



# RADIUS Authentication and Accounting

- [Feature Summary and Revision History, on page 1](#)
- [Feature Description, on page 2](#)
- [How it Works, on page 8](#)
- [Configuring the RADIUS Client, on page 26](#)
- [RADIUS Client OA&M Support, on page 46](#)
- [Troubleshooting Information, on page 46](#)

## Feature Summary and Revision History

### Summary Data

**Table 1: Summary Data**

|                                          |                                   |
|------------------------------------------|-----------------------------------|
| Applicable Product(s) or Functional Area | SMF                               |
| Applicable Platform(s)                   | SMI                               |
| Feature Default Setting                  | Disabled – Configuration Required |
| Related Changes in this Release          | Not Applicable                    |
| Related Documentation                    | Not Applicable                    |

### Revision History

**Table 2: Revision History**

| Revision Details                                                          | Release   |
|---------------------------------------------------------------------------|-----------|
| Added dynamic configuration change support for the RADIUS endpoint.       | 2023.03.0 |
| Added the Secure Group Tag support for RADIUS access response attributes. | 2023.01.4 |

| Revision Details                                                                                                                                                                                                                                                                                                                                                                            | Release        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| Added the support for: <ul style="list-style-type: none"> <li>• 3GPP dictionary</li> <li>• Allow-auth</li> <li>• Consecutive failure</li> <li>• Max-transmissions</li> </ul>                                                                                                                                                                                                                | 2023.03.0      |
| Added support for interworking with ISE.                                                                                                                                                                                                                                                                                                                                                    | 2021.02.2.t1.0 |
| Introduced new CLI option in charging profile to generate the RADIUS accounting trigger on TFT change.                                                                                                                                                                                                                                                                                      | 2021.02.0      |
| To support instance awareness on RADIUS, the SMF allows: <ul style="list-style-type: none"> <li>• Instance-level configuration under RADIUS profile</li> <li>• NAS-IP-Address and NAS-Identifier attribute configuration per instance-id in RADIUS profile configuration</li> <li>• RADIUS Disconnect-Request VIP configuration per instance-id in RADIUS endpoint configuration</li> </ul> | 2021.02.0      |
| Added support for the following: <ul style="list-style-type: none"> <li>• PAP, CHAP, and MSCHAP-based RADIUS authentication</li> <li>• Multiple RADIUS NAS-IP source addresses</li> <li>• Handling RADIUS Disconnect and CoA Requests</li> <li>• RADIUS Accounting on SMF</li> <li>• New attributes in the RADIUS Access Response message</li> </ul>                                        | 2020.02.5.t1   |
| First introduced.                                                                                                                                                                                                                                                                                                                                                                           | Pre-2020.02.0  |

## Feature Description

Remote Authentication Dial-In User Service (RADIUS) is a client and server protocol. The RADIUS client is typically a Network Access Server (NAS) and the RADIUS server is usually a daemon process running on a UNIX or Windows NT machine. The client passes user information to designated RADIUS servers and acts

on the response that is returned. RADIUS servers receive user connection requests, authenticate the user, and then return the configuration information necessary for the client to deliver service to the user.

RADIUS provides Authentication and Accounting services to the users. The SMF supports the following configurations:

- Add RADIUS server details.
- Enable RADIUS accounting and authentication.
- Add RADIUS interface as an option for virtual APN configuration within DNN profile.
- Enable CC trigger reporting.
- Define volume and time limits.

The RADIUS client supports the following functions:

- **Server Selection**

RADIUS servers are configured with IP: Port as the key. The **algorithm** CLI specifies the failover or load-balancing algorithm to select the RADIUS server to which the authentication or accounting request must be sent. Servers that are marked "dead" aren't considered for selection until they are marked "alive". The supported algorithms are first-server and round-robin.

- **First-server**—Specifies that the request must be sent to the RADIUS server with the highest priority. If the server becomes unreachable, the request is sent to the server with the next highest configured priority. This is the default algorithm.
- **Round-robin**—Specifies that the request must be sent based on load balancing in a circular queue manner. The server that is last used is stored to maintain the round-robin selection. The order of the list is purely based on the configuration sequence.

- **Monitor Server and Dead Server Detection**

The Dead-Server Detection feature allows you to configure the criteria to be used to mark a RADIUS server as dead. The two different parameters that you can set up to identify a dead server are as follows.

