Identity Based Networking Services
Demystifying RADIUS Server Configurations

Last Updated: 05/2014

This paper is intended to provide insights into the RADIUS server configurations on a Cisco® Catalyst switch, router or IOS based wireless controllers in the context of enterprise network access security. While IEEE 802.1X enables authenticated access to IEEE 802 media, including Ethernet and 802.11 wireless LANs, the RADIUS infrastructure facilitates centralized Authentication, Authorization, and Accounting (AAA) management for users and devices that connect and use network service(s). To deploy a Cisco identity based network, an understanding about these two protocols is fundamental. This document focuses predominantly on the RADIUS server configurations, best practices and some troubleshooting. For information and details on other Identity Based Networking Services (IBNS) components and solutions, visit: [www.cisco.com/go/ibns](http://www.cisco.com/go/ibns).

Overview

In an identity based network an endpoint (supplicant) initiates its network access session with a 802.1X authentication. The IEEE 802.1X access control protocol is fundamentally a layer 2 transport protocol that carries the Extensible Authentication Protocol (EAP) payload in it. EAP is an authentication framework that defines the transport and usage of identity credentials. EAP encapsulates the usernames, passwords, certificates, tokens, OTPs, etc. that a client sends for the purpose of authentication. The first hop Network Access Server (NAS) (switch/router/wireless controller), hands off the EAP payload to the authentication server via the RADIUS messaging. The RADIUS server either performs lookups with its internal user database or queries an external identity store, and responds to the client accordingly with the appropriate authorization permissions. The availability and servicability of a RADIUS server is fundamental for an enterprise grade secure access solution to operate.
RADIUS is a distributed client/server system that secures networks against unauthorized access. It's an open standard protocol that can be customized with vendor specific attributes. In the Cisco implementation, RADIUS clients run on Cisco switches/routers/wireless controllers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. 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.

Configuring the RADIUS Server

RADIUS server configuration on Cisco IOS is performed in two steps, one set of commands are defined within the AAA paradigm and other set is run with the "radius" commands. The aaa configurations on the Cisco IOS needs to be done with named method lists or the default list can be used. The simplest way to start with the configurations is to use the built-in default method lists.

Table 1. AAA Configuration for IEEE 802.1X and RADIUS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa new-model</td>
<td>Enable Authentication Authorization and Accounting (AAA)</td>
</tr>
<tr>
<td>aaa authentication dot1x default group radius</td>
<td>Specifies RADIUS as the method for 802.1X port based authentication</td>
</tr>
<tr>
<td>aaa authorization network default group radius</td>
<td>Governs network authorizations via RADIUS (VLAN / ACL assignment)</td>
</tr>
<tr>
<td>aaa accounting dot1x default start-stop group radius</td>
<td>To enable accounting for 802.1X authentication sessions</td>
</tr>
<tr>
<td>aaa session-id common</td>
<td>Indicates that all session identification (ID) information that is sent out for a given session is identical.</td>
</tr>
</tbody>
</table>

Table 2. RADIUS Server Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius server &lt;name&gt;</td>
<td>Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.</td>
</tr>
<tr>
<td>address ipv4 X.X.X.X auth-port &lt;0-65535&gt; acct-port &lt;0-65535&gt;</td>
<td>Configures the IPv4 address for the RADIUS server accounting and authentication parameters.</td>
</tr>
<tr>
<td>key &lt;shared-secret&gt;</td>
<td>The shared secret key that's configured on the RADIUS server must be defined for secure RADIUS communications.</td>
</tr>
<tr>
<td>ip radius source-interface &lt;interface&gt;</td>
<td>To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the ip radius source-interface command in global configuration mode. The source IP address of the RADIUS packets must match the NAS IP address configured on the RADIUS server. A mismatch leads to RADIUS packet timeout and the server gets marked “DEAD”.</td>
</tr>
</tbody>
</table>

