

Radius Packet Disconnect

- Revision History, on page 1
- Feature Description, on page 1
- High Level Requirements, on page 1
- Change-of-Authorization Messages, on page 2
- Message Exchange, on page 2
- RADIUS-Initiated Disconnect Messages, on page 2
- Message Exchange, on page 3
- Configuring Radius Change Authorization NAS-IP-Address Functionality, on page 3

Revision History

Revision Details	Release
First introduced	21.26

Feature Description

The RADIUS change of authorization provides a mechanism to change authorization dynamically after the device is authenticated. Once there is a policy change, you can send RADIUS CoA packets from the authorization server to reinitiate authentication and apply the new policy. The RADIUS CoA process allows you to change the user access immediately when needed, without the need to wait for the wired switch or access point to initiate a re-authentication process, or for the device to disconnect and re-connect again.

It is now possible to define more than one radius Change of Authorization (CoA) NAS IP address per context in a context with multiple APNs using different RADIUS servers and different NAS IP addresses.

High Level Requirements

The following table provides the high level requirements for the existing architecture:

Module	Requirements
CLI	You must be able to configure multiple Radius COA NAS-IP-Address in a single context.
SCTRL	You must be able to configure multiple Radius CoA NAS-IP-Address in a single context. These multiple Radius CoA NAS-IP-Address must be broadcasted by SCTRL to all the AAAMGR instances.
AAAMGR	Change the AAAMGR configuration to allow the opening of multiple NAS-IP-Address sockets inside a context. AAAMGR must be able to receive CoA or DM messages on different NAS-IP-Address inside the same context.

Change-of-Authorization Messages

The RADIUS dynamic-request server receives and processes the unsolicited Change-of-Authorization (CoA) messages from RADIUS servers. The RADIUS-initiated CoA feature uses the following codes in its RADIUS request and response messages:

- CoA-Request (43)
- CoA-ACK (44)
- CoA-NAK (45)

Message Exchange

The RADIUS server and the router's RADIUS dynamic-request server exchange messages using UDP. The COA-Request message sent by the RADIUS server has the same format as the Disconnect-Request packet that is sent for a disconnect operation.

The response is either a COA-ACK or a COA-NAK message:

- If AAA successfully changes the authorization, the response is a RADIUS-formatted packet with a COA-ACK message, and the data filter is applied to the session.
- If AAA is unsuccessful, the request is malformed, or attributes are missing, the response is a RADIUS-formatted packet with a COA-NAK message.

RADIUS-Initiated Disconnect Messages

This section describes the RADIUS dynamic-request server's RADIUS-initiated disconnect feature.

To centrally control the disconnection of remote access users, the RADIUS dynamic-request server on the router must receive and process unsolicited messages from RADIUS servers.

The RADIUS-initiated disconnect feature uses the existing format of RADIUS disconnect request and response messages. The RADIUS-initiated disconnect feature uses the following codes in its RADIUS request and response messages:

- Disconnect-Request (40)
- Disconnect-ACK (41)
- Disconnect-NAK (42)

Message Exchange

The RADIUS server and the router's RADIUS dynamic-request server exchange messages using User Datagram Protocol (UDP). The Disconnect-Request message sent by the RADIUS server has the same format as the COA-Request packet that is sent for a change of authorization operation.

The disconnect response is either a Disconnect-ACK or a Disconnect-NAK message:

- If AAA successfully disconnects the user, the response is a RADIUS-formatted packet with a Disconnect-ACK message.
- If AAA cannot disconnect the user, the request is malformed, or attributes are missing from the request, the response is a RADIUS-formatted packet with a Disconnect-NAK message.

Configuring Radius Change Authorization NAS-IP-Address Functionality

The following CLI configures the CP to receive CoA messages from the Radius server and returns an acknowledgment to the server.

```
configure
       context context_name
          radius change-authorize-nas-ip ip_address
             [ encrypted ] key secret
             { port port }
             { no-reverse-path-forward-check }
             { timestamp-window <0-4294967295>}
          exit
    exit
```

Allow multiple rows of the **radius change-authorize-nas-ip** CLI command within certain context. You can configure a maximum of 32 such rows within certain context.

Show Commands and Outputs

This section provides information about the show CLI commands available in support of the feature. Run the show command within certain context.

- **show radius counters**
- **show radius info instance**
- **show session subsystem facility aaamgr instance**