- **Response-timeout**: Monitor Server revisits the server database and marks the server which hasn't received response beyond the configured "response-timeout" value after the first request is sent. The server is marked "dead" and remains in dead-state for minutes configured as "deadtime". After the "deadtime" elapses, the server's dead-variable is reset again to mark it as ready to process requests. If the server is still not reachable, it's marked "dead" as part of the next request response timeout.
- **Consecutive failures**: Consecutive failure helps to configure the number of consecutive timeouts that must occur on the server before the RADIUS server is marked as dead. Whether a request is a retry request or a regular request, the failure count increments when server doesn't return any response (i.e request timeout). When the failure count of the server reaches the threshold for consecutive failures, the server is declared as dead server.

- **Timeout and Retry**

After a server is selected and a request is sent to the server, an entry is maintained in the request queue until response is received from the RADIUS server or until timeout occurs. Monitor Requests is called to check on the requests queue for response timeouts and retry. It walks through all the entries and checks if any request timeout value configured as "timeout" is hit. For such requests, if the number of retries is less than the configured "max-retries" value, the request is resent to the RADIUS server. Else, if the

"max-retries" count is reached, the request is deleted from the request queue. After a request is deleted, even if response comes for such requests, the response is discarded and not sent to the user.

- **Max transmission**

Max transmission helps to configure the transmission parameters for all the available servers. This feature helps to cross-check if the number of transmissions exceeds the number of retries once the retry cycle for a request is finished, and if so, it begins the subsequent retry cycle on a different server if one is available. If no server is available, or if the maxtransmissions limit is reached, then the timeout response is sent.

**Example:** If max-transmissions value is set to 5, max retry value is 2, and there are two servers available. So there are three attempts (one actual attempt and two retries) on the first server, and the remaining 2 (1 actual and one retry) on the second server.

## RADIUS Authentication

Authentication and key management are fundamental to the security of mobile networks because they provide mutual authentication between users and the network.

5G defines various authentication methods to authenticate a user. In the 5G architecture, the serving network authenticates the Subscription Permanent Identifier (SUPI), and key agreement between the UE and the network using the primary authentication mechanism.

For information on enabling the RADIUS Client feature, see [Configuring the RADIUS Client, on page 26](#).

### Identity Services Engine

Identity Services Engine (ISE) is a common point of policy definition for 5G and other enterprise devices. In 5G as a Service (5GaaS) architecture, ISE conducts only the authorization and accounting. The Control Center handles the 5G authentication. You can implement the 5G authorization with the RADIUS Authorize-Only flow.

SMF supports communication with ISE for Cisco private 5G. Based on the policies that SMF receives from ISE, Cisco private 5G supports various behaviors on the enterprise side. ISE provides a mechanism for the enterprise customers to perform tasks, such as identifying the subscriber, define groups for the subscribers, and assign policy.

### Allow-auth

If allow-auth is enabled in the configuration, it allows the ongoing call to continue irrespective of authentication being successful, timed out, or any error message received. The default value is false, configuration is required to enable the allow-auth.

## Throughput Limiting

If you have configured a secondary authentication on the SMF, then the SMF sends the RADIUS access request to ISE based on the configured RADIUS server address. SMF includes PEI in the access request, if available. The configured IMEI-based ISE includes the name of the rule that is to be applied on the private 5G network to achieve the throughput limiting.



**Note** Throughput limiting can use either IMEI or IMSI.

ISE populates the rule name in the 3GPP-Policy-Reference attribute in the access accept request. You can configure this rulebase in SMF. SMF derives the ASCII value from the octet string included in the 3GPP-Policy-Reference attribute. Then, SMF matches this value with the configured rulebase.

Following table lists the octet values for the 3GPP-Policy-Reference AVP.

**Table 3: 3GPP-Policy-Reference AVP**

|        | Bits                                                                                                                                                                            |   |   |   |   |   |   |   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---|---|---|---|
| Octets | 8                                                                                                                                                                               | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 1      | 3GPP Type = 113                                                                                                                                                                 |   |   |   |   |   |   |   |
| 2      | 3GPP Length = m                                                                                                                                                                 |   |   |   |   |   |   |   |
| 3-m    | Policy Data Reference (octet string)<br><br><b>Note</b><br>DN AAA sends the policy data reference value. SMF uses this value to retrieve the SM and QoS policy data in the PCF. |   |   |   |   |   |   |   |

The ISE sends the rulebase to SMF. If the SMF receives the rulebase that is not configured, then the SMF ignores it. If you have not configured the default bandwidth policy on SMF, then the bandwidth policy is ignored.

You can configure the bandwidth limit on SMF when a UE attaches through the 4G RAT or 5G RAT. Based on the bandwidth limit configured through the 4G RAT, the SMF populates the BearerQoS value in the Create Session response. Based on the bandwidth limit configured through the 5G RAT, the SMF populates the QosFlowDescription value in the N1 PDU Establishment Accept request.

Bandwidth limiting is configured locally on UPF based on the predefined rule that SMF sends.