Configuration Example: RADIUS Server

```plaintext
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa session-id common
!
radius server RASERV-1
    address ipv4 172.20.254.4 auth-port 1645 acct-port 1646
    key cisco
```
!  
ip radius source-interface Vlan254
!  
Legacy Configuration for RADIUS Servers
The traditional approach to configure a radius server on a Cisco IOS device would be with the “radius-server” global command. This command is replaced by the “radius server <name>” command, which brings in (1) modularity in configuring RADIUS server host parameters and (2) provides consistent configuration options for IPv4 and IPv6 RADIUS server definitions. The “radius-server” command equivalent of the previous example would be the following:

    radius-server host 172.20.254.4 auth-port 1645 acct-port 1646 key cisco

In IOS versions that support the new “radius server <name>” command, when the “radius-server host” command is configured, the following error message will appear:

switch(config)#radius-server host 10.1.1.1
Warning: The CLI will be deprecated soon
'radius-server host 10.1.1.1'
Please move to 'radius server <name>' CLI.

Note: RADIUS has been officially assigned UDP ports 1812 for RADIUS authentication and 1813 for RADIUS accounting by the Internet Assigned Numbers Authority (IANA). However, prior to IANA allocation of ports 1812 and 1813, ports 1645 and 1646 (authentication and accounting, respectively) were used unofficially, and became the default ports assigned by many RADIUS client/server implementations at that time. The tradition of using 1645 and 1646 for backwards compatibility continues to this day. For this reason, many RADIUS server implementations monitor both sets of UDP ports for RADIUS requests.

The basic configuration mentioned above must suffice for a typical identity deployment requirement. The “show aaa servers” command provides details on the configured AAA servers and its status.

switch#show aaa servers

RADIUS: id 5, priority 1, host 172.20.254.4, auth-port 1645, acct-port 1646
    State: current UP, duration 575s, previous duration 0s
    Dead: total time 0s, count 0
    Quarantined: No
<Output truncated>
To validate that the Cisco IOS device can access and securely communicate with the RADIUS server the “test aaa” exec mode command can be used:

```
switch#test aaa group radius user1 cisco new-code
User successfully authenticated
```

```
switch#test aaa group radius user2 cisco1234 new-code
Usage rejected
```

In the example above, “user1” is the username and “cisco” is the password stored in the identity store that the RADIUS server refers to authenticate. A “User rejected” message too (unless a timeout occurs) indicates that the RADIUS server is alive.

Configuring RADIUS for Vendor Specific Attributes (VSA)
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). Attribute 26 encapsulates vendor specific attributes, allowing vendors to support their own extended attributes otherwise not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor-ID is 9, and the supported option has vendor-type 1, which is named “cisco-avpair.” The value is a string in 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, IPv6, IPX, VOIP, RSVP, SIP, AIRNET, etc. “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. The downloadable IP Access-lists use the Cisco Attribute Value Pair (AVP) “ip:inacl”

**Example:**

```
ip:inacl#100=permit ip any 172.20.254.0 0.0.0.255
ip:inacl#200=deny ip any any
```

| Table 3. RADIUS Vendor Specific Attributes (VSA) Commands |
|---|---|
| **Command** | **Description** |
| radius-server vsa send | To configure the network access server to recognize and use vendor-specific attributes, use the radius-server vsa send command in global configuration mode. To restore the default, use the no form of this command. |
| radius-server vsa send accounting | (Optional) Limits the set of recognized vendor-specific attributes to only accounting attributes. |
| radius-server vsa send authentication | (Optional) Limits the set of recognized vendor-specific attributes to only authentication attributes. |

**Note:** Beginning from Cisco IOS version 15.2(1)E / XE 3.5.0E, the VSA commands are enabled by default. To disable VSA, the “no” option must be used.
To validate default vsa support on your NAS:
switch#show running-config all | include vsa
radius-server vsa send accounting
radius-server vsa send authentication

AAA Method Lists

To enable 802.1X port-based authentication, AAA must be enabled and the authentication specified for the authorization and accounting method lists. A method list is a named list describing the authentication, authorization or accounting methods to be queried (such as RADIUS, TACACS+ or local), in a sequence. The software uses the first method listed to execute the defined AAA operation; if that method fails to respond, the software selects the next method in the method list.

