RADIUS Server Reorder on Failure

First Published: May 19, 2003
Last Updated: February 23, 2006

During periods of high load or when server failure occurs, the RADIUS Server Reorder on Failure feature provides for failover to another server in the server group. 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 will not be automatically switched back to the first server.

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

History for the RADIUS Server Reorder on Failure Feature

Release	Modification
12.3(1)	This feature was introduced.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- Prerequisites for RADIUS Server Reorder on Failure, page 2
- Restrictions for RADIUS Server Reorder on Failure, page 2
- Information About RADIUS Server Reorder on Failure, page 2
- How to Configure RADIUS Server Reorder on Failure, page 3
- Configuration Examples for RADIUS Server Reorder on Failure, page 7

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

© 2003, 2005–2006 Cisco Systems, Inc. All rights reserved.

- Additional References, page 10
- Command Reference, page 11

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. (Refer to the chapter "AAA Overview" in the *Cisco IOS Security Configuration Guide*, Release 12.3.)
- 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 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 will behave as though the reorder feature is not configured.

Information About RADIUS Server Reorder on Failure

To configure the RADIUS Server Reorder on Failure feature, you must understand the following concepts:

- RADIUS Server Failure, page 2
- How the RADIUS Server Reorder on Failure Feature Works, page 3

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 will transmit 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 will go 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 critiera (not configurable; it varies depending on the version of Cisco IOS 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 will be as follows:

- The network access server (NAS) maintains the status of “flagged” server, which is the first server to which a transmission is sent.
- After the transmission is sent to the flagged server, the transmission is sent to the flagged server again for the configured number of retransmissions.
- The NAS then sequentially sends the transmission through the list of nondead servers in the server group, starting with the one listed after the flagged server, until the configured transaction maximum tries is reached or until a response is received.
- At boot time, the flagged server is the first server in the server group list as was established using the **radius-server host** command.
- If the flagged server is marked as dead (even if the dead time is zero), the first nondead server listed after the flagged server becomes the flagged server.
- If the flagged server is the last server in the list, and it is marked as dead, the flagged server becomes the first server in the list that is not marked as dead.
- If all servers are marked as dead, the transaction fails, and no change is made to the flagged server.
- If the flagged server is marked as dead, and the dead timer expires, nothing happens.

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

When RADIUS Servers Are Dead

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

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

How to Configure RADIUS Server Reorder on Failure

This section contains the following procedures.

- Configuring a RADIUS Server to Reorder on Failure, page 4 (required)
- Monitoring RADIUS Server Reorder on Failure, page 5 (optional)

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*}
1. **radius-server host** {*hostname* | *ip-address*} [*key string*]
2. **radius-server host** {*hostname* | *ip-address*} [*key string*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**`enable`** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**`configure terminal`** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**`aaa new-model`** **Example:** `Router (config)# aaa new-model`	Enables the AAA access control model.
Step 4	**`radius-server retry method reorder`** **Example:** `Router (config)# radius-server retry method reorder`	Specifies the reordering of RADIUS traffic retries among a server group.
Step 5	**`radius-server retransmit`** {*retries*} **Example:** `Router (config)# radius-server retransmit 1`	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up. The *retries* argument is the maximum number of retransmission attempts. The default is 3 attempts.

	Command or Action	Purpose
Step 6	**radius-server transaction max-tries** {*number*} **Example:** `Router (config)# radius-server transaction max-tries 3`	Specifies the maximum number of transmissions per transaction that may be retried on a RADIUS server. The *number* argument is the total number of transmissions per transaction. If this command is not configured, the default is eight transmissions. **Note** This command is global across all RADIUS servers for a given transaction.
Step 7	**radius-server host** {*hostname* | *ip-address*} [**key** *string*] **Example:** `Router (config)# radius-server host 10.2.3.4 key radi23`	Specifies a RADIUS server host. **Note** You can also configure a global key for all RADIUS servers that do not have a per-server key configured by issuing the **radius-server key** command.
Step 8	**radius-server host** {*hostname* | *ip-address*} [**key** *string*] **Example:** `Router (config)# radius-server host 10.5.6.7 key rad234`	Specifies a RADIUS server host. **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`** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**`debug aaa sg-server selection`** **Example:** `Router# debug aaa sg-server selection`	Displays information about why the RADIUS and TACAC+ server group system in the router is choosing a particular server.
Step 3	**`debug radius`** **Example:** `Router# debug radius`	Displays information about why the router is choosing a particular RADIUS server.