## RADIUS Accounting

Accounting collects and sends subscriber usage and access information used for billing, auditing, and reporting. For example, user identities the start and stop times, performed actions, number of packets, and number of bytes. Accounting enables an operator to analyze the services that the users access and the amount of network resources they consume. Accounting records comprise accounting Attribute Value Pairs (AVPs) and are stored on the accounting server. This accounting information can then be analyzed for network management, client billing, and/or auditing.

The SMF implements the RADIUS Accounting functionality through the use of CLI configuration. For more details on the configuration, see [Configuring the RADIUS Client, on page 26](#).

If the RADIUS accounting is enabled and server-group is configured within the DNN profile, the SMF sends server-group as AAA group in charging-params in N4 session establishment request. When the SMF sends AAA group which is not present on UPF, then it does not account the traffic for static and predefined rules in RADIUS URR and fails to report. In this scenario, the SMF considers only the dynamic rules traffic for accounting in the RADIUS URR.

## Handling RADIUS Disconnect Request Messages

Dynamic Authorization Client (DAC) sends Disconnect-Request packet to RADIUS endpoint (radius-ep) through UDP port. DAC sends this packet to terminate the user session(s) on Network Access Server (NAS). It also discards all the associated session contexts.

The Disconnect-Request packet contains the following session identification attributes to identify the sessions to be terminated.

- 3GPP-IMSI + 3GPP-NSAPI
- ACCT-SESSION-ID
- CALLED-STATION-ID (DNN) + FRAMED-IP-ADDR
- CALLED-STATION-ID (DNN) + FRAMED-IPV6-PREFIX

The RADIUS endpoint validates the Disconnect-Request packet. If the validation fails, the endpoint rejects the packet and sends Disconnect-NAK message with appropriate cause code to DAC. If the validation is successful, the endpoint performs affinity lookup based on the session identification keys or attributes. Then, the endpoint forwards the Disconnect-Request packet to the particular SMF service instance. The SMF processes the packet and triggers pdu-release or pdn-disconnect procedure. The SMF sends the Disconnect ACK response with the appropriate cause code if the session is identified, removed, and no longer valid. The SMF sends a Disconnect-NAK message with appropriate cause code if the session context is not found. The SMF does not wait for the completion of release procedure to send the Disconnect ACK or NAK response.

In the roaming scenario, the RADIUS Disconnect-Request is supported for home-routed subscribers when the roaming status is roamer. The hSMF acts as the SMF service and initiates the session release procedure.



**Note** Roaming with 4G and EpsInterworkingIndication is not supported. Hence, a combination of IMSI and NSAPI keys is not supported.

This feature uses a combination of the session identification keys or attributes to identify the sessions for termination.



**Important** If multiple key combination is provided for the same session, it is accepted. However, if the multiple key combination leads to multiple session contexts or non-existing session context, the behavior is non-deterministic.

The SMF supports only one session context per Disconnect-Message (DM) request. The SMF supports the following attributes in the DM request to identify the NAS and the user sessions to be terminated.

| Attribute             | Reference Specification                         | Encoding Type |
|-----------------------|-------------------------------------------------|---------------|
| 3GPP-IMSI             | 3GPP 29.061 - 16.4.7.2-1                        | String        |
| 3GPP-NSAPI            | 3GPP 29.061 - 16.4.7.2-10<br>3GPP 29.561 - 11.3 | String        |
| Accounting-Session-Id | RFC 2866                                        | String        |
| FRAMED-IP             | RFC 2865 - 5.1                                  | IPv4 Address  |

| Attribute               | Reference Specification    | Encoding Type        |
|-------------------------|----------------------------|----------------------|
| FRAMED-IPV6-PREFIX      | RFC 3162                   | PrefixLen and String |
| CALLED-STATION-ID (DNN) | RFC 2865 - 5.30            | String               |
| NAS-IP-Address          | RFC 2865 – 5.4 (optional)  | String               |
| NAS-Identifier          | RFC 2864 – 5.32 (optional) | String               |

The SMF silently discards other attributes present in the DM request if the packet decoding is successful.

The SMF supports the following attributes in the DM ACK or NAK response.

| Attribute     | Reference Specification | Encoding Type |
|---------------|-------------------------|---------------|
| ERROR-CAUSE   | RFC 5176 – 3.5          | Integer       |
| REPLY-MESSAGE | RFC 2865 – 5.18         | String        |

The RADIUS endpoint pod supports the following error codes if the Disconnect Request is rejected by radius-ep:

- 402 (Missing Attribute) - Triggered due to invalid key combination
- 403 (NAS Identification Mismatch) - Triggered if NAS-IP attribute in DM request does not match the endpoint COA-NAS VIP-IP or if NAS-Identifier attribute in the request does NAS identifier configuration within RADIUS Dynamic Authorization or CoA configuration
- 407 (Invalid Attribute) - Triggered due to format error, encode error, and so on
- 405 (Unsupported Service) - Triggered if the request is not a disconnect request
- 503 (Session Context Not Found) - Triggered if the session cannot be located

For more information on configuring this feature, see the [Configuring the Session Disconnect Feature, on page 44](#) section.