A default method list exists in the software and is enabled with specific aaa authentication, authorization or accounting command. The default method list is automatically applied to all interfaces. In case of an enterprise identity scenario, the aaa method lists would always point to a RADIUS method and if not for Identity Control Policy, only a default list can be used.

Table 4. AAA Method List Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# aaa group server radius &lt;server_list&gt;</td>
<td>To group different RADIUS server hosts into distinct lists and distinct methods, enter the aaa group server radius command in global configuration mode.</td>
</tr>
<tr>
<td>Switch(config-sg-radius)#server name &lt;name&gt;</td>
<td>(RADIUS) server: The radius server IP address can be defined under the aaa method-list or the name of the radius server defined under &quot;radius server&quot; command can be referenced.</td>
</tr>
<tr>
<td>Switch(config)# aaa authentication dot1x default group &lt;server_list&gt;</td>
<td>&lt;server_list&gt;: Use the list of all RADIUS servers for authentication/authorization/accounting defined by 'aaa group server radius' global command.</td>
</tr>
<tr>
<td>Switch(config)# aaa authorization network default group &lt;server_list&gt;</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa accounting dot1x (default) start-stop group &lt;server_list&gt;</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The “aaa” Cisco IOS global command and the method lists are used for several other security purposes, from network device administration, to remote access connection needs. However, since the scope of this document is limited to identity based networks, the additional commands and its details are not being focused on in this document.

A Typical AAA Method List Configuration for Enterprise Identity:
```
  aaa new-model
  !
  aaa group server radius RASERV
    server name RASERV-1
    server name RASERV-2
  !
  aaa authentication dot1x default group RASERV
  aaa authorization network default group RASERV
  aaa accounting dot1x default start-stop group RASERV
  !
  radius server RASERV-1
```
address ipv4 172.20.254.4 auth-port 1813 acct-port 1814
automate-tester username dummy
key cisco
!
radius server RASERV-2
address ipv4 172.20.254.8 auth-port 1645 acct-port 1646
automate-tester username dummy
key cisco
!

VRF Aware RADIUS

Some enterprises define Virtual Routing and Forwarding (VRF) instances to isolate their IP networks. One of the common practices is to separate the management traffic from the regular data communications. While dealing with the RADIUS server in these scenarios, a few additional configurations need to be done on the NAS.

There are two options to define RADIUS servers over VRF instances; Global and Method-list specific.

Table 5. VRF Aware RADIUS Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# ip radius source-interface &lt;interface&gt; vrf &lt;vrf-instance&gt;</code></td>
<td>Use vrf vrf-name to configure this command per Virtual Route Forwarding (VRF). Although this command can be configured under the server group, all functionalities must be consistent between the NAS and all AAA servers; this feature is better defined once per VRF, rather than per server group.</td>
</tr>
<tr>
<td><code>Switch(config)# aaa group server radius &lt;name&gt;</code></td>
<td>To configure the VRF reference of an AAA RADIUS server group, use the ip vrf forwarding command in the server-group configuration mode. When vrf instances are defined both globally and under server-group, the later takes precedence.</td>
</tr>
</tbody>
</table>

VRF-Aware RADIUS Configuration Example

```
! ip radius source-interface Vlan254 vrf VRF-Blue
! -Or-
 aaa group server radius RASERV
   ip vrf forwarding VRF-Blue
   ip radius source-interface Vlan254
   server name RASERV-1
!```

© 2014 Cisco. All rights reserved. This document is Cisco Public.
RADIUS Timers

The communication between the NAS and the RADIUS server can be engineered with (optional) timer values. The two common timer values used in RADIUS server configurations are:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# radius-server retransmit &lt;retries&gt;</td>
<td>Specifies how many times the switch transmits each RADIUS request to the server before giving up (the default is three times).</td>
</tr>
<tr>
<td>Switch(config)# radius-server timeout &lt;seconds&gt;</td>
<td>Specifies for how many seconds a switch waits for a reply to a RADIUS request before retransmitting the request.</td>
</tr>
</tbody>
</table>

These timers determine how the AAA infra Cisco IOS subsystem within the NAS (Network Access Server; switch / wireless controller / router) will communicate with the registered clients. The 802.1X authentication manager (AuthManager) is an example of a AAA registered client. When a endpoint attempts to authenticate, the AuthManager hands over the EAP packet to the AAA infra for further RADIUS transaction. The AAA infra sends the RADIUS packet towards the server, and initiates the timeout timer. When the timer expires, and there is no response from the RADIUS server, two more attempts (a total of three) are made in five second intervals. If there is no response from the RADIUS server after the third attempt, the client is notified of the AAA unreachability. However, this does not mark the RADIUS server status as “DEAD” until a dead-criteria is configured and is met.

While a RADIUS communication happens between the switch and the RADIUS server, and if the “debug radius” command is executed, the following messages can occur:

