server group to use for preauthentication. |
| **Step 3** | Router(config-preauth)# **clid** [**if-avail** \| **required**] [**accept-stop**] [**password** *string*] | Preauthenticates calls on the basis of the CLID number. |
| **Step 4** | Router(config-preauth)# **ctype** [**if-avail** \| **required**] [**accept-stop**] [**password** *string*] | Preauthenticates calls on the basis of the call type. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | Router(config-preauth)# **dnis** [**if-avail** \| **required**] [**accept-stop**] [**password** *string*] | Preauthenticates calls on the basis of the DNIS number. |
| **Step 6** | Router(config-preauth)# **dnis bypass** {*dnis-group-name*} | Specifies a group of DNIS numbers that will be bypassed for preauthentication. |

# Configuring DNIS Preauthentication

To configure DNIS preauthentication, use the following commands beginning in global configuration mode:

### SUMMARY STEPS

1. Router (config)# **aaa preauth**
2. Router (config-preauth)# **group** {**radius** | **tacacs+** | *server-group*}
3. Router (config-preauth)# **dnis** [**password** *string*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router (config)# **aaa preauth** | Enters AAA preauthentication mode. |
| **Step 2** | Router (config-preauth)# **group** {**radius** \| **tacacs+** \| *server-group*} | (Optional) Selects the security server to use for AAA preauthentication requests. The default is RADIUS. |
| **Step 3** | Router (config-preauth)# **dnis** [**password** *string*] | Enables preauthentication using DNIS and optionally specifies a password to use in Access-Request packets. |

In addition to configuring preauthentication on your Cisco router, you must set up the preauthentication profiles on the RADIUS server.


- Setting Up the RADIUS Profile for DNIS or CLID Preauthentication, page 16
- Setting Up the RADIUS Profile for Call Type Preauthentication, page 17
- Setting Up the RADIUS Profile for Preauthentication Enhancements for Callback, page 17
- Setting Up the RADIUS Profile for a Remote Host Name Used for Large-Scale Dial-Out, page 18
- Setting Up the RADIUS Profile for Modem Management, page 18
- Setting Up the RADIUS Profile for Subsequent Authentication, page 18
- Setting Up the RADIUS Profile for Subsequent Authentication Type, page 19
- Setting Up the RADIUS Profile to Include the Username, page 20
- Setting Up the RADIUS Profile for Two-Way Authentication, page 20
- Setting Up the RADIUS Profile to Support Authorization, page 20


## Setting Up the RADIUS Profile for DNIS or CLID Preauthentication

To set up the RADIUS preauthentication profile, use the DNIS or 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 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.

## Setting Up the 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 following table shows the call type strings that may be used in the preauthentication profile:

| Call Type String | ISDN Bearer Capabilities |
|---|---|
| digital | Unrestricted digital, restricted digital. |
| speech | Speech, 3.1 kHz audio, 7 kHz audio.<br>**Note** This is the only call type available for CAS. |
| v.110 | Anything with V.110 user information layer. |
| v.120 | Anything with 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 check-in item if the RADIUS server supports check-in items.

## Setting Up the 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 555-1111 and the service type set to outbound. The cisco-avpair = “preauth:send-name=<string>” uses the string “user” and the cisco-avpair = “preauth:send-secret=<string>” uses the password “cisco.”

```
5551111 password = “cisco”, Service-Type = Outbound
Service-Type = Callback-Framed
Framed-Protocol = PPP,
Dialback-No = “5551212”
Class = “ISP12”
cisco-avpair
```

```
 = “preauth:send-name=user”
cisco-avpair = “preauth:send-secret=cisco”
```

## Setting Up the RADIUS Profile for a Remote Host Name Used for Large-Scale Dial-Out

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

```
5551111 password = "cisco", Service-Type = Outbound
       Service-Type = Callback-Framed
       Framed-Protocol = PPP,
       Dialback-No = "5551212"
       Class = "ISP12"
       cisco-avpair = "preauth:send-name=user"
       cisco-avpair = "preauth:send-secret=cisco"
       cisco-avpair = "preauth:remote-name=Router2"
```

## Setting Up the RADIUS Profile for Modem Management

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

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

The modem management string within the VSA may contain the following:

| 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 IOS XE 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 and newer technologies. This feature is not supported with Microcom modems.

## Setting Up the RADIUS Profile for Subsequent Authentication

If preauthentication passes, you may use vendor-proprietary RADIUS attribute 201 (Require-Auth) in the preauthentication profile to determine whether subsequent authentication is to be performed. If attribute

201, returned in the access-accept message, has a value of 0, then subsequent authentication will not be performed. If attribute 201 has a value of 1, then subsequent authentication will be performed as usual.

Attribute 201 has the following 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, then a value of 1 is assumed, and subsequent authentication is performed.

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

## Setting Up the RADIUS Profile for Subsequent Authentication Type

If you have 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 the following VSA:

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

where <*string*> can be one of the following:

| String | Description |
|---|---|
| chap | Requires username and password of CHAP for PPP authentication. |
| ms-chap | Requires username and password of MS-CHAP for PPP authentication. |
| pap | Requires username and password of 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 command.