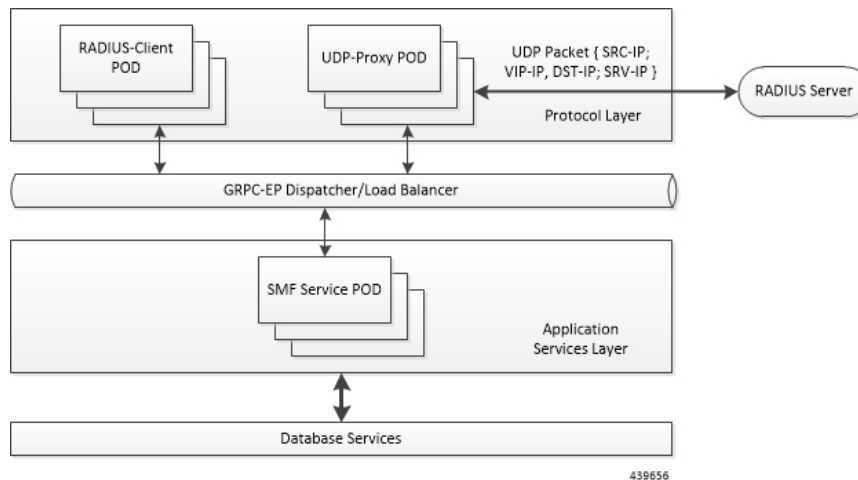
## Architecture

### RADIUS Client Integration in SMF

The RADIUS client pod resides in the protocol layer of the 5G architecture.

The following figure illustrates the integration of RADIUS Client in SMF.

Figure 1: RADIUS Client Integration



**Radius-EP App (RADIUS-Client Pod)**—The RADIUS Client functionality is added in a new pod. It handles RADIUS protocol-specific functions, such as authentication and accounting.

**SMF Service App (SMF Service Pod)**—The SMF Service App provides PDU session service. During session establishment, the SMF service decides if the secondary authentication is required or not, and acts accordingly.

**UDP-Proxy App (UDP-Proxy Pod)**—The UDP-Proxy App is enabled with host-networking and, communicates the packets using external Virtual-IPs. All RADIUS packets are transmitted and received from an outside cluster using this application.

## How it Works

This section describes how the SMF supports RADIUS authentication and accounting functionality.

### RADIUS Interaction for Authentication

The RADIUS server supports various methods to authenticate the user. When the server is provided with the username and original password of the user, it can support Point-to-Point Protocol (PPP), Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), or Microsoft CHAP (MSCHAP), UNIX login, and other authentication methods.

If the secondary authentication is enabled in DNN profile, the SMF interacts with the RADIUS server to perform RADIUS authentication. To implement the authentication, the RADIUS client residing within the SMF sends the User-Name and User-Password attributes in Access-Request message to the RADIUS server.

The SMF uses more attributes to facilitate the RADIUS authentication function. For the complete list of attributes supported, see the [RADIUS Attribute Definition, on page 18](#) section.

The RADIUS server validates the user with the authentication information. If the validation is successful, the server sends the Access-Accept response to the SMF.

## RADIUS Authentication Attributes

### RADIUS Access Request Attributes

The following table lists the supported attributes in the RADIUS access request message.