Examples

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

Debug 1

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 will 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 1.1.1.1
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 "david"
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 2.2.2.2
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]
```

Debug 2

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 "david" 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

This section provides the following configuration examples:

- Configuring a RADIUS Server to Reorder on Failure Example, page 8
- Determining Transmission Order When RADIUS Servers Are Dead, page 8

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:

```
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
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:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 1
radius-server transaction max-tries 3
radius-server host 10.2.3.4
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 will 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:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 1
radius-server max-tries-per-transaction 8
radius-server host 10.1.1.1
radius-server host 10.2.2.2
radius-server host 10.3.3.3
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 will 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 will 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

The following sections provide references related to RADIUS Server Reorder on Failure.

Related Documents

Related Topic	Document Title
AAA and RADIUS	The section "Authentication, Authorization, and Accounting (AAA)" and the chapter "Configuring RADIUS," respectively, in the *Cisco IOS Security Configuration Guide*, Release 12.4 T
AAA and RADIUS commands	*Cisco IOS Security Command Reference*, Release 12.4 T
Enabling AAA	"AAA Overview" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.4 T

Standards

Standards	Title
None	—

MIBs

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

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents modified commands only.

- **debug aaa sg-server selection**
- **radius-server retry method reorder**
- **radius-server transaction max-tries**

debug aaa sg-server selection

To obtain information about why the RADIUS and TACACS+ server group system in a router is choosing a particular server, use the **debug aaa sg-server selection** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug aaa sg-server selection

no debug aaa sg-server selection

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is not turned on.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

The following example shows that debugging has been set to display information about server selection:

```
Router# debug aaa sg-server selection
```

The following two debug outputs display the behavior of RADIUS transactions within a server group with the server-reorder-on-failure feature configured.

Debug 1

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 will 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: 10.0.0.0
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 10.1.1.1
```

```
00:38:59: RAPIUS(0000000F) : Send Access-Request to 1.1.1.1:1645 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 "david"
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 (2.2.2.2:1645,1646) for id 21645/11
00:39:02: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 2.2.2.2
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]
```

Debug 2

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 1.1.1.1 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: 10.0.0.0
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 "david" 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 (10.1.1,1:1645,1646) for id 21645/14
00:43:42: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 1.1.1.1
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 2.2.2.2
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 (10.1.1.1:1645,1646) for id 21645/14
00:43:48: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 1.1.1.1
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 2.2.2.2
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 (10.1.1.1:1645,1646) 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 (1.1.1.1:1645,1646) for id 21645/14 00:43:56:

RADIUS/DECODE: parse response no app start; FAIL 00:43:56: RADIUS/DECODE: parse response;

FAIL
```

The field descriptions are self-explanatory.

Related Commands

Command	Description
radius-server retry method reorder	Specifies the reordering of RADIUS traffic retries among a server group.
radius-server transaction max-tries	Specifies the maximum number of transmissions per transaction that may be retried on a RADIUS server.

radius-server retry method reorder

To specify the reordering of RADIUS traffic retries among a server group, use the **radius-server retry method reorder** command in global configuration mode. To disable the reordering of retries among the server group, use the **no** form of this command.

radius-server retry method reorder

no radius-server retry method reorder

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, RADIUS traffic is not reordered among the server group.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use this command to reorder RADIUS traffic to another server in the server group when the first server fails in periods of high load. 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 will not be automatically switched back to the first server.

If the **radius-server retry method reorder** command is not configured, each RADIUS server is used until marked dead. The nondead server that is closest to the beginning of the list is used for the first transmission of a transaction and for the configured number of retransmissions. Each nondead server in the list is thereafter tried in turn.

Examples

The following example shows that RADIUS server retry has been configured:

```
Router (config)# 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
```

Related Commands

Command	Description
radius-server transaction max-tries	Specifies the maximum number of transmissions that may be retried per transaction on a RADIUS server.

radius-server transaction max-tries

To specify the maximum number of transmissions that may be retried per transaction on a RADIUS server, use the **radius-server transaction max-retries** command in global configuration mode. To disable the number of retries that were configured, use the **no** form of this command.

radius-server transaction max-tries *number*

no radius-server transaction max-tries *number*

Syntax Description

number	Total number of transmissions per transaction. The default is eight.

Defaults

Eight transmissions

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use this command to specify the maximum number of transmissions that may be retried per transaction on a RADIUS server. This command has no meaning if the **radius-server retry method order** command has not been already configured.

Examples

The following example shows that a RADIUS server has been configured for six retries per transaction:

```
aaa new-model
radius-server retry method reordeer
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 10.2.3.4
radius-server host 10.6.7.8
```

Related Commands

Command	Description
radius-server retry method reorder	Specifies the reordering of RADIUS traffic retries among a server group.

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

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

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

© 2003, 2005–2006 Cisco Systems, Inc. All rights reserved.