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

## Setting Up the 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 may 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 the following 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 that has been configured (for example, if **clid** was the last preauthentication command configured, the CLID number will be 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.

## Setting Up the RADIUS Profile for Two-Way Authentication

In the case of two-way authentication, the calling networking device will need to authenticate the NAS. The Password Authentication Protocol (PAP) username and password or Challenge Handshake Authentication Protocol (CHAP) username and password need not be configured locally on the NAS. Instead, username and password can be included in the access-accept messages for preauthentication.

**Note** The **ppp authentication** command must be configured with the **radius** method.

To apply for PAP, do not configure the **ppp pap sent-name password**command on the interface. The vendor-specific attributes (VSAs) “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication.

For CHAP, “preauth:send-name” will be used not only for outbound authentication, but also for inbound authentication. For a CHAP inbound case, the NAS will use 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” will be used in the response packet.

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

```
5551111 password = "cisco", Service-Type = Outbound
Service-Type = Framed-User
cisco-avpair = "preauth:auth-required=1"
cisco-avpair = "preauth:auth-type=pap"
cisco-avpair = "preauth:send-name=andy"
cisco-avpair = "preauth:send-secret=cisco"
class = "<some class>"
```

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

## Setting Up the RADIUS Profile to Support Authorization

If only preauthentication is configured, then subsequent authentication will be bypassed. Note that because the username and password are not available, authorization will also be bypassed. However, you may

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 may 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 the following syntax:

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

where <*n*> is one of the standard RFC 2138 values for attribute 6. For a list of possible Service-Type values, refer to the appendix RADIUS Attributes.

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

# Configuring a Guard Timer

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.

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, use one of the following commands in interface configuration mode:

| Command | Purpose |
|---|---|
| `Router(config-if)#` **isdn guard-timer** *milliseconds* [**on-expiry** {**accept** \| **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. |
| `Router(control-config)#` **call guard-timer** *milliseconds* [**on-expiry** {**accept** \| **reject**}] | 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. |

# Specifying 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. For more information, refer to the chapter “Configuring Authentication.”

# Specifying 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, ARA, and Telnet. Because RADIUS authorization is facilitated through AAA, you must issue the **aaa authorization**

command, specifying RADIUS as the authorization method. For more information, refer to the chapter "Configuring Authorization."

# Specifying RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must issue the **aaa accounting** command, specifying RADIUS as the accounting method. For more information, refer to the chapter "Configuring Accounting."

# Configuring RADIUS Login-IP-Host

To enable the network access server 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 have been configured for the user >*joeuser*, and that TCP-Clear will be used for the connection:

```
joeuser       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 network access server 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 network access server supports only three hosts in access-accept packets.

# Configuring 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:

```
joeuser 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, then the user responses are echoed.

**Note** To use the Prompt attribute, your RADIUS server must be configured to support access-challenge packets.

# Configuring Suffix and Password in RADIUS Access Requests

Large-scale dial-out eliminates the need to configure dialer maps on every NAS for every destination. Instead, you can create remote site profiles that contain outgoing call attributes on the AAA server. The profile is downloaded by the NAS when packet traffic requires a call to be placed to a remote site.

You can configure the username in the access-request message to RADIUS. The default suffix of the username, "-out," is appended to the username. The format for composing the username attribute is IP address plus configured suffix.

To provide username configuration capability for large-scale dial-out, the **dialer aaa**command is implemented with the new **suffix** and **password** keywords.

### SUMMARY STEPS

1. Router(config)# **aaa new-model**
2. Router(config)# **aaa route download** *min*
3. Router(config)# **aaa authorization configuration default**
4. Router(config)# **interface dialer** *1*
5. Router(config-if)# **dialer aaa**
6. Router(config-if)# **dialer aaa suffix** *suffix* **password** *password*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **aaa new-model** | Enables the AAA access control model. |
| **Step 2** | Router(config)# **aaa route download** *min* | Enables the download static route feature and sets the amount of time between downloads. |
| **Step 3** | Router(config)# **aaa authorization configuration default** | Downloads static route configuration information from the AAA server using TACACS+ or RADIUS. |
| **Step 4** | Router(config)# **interface dialer** *1* | Defines a dialer rotary group. |
| **Step 5** | Router(config-if)# **dialer aaa** | Allows a dialer to access the AAA server for dialing information. |
| **Step 6** | Router(config-if)# **dialer aaa suffix** *suffix* **password** *password* | Allows a dialer to access the AAA server for dialing information and specifies a suffix and nondefault password for authentication. |

# Monitoring and Maintaining RADIUS

To monitor and maintain RADIUS, use the following commands in privileged EXEC mode:

| Command | Purpose |
|---|---|
| `Router#` **debug radius** | Displays information associated with RADIUS. |

| Command | Purpose |
|---|---|
| `Router#` **show radius statistics** | Displays the RADIUS statistics for accounting and authentication packets. |

# RADIUS Configuration Examples



## RADIUS Authentication and Authorization Example

The following example shows how to configure the router 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 router 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 IOS XE 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.