| Attribute                     | Reference Specification          | Encoding Type          |
|-------------------------------|----------------------------------|------------------------|
| USER-NAME                     | RFC2865 - 5.1                    | String                 |
| PASSWORD                      | RFC2865 - 5.2                    | Encrypted String       |
| CALLING-STATION-ID            | RFC2865 - 5.31                   | String                 |
| CALLED-STATION-ID             | RFC2865 - 5.30                   | String                 |
| NAS-IP-ADDRESS                | RFC2865 - 5.4                    | IPv4 Address           |
| NAS-IDENTIFIER                | RFC2865 - 5.32                   | String                 |
| SERVICE-TYPE                  | RFC2865 - 5.6                    | Octets - 4 bytes       |
| FRAMED-PROTOCOL               | RFC2865 - 5.7                    | Octets - 4 bytes       |
| NAS-PORT-TYPE                 | RFC2865 - 5.41                   | Octets - 4 bytes       |
| NAS-PORT                      | RFC2865 - 5.5                    | Octets - 4 bytes       |
| SERVING-NETWORK-NAME          | 3GPP TS 29.561 - 16.4.0, RFC2865 | String                 |
| 3GPP-IMSI                     | 3GPP 29.061 - 16.4.7.2-1         | String                 |
| 3GPP-CHARGING-ID              | 3GPP 29.061 - 16.4.7.2-2         | Octets - 4 bytes       |
| 3GPP-PDP-TYPE                 | 3GPP 29.061 - 16.4.7.2-3         | Octets - 4 bytes       |
| 3GPP-CHARGING-GATEWAY-ADDR    | 3GPP 29.061 - 16.4.7.2-4         | IPv4 Address           |
| 3GPP-GPRS-NEG-QOS-PROFILE     | 3GPP 29.061 - 16.4.7.2-5         | Special Encoded Octets |
|                               | 3GPP 29.274 - 8.7                |                        |
| 3GPP-SGSN-ADDRESS             | 3GPP 29.061 - 16.4.7.2-6         | IPv4 Address           |
| 3GPP-GGSN-ADDRESS             | 3GPP 29.061 - 16.4.7.2-7         | IPv4 Address           |
| 3GPP-IMSI-MCC-MNC             | 3GPP 29.061 - 16.4.7.2-8         | String                 |
| 3GPP-GGSN-MCC-MNC             | 3GPP 29.061 - 16.4.7.2-9         | String                 |
| 3GPP-NSAPI                    | 3GPP 29.061 - 16.4.7.2-10        | String                 |
|                               | 3GPP 29.561 - 11.3               |                        |
| 3GPP-SELECTION-MODE           | 3GPP 29.061 - 16.4.7.2-12        | String                 |
| 3GPP-CHARGING-CHARACTERISTICS | 3GPP 29.061 - 16.4.7.2-13        | String                 |
| 3GPP-SGSN-MCC-MNC             | 3GPP 29.061 - 16.4.7.2-18        | String                 |
| 3GPP-IMEISV                   | 3GPP 29.061 - 16.4.7.2-20        | String                 |
| 3GPP-RAT-TYPE                 | 3GPP 29.061 - 16.4.7.2-21        | Octet - 1 byte         |

| Attribute            | Reference Specification                                                                      | Encoding Type          |
|----------------------|----------------------------------------------------------------------------------------------|------------------------|
| 3GPP-USER-LOCATION   | 3GPP 29.061 - 16.4.7.2-22<br>3GPP 29.274 - 8.21-4, 8.21-5<br>3GPP 38.413 – 9.3.1.7, 9.3.3.10 | Special Encoded Octets |
| 3GPP-MS-TIMEZONE     | 3GPP 29.061 - 16.4.7.2-23                                                                    | Special Encoded Octets |
|                      | 3GPP 29.274 - 8.44                                                                           |                        |
| 3GPP-NEGOTIATED-DSCP | 3GPP 29.061 - 16.4.7.2-26                                                                    | Octet - 1 byte         |
| REPLY-MESSAGE        | RFC2865 – 5.18                                                                               | String                 |



**Note** The Wi-Fi call attributes are the same as the 4G call.

### RADIUS Access Response Attributes

The following table lists the supported attributes in the RADIUS access response message.

| Attribute               | Reference Specification | Encoding Type        |
|-------------------------|-------------------------|----------------------|
| Class                   | RFC 2865                | String               |
| FRAMED-IP               | RFC2865 - 5.1           | IPv4 Address         |
| FRAMED-IPv6-PREFIX      | RFC3162                 | PrefixLen and String |
| Framed-IP-Netmask       | RFC 2865                | Octet                |
| IDLE-TIMEOUT            | RFC2865 - 5.28          | Integer              |
| 3GPP-POLICY-REFERENCE   | 3GPP TS 29.061          | Octet                |
| MS-Primary-DNS-Server   | RFC 2548                | Octet                |
| MS-Secondary-DNS-Server | RFC 2548                | Octet                |
| SN-VIRTUAL-APN-NAME     | Starent Dictionary      | Opaque               |
| SESSION-TIMEOUT         | RFC2865 - 5.27          | Integer              |
| cts:security-group-tag  | Cisco Dictionary        | Opaque               |