```
Mar 30 05:18:13.909: RADIUS(00000000): Started 5 sec timeout
Mar 30 05:18:18.942: RADIUS(00000000): Started 5 sec timeout
Mar 30 05:18:23.975: RADIUS(00000000): Started 5 sec timeout
```

The retransmit retry defaults to three attempts and the default timeout period is five seconds. To change the default values, the following commands can be used:

**New Mode Commands:**

```
radius server RASERV-1
    address ipv4 172.20.254.4 auth-port 1645 acct-port 1646
    automate-tester username dummy
```
key cisco
timeout 10
retransmit 5
!

Legacy Commands:
radius-server timeout 10
radius-server retransmit 5
!

AAA Server Group Commands:
aaa group server radius RASERV
server name RASERV-1
timeout 10
retransmit 5
!

Note: When the timer values are defined under the server group (aaa group server) and under the radius server configurations (radius-server or radius server <name> commands), the radius server configuration overrides the global server group timer settings.

RADIUS Server Failure Handling

The availability and serviceability of the RADIUS server(s) is fundamental for an identity-enabled network to function. However, due to several reasons, the RADIUS server may become inaccessible to the NAS. Some of the common reasons are hardware / software failures or LAN / WAN connectivity losses. In terms of identity networking, a condition where a AAA server is unreachable is considered as a critical condition. During this condition, RADIUS authentications and authorizations cannot take place.

Some key configurations on the NAS play an important role in determining how the system will behave when the RADIUS server connectivity is lost or resumed. It’s important to understand these configurations, their default values, and how they impact the system operation during a failure.

The following commands are necessary for a deterministic behavior during a RADIUS server reachability failure:

Table 6. RADIUS Server Failure Handling Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius-server dead-criteria time &lt;seconds&gt; tries &lt;number&gt;</td>
<td>Use the radius-server dead-criteria global configuration command to configure the conditions that determine when a RADIUS server is considered unavailable or dead.                                                                                              &lt;br&gt;<strong>time seconds:</strong> (Optional) Set the time in seconds during which the switch does not need to get a valid response from the RADIUS server. The range is from one to 120 seconds.  &lt;br&gt;<strong>tries number:</strong> (Optional) Set the number of times that the switch does not get a valid response from the RADIUS server before the server is considered unavailable.</td>
</tr>
<tr>
<td>radius-server deadtime &lt;minutes&gt;</td>
<td>Defines time in minutes a server marked as DEAD will be held in that state. This command improves RADIUS response times when some servers might be unavailable, and causes the unavailable servers to be skipped immediately.                                                                                                                   &lt;br&gt;Once the deadtime expires, the switch marks the server as UP (ALIVE) and notifies the registered clients about the state change. If the server is still unreachable after the state is marked as UP and if the DEAD criteria is met, then server is marked as DEAD again for the deadtime interval.</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>automate-tester (under &quot;radius server &lt;name&gt;&quot; command)</td>
<td>To enable the automated testing feature for the RADIUS server, use the automate-tester command in RADIUS server configuration mode. With this practice, the switch sends periodic test authentication messages to the RADIUS server. It looks for a RADIUS response from the server. A success message is not necessary - a failed authentication will suffice, because it shows that the server is alive.</td>
</tr>
</tbody>
</table>

    automate-tester username user [ ignore-auth-port ] [ ignore-acct-port ] [ idle-time minutes ]

    username user: Specifies the automatic test user ID username
    ignore-auth-port: (Optional) Disables testing on the User Datagram Protocol (UDP) port for the RADIUS authentication server.
    ignore-acct-port: (Optional) Disables testing on the UDP port for the RADIUS accounting server.

**Legacy Command:**

    radius-server host {hostname | ip-address} [test username user-name]

**Example Configuration:**