# RADIUS Authentication Authorization and Accounting Example

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 will be used on serial lines using PPP.
- The **ppp authentication pap dialins**command applies the “dialins” method list to the lines specified.
- 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.

# Vendor-Proprietary RADIUS Configuration Example

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

```
radius-server host alcatraz non-standard
radius-server key myRaDiUSpassWoRd
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
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 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 **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **radius-server configure-nas** command defines that the Cisco router or access server will query 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 will be used on serial lines using PPP.
- The **ppp authentication pap dialins**command applies the "dialins" method list to the lines specified.
- 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.

# RADIUS Server with Server-Specific Values Example

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
```

# Multiple RADIUS Servers with Global and Server-Specific Values Example

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 router, while specific AAA commands define the AAA services. The **radius-server retransmit** command changes the global retransmission value to 4 for all RADIUS servers. The **radius-server 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 router 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
!
! Change the global retransmission value for all RADIUS servers.
radius-server retransmit 4
!
! Configure per-server specific timeout, retransmission, and key values.
! Change the default auth-port and acct-port values.
radius-server host 172.16.1.1 auth-port 1612 acct-port 1616 timeout 3 retransmit 3 key
radkey
!
! Configure per-server specific timeout and key values. This server uses the global
! retransmission value.
radius-server host 172.29.39.46 timeout 6 key rad123
```

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

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 fail-over backup to the first one. (The RADIUS host entries will be 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 2000
```

# RADIUS Server Group Examples

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
```

# Multiple RADIUS Server Entries Using AAA Server Groups Example

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 deadtime; deadtime for group 1 is one minute, and deadtime for group 2 is two minutes.

**Note** In cases where both global commands and server commands are used, the server command will take 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
```

# AAA Server Group Selection Based on DNIS Example

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
```

# AAA Preauthentication Examples

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

```
aaa preauth
```

```
 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 will be performed first, followed by CLID preauthentication.

```
aaa preauth
 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 “hawaii”:

```
aaa preauth
 group radius
 dnis required
 dnis bypass hawaii
dialer dnis group hawaii
 number 12345
 number 12346
```

The following example shows 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 preauth
 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.

# RADIUS User Profile with RADIUS Tunneling Attributes Example

The following example shows a RADIUS user profile (Merit Daemon format) that includes RADIUS tunneling attributes.

```
cisco-avpair = vpdn:l2tp-cm-local-window-size=1024
```

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

# Guard Timer Examples

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

```
interface serial1/0/0:23
 isdn guard-timer 8000 on-expiry reject
aaa preauth
 group radius
 dnis required
```

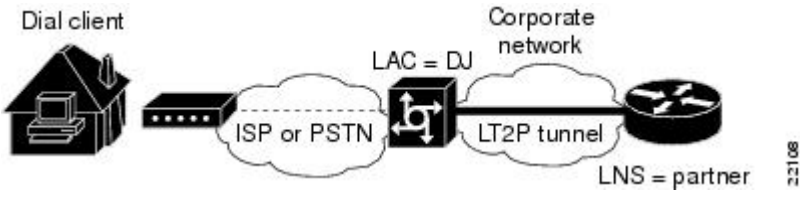
The following example shows a CAS guard timer that is set at 20,000 milliseconds. A call will be accepted if the RADIUS server has not responded to a preauthentication request when the timer expires.

```
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 preauth
group radius
dnis required
```

# L2TP Access Concentrator Examples

The following example shows a basic L2TP configuration for the L2TP access concentrator (LAC) for the topology shown in the figure below. The local name is not defined, so the host name used is the local name. Because the L2TP tunnel password is not defined, the username password is used. In this example, VPDN is configured locally on the LAC and does not take advantage of the new RADIUS tunnel attributes.

***Figure 1 Topology for Configuration Examples***




```
! Enable AAA globally.
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
! authentication.
aaa authentication ppp default local
! Define the username as “DJ.”
```

```
username DJ password 7 030C5E070A00781B
! Enable VPDN.
vpdn enable
! Define VPDN group number 1.
vpdn-group 1
! Allow the LAC to respond to dialin requests using L2TP from IP address 172.21.9.13
! domain “cisco.com.”
 request dialin
  protocol l2tp
  domain cisco.com
 initiate-ip to 172.21.9.13
 local name nas-1
```

The following example shows how to configure the LAC if RADIUS tunnel attributes are supported. In this example, there is no local VPDN configuration on the LAC; the LAC, instead, is configured to query the remote RADIUS security server.

