

RADIUS Server State

- Revision History, on page 1
- Feature Description, on page 1
- How it Works, on page 1
- Configuring AAA RADIUS Servers , on page 2
- Monitoring and Troubleshooting, on page 2

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
The feature is available in 21.25 and later releases.	21.25
First introduced.	Pre 21.24

Feature Description

This feature enables the RADIUS server to indicate the appropriate state regardless of the timing of keep-alive transmissions.

How it Works

When the AAA RADIUS servers are configured, the Authentication server state is set to “INIT”. In "INIT" state, the server is initialized with the context-specific configuration and prepared to send the Access request. Once the Access request is sent, the server state is moved to “Active Pending”. After receiving positive response on the SRP Active chassis, the server state is moved to “ACTIVE”. Meanwhile, after configuring the Accounting server, the state is set as "Active" on both chassis.

To implement this feature, the server states are updated at the time of initial configuration and during Interchassis Session Recovery (ICSR) switchover on SRP Standby Chassis. Initially on standby chassis,

servers are kept in “Active Pending” state, as the RADIUS servers are being initialized with the context-specific configuration. After the configuration completion, Access-request is sent for the Authentication server, and accounting request is sent for the accounting server as a significance of keep-alive messages. But, no response is received for these keep-alive messages because of the standby chassis. So, after the keep-alive timeout, the server state is automatically changed to “Down”.

In ICSR switchover scenario, when SRP messages are received on the Active chassis, which is going to be a new Standby chassis, the state of the servers are changed to “Active Pending”. As per the state flow, keep-alive messages are sent towards the RADIUS servers, and like the previous scenario, no response is received from the RADIUS servers. So, after the keep-alive timeouts, the server state is automatically changed to “Down”.

Configuring AAA RADIUS Servers

There is no specific configuration required for this feature. When you configure any RADIUS accounting server, it displays the appropriate state according to the chassis state.

The following is a sample configuration for configuring the AAA RADIUS servers:

```
config
 context ISP1
  apn intershat
  mediation-device context-name ISP1
  exit
 exit
exit
config
 context ISP1
  aaa group default
   radius attribute nas-ip-address address 209.165.200.225
   radius accounting interim interval 60
   radius mediation-device accounting server 209.165.200.226 key secret port 1813
   radius keepalive timeout 4
   radius keepalive retries 3
   radius keepalive interval 30
   radius accounting algorithm round-robin
   radius accounting detect-dead-server keepalive
   radius accounting keepalive timeout 4
   radius accounting keepalive username 001001110990001@pgw.keepalive
   radius accounting keepalive calling-station-id 999255255255005
   radius accounting keepalive framed-ip-address 255.255.255.224
   radius max-retries 0
   radius accounting max-retries 0
   radius max-transmissions 2
   radius accounting max-transmissions 2
   radius timeout 1
   radius accounting timeout 15
   no radius accounting archive
   exit
  exit
 exit
exit
```

Monitoring and Troubleshooting

This section describes the CLI commands available to monitor and/or troubleshoot the feature.

Show Commands and Outputs

show radius accounting servers detail

Use this CLI command to display the RADIUS Accounting server details configured in a particular context.

show radius authentication servers detail

Use this CLI command to display the RADIUS Authentication server details configured in a particular context.