**Note** The Wi-Fi call attributes are the same as the 4G call.

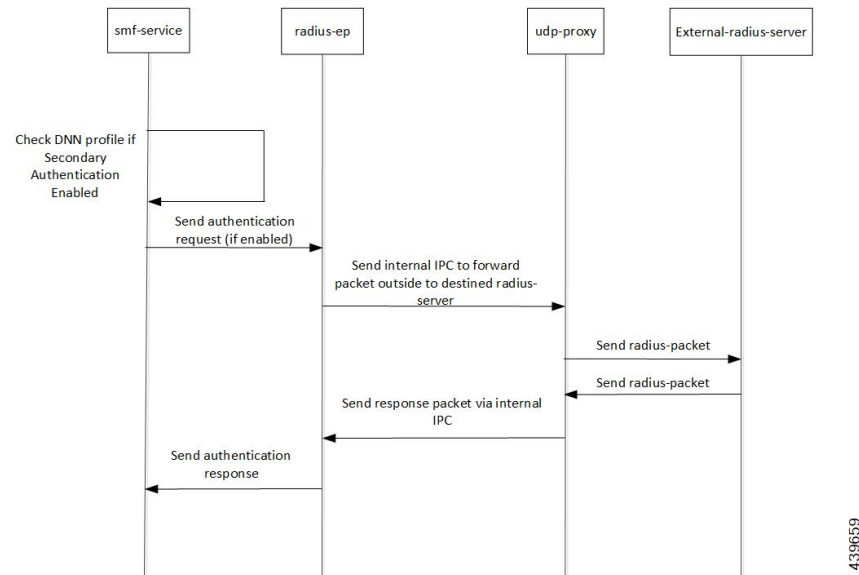
For complete description of the RADIUS authentication attributes, see the [RADIUS Attribute Definition, on page 18](#) section in this guide.

## Call Flows

### RADIUS Authentication Call Flow

The following figure illustrates the end to end call flow between the SMF server and RADIUS endpoint.

**Figure 2: RADIUS Authentication Call Flow**



**Table 4: RADIUS Authentication Call Flow Description**

| Step | Description                                                                                                                                                                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Bringing up RADIUS pod: Add the respective endpoint configuration, with VIP-IP similar to Protocol-EP VIP-IP. Add the RADIUS server information to the RADIUS profile configuration.                                                                                                                                                                                  |
| 2    | Add the secondary authentication configuration to the required DNN profiles.                                                                                                                                                                                                                                                                                          |
| 3    | During session bringup, the DNN profile checks if secondary authentication is enabled after successful UDM validation. <ul style="list-style-type: none"> <li>• If authentication is not enabled, continue with PCF.</li> <li>• If authentication is enabled, send inter-process communication (IPC) message to RADIUS pod to authenticate the subscriber.</li> </ul> |
| 4    | The RADIUS pod prepares the Access Request packet that is destined to a configured RADIUS server, sends the packet to UDP proxy pod to proxy the packet out.                                                                                                                                                                                                          |
| 6    | The UPD proxy pod creates a socket (if not already present) and sends the packet to the RADIUS server.                                                                                                                                                                                                                                                                |
| 7    | The RADIUS server validates the Access Request. If accepted, it responds with the Access Accept message. Else, it responds with the Access Reject message.                                                                                                                                                                                                            |
| 8    | The UDP proxy responds to the respective RADIUS-EP instance.                                                                                                                                                                                                                                                                                                          |

| Step | Description                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 9    | The RADIUS-EP instance validates the response, fetches the framed-IP (if present), and updates the SMF service.                               |
| 10   | The SMF service, upon successful response from RADIUS-EP, continues with the PCF flow. Else, the SMF service disconnects from the subscriber. |

## RADIUS Interaction for Accounting

The SMF exchanges the following messages with RADIUS server through the RADIUS-client RADIUS-EP.

- **Accounting-Request:** This message carries any of the following packets to relay the accounting information to the RADIUS server.

- **Accounting Start packet:** This packet describes the type of service being delivered and the user it is being delivered to.

The SMF sends accounting-start packet during the session establishment procedure. The RADIUS Accounting server returns an acknowledgement upon receiving the accounting-start packet.

For details on configuring the RADIUS Accounting, see [Configuring the RADIUS Client, on page 26](#) section.

- **Accounting Stop packet:** This packet describes the type of service that was delivered and optionally statistics, such as elapsed time, input and output octets, or input and output packets.

At the end of service delivery, the SMF sends the accounting-stop packet for all session deletion scenarios and when the RADIUS accounting is enabled during the call setup.

- **Accounting-Request Interim-Update:** During the session, the SMF sends the updated cumulative usage report to the RADIUS accounting server.

- **Accounting-Response:** For each successfully processed accounting request, the RADIUS server returns an accounting acknowledgment confirming the receipt of the information.

For CLI details associated with accounting, see the [Configuring the RADIUS Client, on page 26](#) section.