```
! Enable global AAA securities services.
aaa new-model
! Enable AAA authentication for PPP and list RADIUS as the default method to use
! for PPP authentication.
aaa authentication ppp default group radius local
! Enable AAA (network) authorization and list RADIUS as the default method to use for
! authorization.
aaa authorization network default group radius
! Define the username as “DJ.”
username DJ password 7 030C5E070A00781B
! Enable VPDN.
vpdn enable
! Configure the LAC to interface with the remote RADIUS security server.
radius host 171.19.1.1 auth-port 1645 acct-port 1646
radius-server key cisco
```

# L2TP Network Server Examples

The following example shows a basic L2TP configuration with corresponding comments on the L2TP network server (LNS) for the topology shown in the L2TP Access Concentrator Examples module:

```
! Enable AAA globally.
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
! authentication.
aaa authentication ppp default local
! Define the username as “partner.”
username partner password 7 030C5E070A00781B
! Create virtual-template 1 and assign all values for virtual access interfaces.
interface Virtual-Template1
! Borrow the IP address from loopback interface.
 ip unnumbered loopback0
! Disable multicast fast switching.
 no ip mroute-cache
! Use CHAP to authenticate PPP.
 ppp authentication chap
! Enable VPDN.
vpdn enable
! Create vpdn-group number 1.
vpdn-group 1
! Accept all dialin l2tp tunnels from virtual-template 1 from remote peer DJ.
 accept dialin l2tp virtual-template 1 remote DJ
  protocol any
  virtual-template 1
 terminate-from hostname nas1
local name hgw1
```

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

```
aaa new-model
```

```
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface GigabitEthernet1/0/0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered loopback0
ppp authentication pap
!
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| RADIUS commands | *Cisco IOS Security Command Reference* |
| Other configuration commands | Cisco IOS Master Command List, All Releases |
| L2TP, VPN, or VPDN | *Cisco IOS XE VPDN Configuration Guide* , Release 2 |

### Standards

| Standard | Title |
|---|---|
| None. | -- |

### 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:<br>http://www.cisco.com/go/mibs |

### RFCs

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

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>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.<br>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 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 1 Feature Information for Configuring RADIUS*

| Feature Name | Releases | Feature Information |
|---|---|---|
| AAA Server Group | Cisco IOS XE Release 2.1 | Configuring the router 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 in conjunction with a global server-host list. The server group lists the IP addresses of the selected server hosts.<br><br>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.<br><br>The following commands were introduced or modified: **aaa group server radius**, **aaa group server tacacs+**, and **server (RADIUS)**. |
| AAA Server Group Enhancements | Cisco IOS XE Release 2.1 | AAA Server Group Enhancements enables the full configuration of a server in a server group.<br><br>In Cisco IOS XE Release 2.1, this feature is supported on the Cisco ASR 1000 Series Aggregation Services Routers. |
| RADIUS | Cisco IOS XE Release 2.1 | RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.<br><br>In Cisco IOS XE Release 2.1, this feature is introduced on the Cisco ASR 1000 Series Aggregation Services Routers. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| AAA Server Group Deadtimer | Cisco IOS XE Release 2.1 | Configuring deadtime within a server group allows you to direct AAA traffic to separate groups of servers that have different operational characteristics. A separate timer has been 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.<br><br>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.<br><br>The following command was introduced or modified:<br><br>**deadtime** . |

| Feature Name | Releases | Feature Information |
|---|---|---|
| AAA DNIS Map for Authorization | Cisco IOS XE Release 2.3 | Cisco IOS XE software 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.<br><br>In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.<br><br>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**. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| RADIUS for Multiple User Datagram Protocol Ports | Cisco IOS XE Release 2.4 | RADIUS security servers are identified on the basis of their host name or IP address, host name 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. In other words, this unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.<br><br>In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.<br><br>The following command was introduced or modified:<br><br>**radius-server host** . |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

# 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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

## Prerequisites for 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.

# Configuration Examples for Framed-Route in RADIUS Accounting



## 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:<br>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.<br>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.<br>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 2 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.<br><br>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

# 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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

## 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 3 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<br>• NAS-IP-Address (4)--from AAA<br>• Acct-Delay-Time (41)--from AAA<br>• Event-Timestamp (55)--from AAA<br>• Tunnel-Type (64)--from client<br>• Tunnel-Medium-Type (65)--from client<br>• Tunnel-Client-Endpoint (66)--from client<br>• Tunnel-Server-Endpoint (67)--from client<br>• 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.

| 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<br>• NAS-IP-Address (4)--from AAA<br>• Acct-Delay-Time (41)--from AAA<br>• Acct-Input-Octets (42)--from AAA<br>• Acct-Output-Octets (43)--from AAA<br>• Acct-Session-Id (44)--from AAA<br>• Acct-Session-Time (46)--from AAA<br>• Acct-Input-Packets (47)--from AAA<br>• Acct-Output-Packets (48)--from AAA<br>• Acct-Terminate-Cause (49)--from AAA<br>• Acct-Multi-Session-Id (51)--from AAA<br>• Event-Timestamp (55)--from AAA<br>• Tunnel-Type (64)--from client<br>• Tunnel-Medium-Type (65)--from client<br>• Tunnel-Client-Endpoint (66)--from client<br>• Tunnel-Server-Endpoint (67)--from client<br>• Acct-Tunnel-Connection (68)--from client<br>• Acct-Tunnel-Packets-Lost (86)--from client |