```plaintext
radius-server dead-criteria time 15 tries 3
radius-server deadtime 10
!
radius server RASERV-1
    address ipv4 172.20.254.4 auth-port 1813 acct-port 1814
    automate-tester username dummy
    key cisco
!
radius server RASERV-2
    address ipv4 172.20.254.8 auth-port 1645 acct-port 1646
    automate-tester username dummy
    key cisco
!
```

The configuration can be validated by the “show aaa dead-criteria” and “show radius server-group” exec commands:

```plaintext
Switch#show aaa dead-criteria radius RASERV-1 RASERV
RADIUS Server Dead Criteria:
===================================
Server Details:
    Address   : 172.20.254.4
    Auth Port : 1645
    Acct Port : 1646
Server Group : ise
Dead Criteria Details:
    Configured Retransmits : 3
    Configured Timeout     : 5
    Estimated Outstanding Access Transactions: 0
    Estimated Outstanding Accounting Transactions: 0
```
Dead Detect Time        : 15s
Computed Retransmit Tries: 3

Statistics Gathered Since Last Successful Transaction
============================================================================================================
  Max Computed Outstanding Transactions: 0
  Max Computed Dead Detect Time: 0s
  Max Computed Retransmits : 0

! The same command can be executed for RASERV-2 aswell.

Switch#show radius server-group RASERV
Server group RASERV
  Sharecount = 1  sg_unconfigured = FALSE
  Type = standard  Memlocks = 1
  Server(172.20.254.4:1645,1646) Transactions:
    Authen: 0   Author: 0       Acct: 0
    Server_auto_test_enabled: TRUE
    Keywrap enabled: FALSE
  Server(172.20.254.8:1645,1646) Transactions:
    Authen: 0   Author: 0       Acct: 0
    Server_auto_test_enabled: TRUE
    Keywrap enabled: FALSE
When the RADIUS server becomes unreachable from the NAS, the NAS doesn’t disturb the RADIUS server state (UP/DEAD) until a new RADIUS request is originated. The new RADIUS server request can be triggered in multiple ways, some of the common triggers are, an endpoint trying to authenticate, “idle-time” expiry of the automate-tester (test username) configuration, or if the admin manually types in the “test aaa group radius” exec command. When a new RADIUS request is made while the server is unreachable, then the NAS marks it as “DEAD”, if the dead criteria(s) are met. Once a server is marked DEAD, the dead timer (configured by radius-server dead time) initiates, and if there is an endpoint trying to authenticate, then it is authorized in to critical VLAN (configurable with the “authentication event server dead action authorize vlan x” interface config command).

The NAS attempts to transition a RADIUS server status from DEAD to UP in the following conditions:

- **Deadtime Expiry**: When the dead time expires, the NAS marks the server as UP, and notifies the authentication manager about the state change. The Auth-Manager will try to clear the critical authentication session and attempt to re-authenticate the client(s) if they were authorized, in to critical VLAN. During reauthentication the NAS tries to reach the RADIUS server, if the server responds, the client is authorized as per the server policy, if not, the dead criteria will be met, the server state is marked “DEAD” again, and the endpoint will be authorized for critical VLAN.

- **Automate-tester idle-time Expiry**: The other trigger to force NAS to attempt for a RADIUS server state change is when the automate-tester (test username) idle-time expires. The default time is 60 minutes. When the idle time expires, then the NAS tries to authenticate with the RADIUS server, with the configured username. If the server responds, the server state is marked UP, if not, the “DEAD” state will continue.

- **New Authentication Request**: This is similar to the previous case, except that the authentication requests are either initiated from a connected endpoint, or by the admin probing the server by the “test aaa group radius” exec command. If the request is from the endpoint, it could be an 802.1X authentication request, such that the RADIUS transaction has to be made by the NAS.

**Note**: If dead-criteria and deadtime is not user defined on the NAS, then the system will behave in a nondeterministic manor. The default dead-criteria is 10 tries and a 10 second wait time. The server will toggle between the DEAD and UP statuses when the server goes unreachable. Even when the server is not reachable, the system throws up syslog messages that state that the “previously DEAD server is now responding”. This is due to the fact that the default deadtime is “0” seconds and the system unconditionally marks the server state to “UP” on dead time expiry.

**Automate-tester Probe-on**

When the RADIUS server is marked “DEAD” the “automate-tester username <username>” radius server configuration command helps in proactive detection of the server reachability. The default behavior of this command is such that the probes are sent out after “idle-time” expiry, even when the server is marked “UP”. This behavior is instrumental in detecting the server status, without the need for an endpoint activity. In larger enterprises, there can be several NAS (switches and wireless controllers), and if they are configured for the automate-tester, then there will be multiple periodic RADIUS transactions apart from the regular endpoint related authentication, authorization and accounting activities.
From Cisco IOS 15.2(2)E / XE 03.04.00E, there is a new item introduced to this feature; the “probe-on” keyword.

The use of this additional key word in the automate-tester command ensures that:

- The probes are sent out only when the RADIUS server is marked DEAD
- A DEAD server will be marked “UP” only when a response is received from the RADIUS server. This is unlike the behavior with the current software versions, where the RADIUS server status is marked “UP” unconditionally after the deadtime expiry.

Configuration:

```
!  
radius server RASERV-1  
  address ipv4 172.20.254.4 auth-port 1813 acct-port 1814  
  automate-tester username dummy probe-on  
  key cisco  
!  
```

RADIUS Server Load Balancing

It’s a common practice to have more than one RADIUS server in an enterprise identity deployment. It mainly serves two purposes (1) helps in handling authentications and authorizations during a server failure and (2) ensures that the server resources are not overwhelmed due to heavy transactions.

Typical recommendation for large enterprises is to have a RADIUS infrastructure setup in a manor that all of the RADIUS servers refer to a common identity store, (Microsoft Active Directory or an LDAP identity store) and have identical AAA policies on them.

RADIUS Server Redundancy

When multiple RADIUS servers are defined on a NAS, without additional load-balancing related configuration, then the servers will accessed in a fail-over mechanism. Which means that when a preferred RADIUS server is marked “DEAD”, only then an alternate RADIUS server is tried. When there are no RADIUS servers to try, the next method (such as “local” method) as defined by the method-list, will be attempted.
The configuration for this requirement is identical to the method-list configuration example given under the AAA method-list section.

Reordering the Server Preference

When there are multiple RADIUS servers defined on the NAS, the default behavior is that the non-dead 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 non-dead server in the list is thereafter tried in turn. The DEAD servers are anyways skipped.

There can be two reasons to change this default preference order:

1. There can be instances where certain server(s) that are on the top of the list are busy, and are not responding to the RADIUS requests in a timely manner.
2. A server on the top of the list is toggling between DEAD and UP statuses frequently.

To change the RADIUS server preference order on the NAS, the following commands can be used:

**Table 7. Reordering RADIUS Server Preference Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>radius-server retry method reorder</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>radius-server transaction max-tries</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Note:** There are three retry timers that can be defined by the global commands: “`radius-server retransmit <retries>``”, “`radius-server transmission max-tries <retries>`” and the “`radius-server dead-criteria tries <tries>`”. These three timers have unique functionality and complement each other in handling the RADIUS server status and preferential order. The “retransmit tries” determines the number of attempts the NAS uses per RADIUS transaction during no response from a RADIUS server, Upon exhausting all the attempts, the client process is informed about the timeout, the client process (e.g. AuthManager) may retry multiple times. Each time the same server will be queried. Upon exhausting the maximum “transmission tries” (with retry method reorder), the next server in the list is preferred, and is attempted for a transaction. While this happens, the first RADIUS server status need not necessarily be marked DEAD. The “dead-criteria tries” determines how many number of consecutive transaction failures for a given server, when unreachable, can be considered as down and be marked “DEAD”. 
The recommendation is to have “retransmit tries” < “transmission tries” < “dead-criteria tries”. This configuration ensures that a busy server is neither marked DEAD falsely, nor preferred for every transaction.

The RADIUS server preference is an internal marking that the Cisco IOS software performs to handle RADIUS requests; it cannot be viewed with any show commands. “debug radius” and “debug aaa sg-server-selection” exec command can be used to see the server being used for a specific RADIUS transaction.

RADIUS Server Load Balancing on Batch Size

The RADIUS servers can be defined on the NAS to do load balancing with redundancy. To enable load balancing on the NAS, the “radius-server load-balance method least-outstanding” command must be used. 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 of 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. If there are 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

Load balancing can be configured 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.

The ignore-preferred-server keyword may be used if either of the following configurations exist:

- Dedicated authentication server and a separate dedicated accounting server
- Network where all call record statistics and call record details can be tracked, including start- and stop-records, and those records are stored on separate servers.

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

Configuration Example: RADIUS Server load-balancing:

```
radius-server load-balance method least-outstanding
! If preferred-server needs to be ignored then:
radius-server load-balance method least-outstanding ignore-preferred-server
!
! load-balance configuration under server-group:
!
aaa group server radius RASERV
  server name RASERV-1
  server name RASERV-2
  load-balance method least-outstanding
!```
RADIUS Change of Authorization

The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an Authentication, Authorization, and Accounting (AAA) session after it is authenticated. When a policy changes for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server to reinitialize authentication and apply the new policy.

A standard RADIUS interface is typically used in a pulled model, in which the request originates from a device attached to a network, and the response is sent from the queried servers. Cisco software supports the RADIUS CoA request defined in RFC 5176 that is used in a pushed model, and enables the dynamic reconfiguring of sessions from external AAA or policy servers.

The following are some of the CoA request commands from the RADIUS server:

- Session reauthentication
- Session termination
- Session termination with port shutdown
- Session termination with port bounce
- Session Query

In response to a CoA request from the RADIUS server, the NAS can respond with either a CoA Acknowledgement [CoA-ACK] or a CoA Non-Acknowledgement [CoA-NAK] messages.

Configuring NAS for RADIUS CoA

To configure the NAS to accept CoA commands from a valid RADIUS server, and to be able to respond to the requests, apart from the other AAA and RADIUS server configurations, the following configuration is necessary:

```bash
aaa server radius dynamic-author
    client 172.20.254.4 server-key cisco
    server-key cisco
```

RADIUS Change of Authorization (CoA)
Session Identification

For disconnect and CoA requests targeted at a particular session, the device locates the session based on one or more of the following attributes:

- Acct-Session-Id (IETF attribute #44)
- Audit-Session-Id (Cisco VSA)
- Calling-Station-Id (IETF attribute #31, which contains the host MAC address)
- IPv6 Attributes, which can be one of the following:
  - Framed-IPv6-Prefix (IETF attribute #97) and Framed-Interface-Id (IETF attribute #96), which together create a full IPv6 address per RFC 3162
  - Framed-IPv6-Address
- Plain IP Address (IETF attribute #8)

If more than one session identification attribute is included in the message, all of the attributes must match the session, or the device returns a Disconnect-NAK or CoA-NAK with the error code "Invalid Attribute Value." For CoA requests targeted at a particular enforcement policy, the device returns a CoA-NAK with the error code "Invalid Attribute Value" if any of the above session identification attributes are included in the message.

For More Information

Visit the following URLs:

- [http://www.cisco.com/go/ibns](http://www.cisco.com/go/ibns)
- [http://www.cisco.com/go/trustsec](http://www.cisco.com/go/trustsec)