## RADIUS Accounting Attributes

The following table lists the RADIUS accounting attributes supported in the accounting request message.

| Attribute          | Reference Spec  | Encoding Type | Supported Accounting Type   |
|--------------------|-----------------|---------------|-----------------------------|
| USER-NAME          | RFC 2865 - 5.1  | String        | Start, Stop, Interim update |
| CALLING-STATION-ID | RFC 2865 - 5.31 | String        | Start, Stop, Interim update |
| CALLED-STATION-ID  | RFC 2865 - 5.30 | String        | Start, Stop, Interim update |
| Class              | RFC 2865 - 5.25 | String        | Start, Stop, Interim update |

| Attribute                  | Reference Spec                                | Encoding Type          | Supported Accounting Type                                                                             |
|----------------------------|-----------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------|
| NAS-IP-ADDRESS             | RFC 2865 - 5.4                                | IPV4 Address           | Start, Stop, Interim update                                                                           |
| NAS-IDENTIFIER             | RFC 2865 - 5.32                               | String                 | Start, Stop, Interim update                                                                           |
| SERVICE-TYPE               | RFC 2865 - 5.6                                | Octets - 4 bytes       | Start, Stop, Interim update                                                                           |
| FRAMED-PROTOCOL            | RFC 2865 - 5.7                                | Octets - 4 bytes       | Start, Stop, Interim update                                                                           |
| FRAMED-IP                  | RFC2865 - 5.1                                 | IPv4 Address           | Start, Stop, Interim update                                                                           |
| FRAMED-IPv6-PREFIX         | RFC3162                                       | PrefixLen and String   | Start, Stop, Interim update                                                                           |
| Framed-IP-Netmask          | RFC 2865 - 5.9                                | Octets - 4 bytes       | Start, Stop, Interim update                                                                           |
| NAS-PORT-TYPE              | RFC 2865 - 5.41                               | Octets - 4 bytes       | Start, Stop, Interim update                                                                           |
| NAS-PORT                   | RFC 2865 - 5.5                                | Octets - 4 bytes       | Start, Stop, Interim update                                                                           |
| 3GPP-IMSI                  | 3GPP 29.061 - 16.4.7.2-1                      | String                 | Start, Stop, Interim update                                                                           |
| 3GPP-CHARGING-ID           | 3GPP 29.061 - 16.4.7.2-2                      | Octets - 4 bytes       | Start, Stop, Interim update                                                                           |
| 3GPP-PDP-TYPE              | 3GPP 29.061 - 16.4.7.2-3                      | Octets - 4 bytes       | Start, Stop, Interim update                                                                           |
| 3GPP-CHARGING-GATEWAY-ADDR | 3GPP 29.061 - 16.4.7.2-4                      | IPV4 Address           | Start, Stop, Interim update                                                                           |
| 3GPP-GPRS-NEG-QOS-PROFILE  | 3GPP 29.061 - 16.4.7.2-5<br>3GPP 29.274 - 8.7 | Special Encoded Octets | Start, Stop, Interim update                                                                           |
| 3GPP-SGSN-ADDRESS          | 3GPP 29.061 - 16.4.7.2-6                      | IPV4 Address           | Start, Stop, Interim update<br><br>This attribute is not included in the 5G accounting-start message. |
| 3GPP-GGSN-ADDRESS          | 3GPP 29.061 - 16.4.7.2-7                      | IPV4 Address           | Start, Stop, Interim update                                                                           |

| Attribute                     | Reference Spec                                                            | Encoding Type          | Supported Accounting Type                                                                                  |
|-------------------------------|---------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------|
| 3GPP-IMSI-MCC-MNC             | 3GPP 29.061 - 16.4.7.2-8                                                  | String                 | Start, Stop, Interim update                                                                                |
| 3GPP-GGSN-MCC-MNC             | 3GPP 29.061 - 16.4.7.2-9                                                  | String                 | Start, Stop, Interim update                                                                                |
| 3GPP-NSAPI                    | 3GPP 29.061 - 16.4.7.2-10                                                 | String                 | Start, Stop, Interim update                                                                                |
| 3GPP-SELECTION-MODE           | 3GPP 29.061 - 16.4.7.2-12                                                 | String                 | Start, Stop, Interim update                                                                                |
| 3GPP-CHARGING-CHARACTERISTICS | 3GPP 29.061 - 16.4.7.2-13                                                 | String                 | Start, Stop, Interim update                                                                                |
| 3GPP-SGSN-MCC-MNC             | 3GPP 29.061 - 16.4.7.2-18                                                 | String                 | Start, Stop, Interim update                                                                                |
| 3GPP-IMEISV                   | 3GPP 29.061 - 16.4.7.2-20                                                 | String                 | Start, Stop, Interim update                                                                                |
| 3GPP-RAT-TYPE                 | 3GPP 29.061 - 16.4.7.2-21                                                 | Octet - 1 byte         | Start, Stop, Interim update                                                                                |
| 3GPP-USER-LOCATION            | 3GPP 29.061 - 16.4.7.2-22<br>3GPP 29.274 - 8.21-4<br>3GPP 29.274 - 8.21-5 | Special Encoded Octets | Start, Stop, Interim update                                                                                |
| 3GPP-MS-TIMEZONE              | 3GPP 29.061 - 16.4.7.2-23<br>3GPP 29.274 - 8.44                           | Special Encoded Octets | Start, Stop, Interim update                                                                                |
| 3GPP-NEGOTIATED-DSCP          | 3GPP 29.061 - 16.4.7.2-26                                                 | Octet - 1 byte         | Start, Stop, Interim update<br><br>This attribute is sent only if the associated configuration is present. |
| Acct-Status-Type              | RFC 2866                                                                  | Start/Stop/Interim     | Start, Stop, Interim update                                                                                |
| Accounting-Session-Id         | RFC 2866                                                                  | String                 | Start, Stop, Interim update                                                                                |
| Acct-Delay-time               | RFC 2866                                                                  | Octet                  | Start, Stop, Interim update                                                                                |