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

| 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<br>• NAS-IP-Address (4)--from AAA<br>• Acct-Delay-Time (41)--from AAA<br>• Acct-Terminate-Cause (49)--from client<br>• Event-Timestamp (55)--from AAA<br>• Tunnel-Type (64)--from client<br>• Tunnel-Medium-Type (65)--from client<br>• Tunnel-Client-Endpoint (66)--from client<br>• Tunnel-Server-Endpoint (67)--from client<br>• 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<br>• NAS-IP-Address (4)--from AAA<br>• NAS-Port (5)--from AAA<br>• Acct-Delay-Time (41)--from AAA<br>• Event-Timestamp (55)--from AAA<br>• Tunnel-Type (64)--from client<br>• Tunnel-Medium-Type (65)--from client<br>• Tunnel-Client-Endpoint (66)--from client<br>• Tunnel-Server-Endpoint (67)--from client<br>• 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.

| 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<br>• NAS-IP-Address (4)--from AAA<br>• NAS-Port (5)--from AAA<br>• Acct-Delay-Time (41)--from AAA<br>• Acct-Input-Octets (42)--from AAA<br>• Acct-Output-Octets (43)--from AAA<br>• Acct-Session-Id (44)--from AAA<br>• Acct-Session-Time (46)--from AAA<br>• Acct-Input-Packets (47)--from AAA<br>• Acct-Output-Packets (48)--from AAA<br>• Acct-Terminate-Cause (49)--from AAA<br>• Acct-Multi-Session-Id (51)--from AAA<br>• Event-Timestamp (55)--from AAA<br>• NAS-Port-Type (61)--from AAA<br>• Tunnel-Type (64)--from client<br>• Tunnel-Medium-Type (65)--from client<br>• Tunnel-Client-Endpoint (66)--from client<br>• Tunnel-Server-Endpoint (67)--from client<br>• Acct-Tunnel-Connection (68)--from client<br>• Acct-Tunnel-Packets-Lost (86)--from client |

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

| 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<br>• NAS-IP-Address (4)--from AAA<br>• Acct-Delay-Time (41)--from AAA<br>• Acct-Terminate-Cause (49)--from AAA<br>• Event-Timestamp (55)--from AAA<br>• Tunnel-Type (64)--from client<br>• Tunnel-Medium-Type (65)--from client<br>• Tunnel-Client-Endpoint (66)--from client<br>• Tunnel-Server-Endpoint (67)--from client<br>• Acct-Tunnel-Connection (68)--from client |

# 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

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

**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**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| Command or Action | Purpose |
|---|---|
| **Step 3** Router(config)# **aaa accounting network default** *list-name*} {**start-stop** \| **stop-only** \| **wait-start** \| **none group** *groupname*<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>`Router(config)# aaa accounting network m1 start-stop group radius` | Enables network accounting.<br><br>• **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.<br><br>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.<br><br>• *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 |
|---|---|---|
| **Step 4** | Router(config)# **vpdn enable**<br><br>**Example:**<br><br>`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*<br><br>**Example:**<br><br>`Router(config)# vpdn tunnel accounting network m1` | Enables Tunnel-Start, Tunnel-Stop, and Tunnel-Reject accounting records.<br><br>• *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*<br><br>**Example:**<br><br>`Router(config)# vpdn session accounting network m1` | Enables Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject accounting records.<br><br>• *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, page 53

## 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**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | Router# **show accounting**<br><br>**Example:**<br>`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**]<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br>`Router# show vpdn session` | Displays information about active L2TP tunnel and message identifiers in a VPDN.<br>• **session** --Displays a summary of the status of all active tunnels.<br>• **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*<br>• *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:<br>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.<br>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.<br>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 4 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).<br><br>This feature also introduces two new virtual private virtual private dialup network (VPDN) commands that help users better troubleshoot VPDN session events.<br><br>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.<br><br>The following commands were introduced or modified: **aaa accounting**, **vpdn session accounting network**, **vpdn tunnel accounting network**. |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

# 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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

## Prerequisites for 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**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip radius source-interface** *interface-name*<br><br>**Example:**<br><br>**Example:**<br>`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**]<br><br>**Example:**<br><br>**Example:**<br>`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.<br>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.<br>• 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**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **debug radius**<br><br>**Example:**<br>`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

### 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* |
| AAA authentication | Configuring Authentication feature module. |
| Attribute screening for access requests | RADIUS Attribute Value Screening feature module. |

### Standards

| Standard | Title |
|---|---|
| None. | -- |

### 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:<br>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.<br>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.<br>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 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 5 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.<br>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.<br>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. |
| LLID Blocking | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |

# Glossary

**LLID Blocking** --A feature that enables administrators to track their customers on the basis of the physical lines on which the calls of the customers originate. Also known as RADIUS Logical Line ID.

**RADIUS Logical Line ID** --A feature that enables administrators to track their customers on the basis of the physical lines on which the calls of the customers originate. Also known as LLID Blocking.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

# 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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

## Prerequisites for 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:<br>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.<br>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.<br>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 6 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.<br><br>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.<br><br>The following commands were introduced: **aaa route download** |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

# RADIUS Server Load Balancing

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.



## Finding Feature Information

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

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

## Prerequisites for RADIUS Server Load Balancing

- AAA must be configured on your RADIUS server.
- RADIUS must be configured for functions such as authentication, accounting, or static route download.
- AAA RADIUS server groups must be established.

## Restrictions for RADIUS Server Load Balancing

- Load balancing is not supported on proxy RADIUS servers.

- Incoming RADIUS requests, such as Packet of Disconnect (POD) requests, are not supported.
- Load balancing is not supported for private server-groups.

# Information About RADIUS Server Load Balancing



## How RADIUS Server Load Balancing Works

Load balancing distributes batches of transactions to servers within a server group. It 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:

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

Batch size is a user configured parameter. Changes in 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. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.

**Note** There is no set number for large or small batch sizes. As a frame of reference, a batch size greater than 50 is considered large and a batch size less than 25 is considered small.

**Note** If you have ten or more servers in a server group, it is recommended that a high batch size be set in order to reduce CPU load.

## How Transactions Are Load-Balanced Across RADIUS Server Groups

You can configure load balancing either per named RADIUS server group or for the global RADIUS server group. This server group must be referred to as “radius” in the AAA method lists. All public servers that are part of this server group will then be load balanced.

Authentication and accounting can be configured to use the same server or different servers. In some cases, the same server is used for preauthentication, authentication, or accounting transactions for a session. The preferred server, which is an internal setting and set as default, tells AAA to use same server for the start and stop record for a session regardless of server cost. When using the preferred server setting, it is expected that the server used for the initial transaction (for example, authentication), the preferred server, should also be part of any other server group that is used for a subsequent transaction (for example, accounting).

The preferred server is used unless one of the following states is true:

- The **ignore-preferred-server** keyword 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 server cost. If the want server is not available, the transaction fails.

You may want to use the **ignore-preferred-server** keyword 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 those records are stored on separate servers.

Also, if you have a configuration where your authentication servers are a superset of your accounting servers, then the preferred server will not be used.

# RADIUS Server Status and Automated Testing

The RADIUS Server Load Balancing feature takes server status into account when assigning batches. Only servers that are verified alive are sent transaction batches. It is recommended that you test the status 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 is in quarantine. A server is in quarantine until it is verified alive by the RADIUS automated tester functionality.

The RADIUS automated tester uses the following steps to determine if a server is alive and available to process transactions:

- A request is sent periodically to the server for a test user ID.
- If an Access-Reject message is returned from the server, the server is alive.
- If no message is returned from the server, it is not alive; that is, the server is either dead or quarantined.

If transactions have been sent to a server that is not responding, before it is marked dead, that transaction is failed over to the next available server. It is recommended that the retry reorder mode for failed transactions be used.

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

**Caution** It is recommended that a test user, one that is not defined on the RADIUS server, be used for RADIUS server automated testing to protect against security issues that may arise if the test user is not correctly configured.

**Note** If you want to check load balancing transactions at a specific point in time, you can use the **test aaa group** command.

# How to Configure RADIUS Server Load Balancing



## Enabling Load Balancing for Named RADIUS Server Group

Use the following task to enable RADIUS Server Load Balancing for a named server group.

### SUMMARY STEPS

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

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **radius-server host** {*hostname*| *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**idle-time** *seconds*]<br><br>**Example:**<br>`Router(config)# radius-server host 192.0.2.1 test username test1 idle-time 1` | Enables RADIUS automated testing.<br>• The **test username** keyword must be used to enable RADIUS automated testing, followed by the value for the *user-name* argument.<br>• By default, **auth-port** is tested using port 1645.<br>• Use **ignore-auth-port** to turn off testing of the authentication port.<br>• By default, **acct-port** is tested using port 1645.<br>• Use **ignore-acct-port** to turn off testing of the accounting port.<br>• By default, the **idle-time**is 3600 seconds. The range is 1 - 35791. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **aaa group server radius** *group-name*<br><br>**Example:**<br><br>`Router(config)# aaa group server radius rad-sg` | Enters server group configuration mode. |
| **Step 5** | **load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]<br><br>**Example:**<br><br>`Router(config-sg)# load-balance method least-outstanding batch-size 30` | Enables least-outstanding load balancing for a server group.<br>• By default, the **batch-size** is set to 25. A range of 1 - 2147483647 may be used.<br>• By default, the preferred server is enabled.<br>• If you want to disable the preferred-server setting, use the keyword **ignore-preferred-server**. |

# Enabling Load Balancing for Global RADIUS Server Group

Use the following task to enable RADIUS Server Load Balancing for the global RADIUS server group. This is the group referred to as “radius” in the AAA method lists.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname*| *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *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**

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **radius-server host** {*hostname*\| *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**idle-time** *seconds*]<br><br>**Example:**<br><br>`Router(config)# radius-server host 192.0.2.1 test username test1 idle-time 1` | Enables RADIUS automated testing.<br>• The **test username** keyword must be used to enable RADIUS automated testing, followed by the value for the *user-name* argument.<br>• By default, **auth-port** is tested using port 1645.<br>• Use **ignore-auth-port** to turn off testing of the authentication port.<br>• By default, **acct-port** is tested using port 1645.<br>• Use **ignore-acct-port** to turn off testing of the accounting port.<br>• By default, the **idle-time**is 3600 seconds. The range is 1 - 35791. |
| **Step 4** | **radius-server load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]<br><br>**Example:**<br><br>`Router(config)# radius-server load-balance method least-outstanding` | Enables least-outstanding load balancing for the global RADIUS server group and enters server group configuration mode.<br>• By default, the **batch-size** is set to 25. A range of 1 - 2147483647 may be used.<br>**Note** Batch size may impact throughput and CPU load. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.<br>• By default, the preferred server is enabled.<br>• If you want to disable the preferred server setting, use the **ignore-preferred-server** keyword. |
| **Step 5** | **load-balance method least-outstanding batch-size** *number* **ignore-preferred-server**<br><br>**Example:**<br><br>`load-balance method least-outstanding batch-size 5` | Enables RADIUS server load balancing for a named RADIUS server group.<br>• By default, the **batch-size** is set to 25. A range of 1 - 2147483647 may be used.<br>• By default, the preferred server is enabled.<br>• If you want to disable the preferred server setting, use the **ignore-preferred-server** keyword. |

# Troubleshooting RADIUS Server Load Balancing

After configuring the RADIUS Server Load Balancing feature, you may monitor the idle timer, dead timer, load balancing server selection, or issue a manual test command to verify server status.

Use the following commands as appropriate for troubleshooting the RADIUS Server Load Balancing feature:

- The **debug aaa test** command can be used to determine when the idle timer or dead timer has expired, when test packets are sent, the status of the server, or to verify server state.
- The **debug aaa sg-server selection**command can be used to examine which server is being selected for load balancing.
- The **test aaa group** command can be used to manually verify RADIUS load-balanced server status.

### SUMMARY STEPS

1. The idle timer is used to check the server status and is updated with or without any incoming requests. It is useful to monitor the idle timer to determine if there are nonresponsive servers and to keep your RADIUS server status updated in order to efficiently utilize your available resources. For instance, an updated idle timer would help ensure that incoming requests are being sent to servers that are alive.
2. For example, the following debug output shows 5 access requests being sent to a server group with a batch size of 3:
3. The following example 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 a AAA packet generated by the **test aaa group** command.

### DETAILED STEPS

**Step 1** The idle timer is used to check the server status and is updated with or without any incoming requests. It is useful to monitor the idle timer to determine if there are nonresponsive servers and to keep your RADIUS server status updated in order to efficiently utilize your available resources. For instance, an updated idle timer would help ensure that incoming requests are being 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 can help you determine how often the server selection changes. This is effective in analyzing if there is a bottleneck, a large number of queued up requests, or if only specific servers are processing incoming requests.

For example, the following debug output shows when the idle-timer has expired:

**Example:**

```
Router# 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** For example, the following debug output shows 5 access requests being sent to a server group with a batch size of 3:

**Example:**

```
Router# 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** The following example 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 a AAA packet generated by the **test aaa group** command.

**Example:**

```
Router# 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



## Global RADIUS Server Group Examples

The following example shows how to enable load balancing for global RADIUS server groups. It is shown in three parts: the current configuration of RADIUS command output, debug output, and AAA server status information. You can use the delimiting characters to display only the relevant parts of the configuration.

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

The following shows the relevant RADIUS configuration.

```
Router# 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
```

The lines in the current configuration of 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 the AAA server once the client is authenticated and after the disconnect using the keyword **start-stop**.
- 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 key identified.
- The **radius-server load-balance** command enables load balancing for the global radius server groups with the batch size specified.

## Debug Output for Global RADIUS Server Group Example

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

```
Router# show debug
General OS:
  AAA server group server selection debugging is on
#
<sending 10 pppoe requests>
Router#
*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.
```

## Server Status Information for Global RADIUS Server Group Example

The output below shows the AAA server status for the global RADIUS server group configuration example.

```
Router# 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 output shows the status of two RADIUS servers. Both servers are up and, in the last 2 minutes, have successfully processed:

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

# Named RADIUS Server Group Examples

The following example shows load balancing enabled for a named RADIUS server group. It is shown in three parts: the current configuration of RADIUS command output, debug output, and AAA server status information.



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

The following shows the relevant RADIUS configuration.

```
Router# 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 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 the 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 the sending of all accounting requests to the AAA server once the client is authenticated and after the disconnect using the **start-stop** keyword.

## Debug Output for Named RADIUS Server Group Example

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

```
Router#
*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.
.
.
.
```

## Server Status Information for Named RADIUS Server Group Example

The output below shows the AAA server status for the named RADIUS server group configuration example.

```
Router# 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 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.

# Idle Timer Monitoring Examples

The following example shows idle timer and related server state for load balancing enabled for a named RADIUS server group. It is shown in two parts: the current configuration of RADIUS command output and debug output.


- Server Configuration and Enabling Load Balancing for Idle Timer Monitoring Example, page 87
- Debug Output for Idle Timer Monitoring Example, page 87


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

The following shows the relevant RADIUS configuration.

```
Router# 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 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 the 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.

## Debug Output for Idle Timer Monitoring Example

The debug output below shows the 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.

```
Router#
*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.
.
.
.
```

# Preferred Server with the Same Authentication and Authorization Server Example

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
```

Once 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 will be load balanced based on sessions rather than transactions.

# Preferred Server with Different Authentication and Authorization Servers Example

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 will never be found for accounting transactions, therefore, authentication and accounting servers will be load balanced based on transactions. Start and stop records will be sent to the same server for a session.

# Preferred Server with Overlapping Authentication and Authorization Servers Example

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 will be directed towards server 209.165.201.1. Therefore, one-third of all accounting transactions will also be directed towards server 209.165.201.1. The remaining two-thirds accounting transactions will be load balanced equally between servers 209.165.201.1 and 209.165.201.2. The server 209.165.201.1 will receive fewer authentication transactions since server 209.165.201.1 will have outstanding accounting transactions.

# Preferred Server with Authentication Servers As a Subset of Authorization Servers Example

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 will be sent to server 209.165.200.225 and the other half to server 209.165.200.226. Servers 209.165.200.225 and 209.165.200.226 will be the preferred servers for authentication and accounting transaction, therefore there will be an equal distribution of authentication and accounting transactions across servers 209.165.200.225 and 209.165.200.226. Server 209.165.201.1 will be relatively unused.

# Preferred Server with Authentication Servers As a Superset of Authorization Servers Example

The following example shows an authentication server group that uses servers 209.165.200.225 and 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 will be assigned to each server in the authorization server group. As accounting transactions are generated for more sessions, the accounting transactions will only be sent to servers 209.165.200.225 and 209.165.200.226, since 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. The transaction requests authenticated by server 209.165.201.1, will not have any preferred server setting and will be 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

### 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* |
| AAA and RADIUS | Configuring Authentication, Configuring Authorization, and Configuring Accounting feature modules. |
| Configuring RADIUS | Configuring RADIUS feature module. |
| Failover retry reorder mode | RADIUS Server Reorder on Failure feature module. |

### Standards

| Standards | Title |
|---|---|
| None. | -- |

### MIBs

| MIBs | 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:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | 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.<br><br>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.<br><br>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 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 7 Feature Information for RADIUS Server Load Balancing*

| Feature Name | Releases | Feature Information |
|---|---|---|
| RADIUS Server Load Balancing | Cisco IOS XE Release 2.1 | 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.<br><br>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.<br><br>The following commands were introduced or modified by this feature: **debug aaa sg-server selection debug aaa test, load-balance (server-group) radius-server host radius-server load-balance test aaa group** |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

# 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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

## Prerequisites for 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 Cisco IOS XE 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 Cisco IOS XE 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, page 95

### 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, page 95
- Monitoring RADIUS Server Reorder on Failure, page 97

## 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**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Router (config)# aaa new-model` | Enables the AAA access control model. |
| **Step 4** | **radius-server retry method reorder**<br><br>**Example:**<br><br>**Example:**<br>`Router (config)# radius-server retry method reorder` | Specifies the reordering of RADIUS traffic retries among a server group. |
| **Step 5** | **radius-server retransmit** {*retries*}<br><br>**Example:**<br>`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.<br>The *retries* argument is the maximum number of retransmission attempts. The default is 3 attempts. |
| **Step 6** | **radius-server transaction max-tries {** *number* **}**<br><br>**Example:**<br>`Router (config)# radius-server transaction max-tries 3` | Specifies the maximum number of transmissions per transaction that may be retried on a RADIUS server.<br>The *number* argument is the total number of transmissions per transaction. If this command is not configured, the default is eight transmissions.<br>**Note** This command is global across all RADIUS servers for a given transaction. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **radius-server host {** *hostname* \| *ip-address* **} [ key** *string* **]**<br><br>**Example:**<br><br>`Router (config)# radius-server host 10.2.3.4 key radi23` | Specifies a RADIUS server host.<br><br>**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* **]**<br><br>**Example:**<br><br>`Router (config)# radius-server host 10.5.6.7 key rad234` | Specifies a RADIUS server host.<br><br>**Note** At least two servers must be configured. |

# 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**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **debug aaa sg-server selection**<br><br>**Example:**<br><br>`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. |

| Command or Action | Purpose |
|---|---|
| **Step 3** **debug radius**<br><br>**Example:**<br><br>`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* |

| Related Topic | Document Title |
|---|---|
| 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:<br>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.<br>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.<br>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 8 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.<br>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.<br>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.** |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

# 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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

## 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**<br><br>**Example:**<br>`Router> enable` | Enters privileged EXEC mode.<br>Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | Router(config)# **radius-server backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *retransmits*<br><br>**Example:**<br>`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*}]<br><br>**Example:**<br>`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**<br><br>**Example:**<br>`Router> enable` | Enters privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`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**<br><br>**Example:**<br>`Router> enable` | Enters privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **debug radius**<br><br>**Example:**<br>`Router# debug radius` | Displays information associated with RADIUS. |
| **Step 3** | **show accounting**<br><br>**Example:**<br>`Router# show accounting` | Displays all active sessions and prints all the accounting records for actively accounted functions. |
| **Step 4** | **show radius statistics**<br><br>**Example:**<br>`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, page 109
- Per-Server Configuration Example, page 110


## 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<br>• 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:<br>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.<br>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.<br>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 9 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.<br><br>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.<br><br>The following commands were introduced or modified: **backoff exponential**, **radius-server host**, **radius-server backoff exponential**. |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.