| Attribute                   | Reference Spec | Encoding Type | Supported Accounting Type   |
|-----------------------------|----------------|---------------|-----------------------------|
| Acct-Input-Octets           | RFC 2866       | Integer       | Stop, Interim update        |
| Acct-Output-Octets          | RFC 2866       | Integer       | Stop, Interim update        |
| Acct-Input-Gigawords        | RFC 2869       | Integer       | Stop, Interim update        |
| Acct-Output-Gigawords       | RFC 2869       | Integer       | Stop, Interim update        |
| Acct-Input-packets          | RFC 2866       | Integer       | Stop, Interim update        |
| Acct-Output-Packets         | RFC 2866       | Integer       | Stop, Interim update        |
| Acct-Session-Time           | RFC 2866       | Integer       | Stop, Interim update        |
| Acct-Terminate-Cause        | RFC 2866       | String        | Stop                        |
| Framed-MTU                  | RFC 2866       | String        | Start, Stop, Interim update |
| 3GPP-Session-Stop-Indicator | 3GPP 29.061    | Bit String    | Stop                        |
| Framed-Ip-Addr              | RFC 2866       | IPV4 Address  | Start, Stop, Interim update |
| Acct-Authentic              | RFC 2866       | String        | Start, Stop, Interim update |
| EventTimeStamp              | RFC 2869       | String        | Start, Stop, Interim update |



**Note** The WiFi call attributes are the same as the 4G call.

For complete description of the RADIUS accounting attributes, see the [RADIUS Attribute Definition, on page 18](#) section in this guide.

## Call Flows

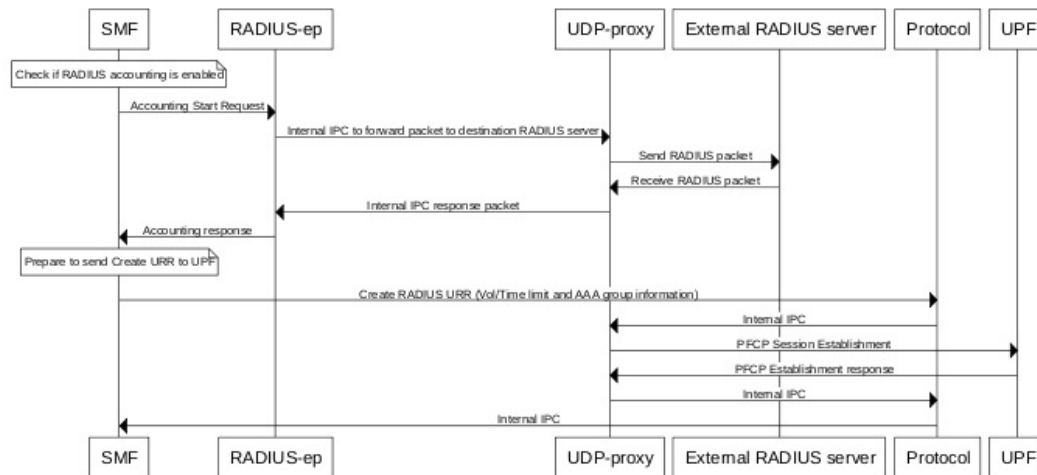
This section describes the following call flows:

- [RADIUS Accounting Start Call Flow](#)
- [RADIUS Accounting Stop Call Flow](#)
- [RADIUS Accounting Interim-update Asynchronous Call Flow](#)
- [Synchronous Accounting Interim-Update Call Flow, on page 17](#)

### RADIUS Accounting Start Call Flow

This section describes the call flow associated with the initiation of RADIUS accounting procedure.

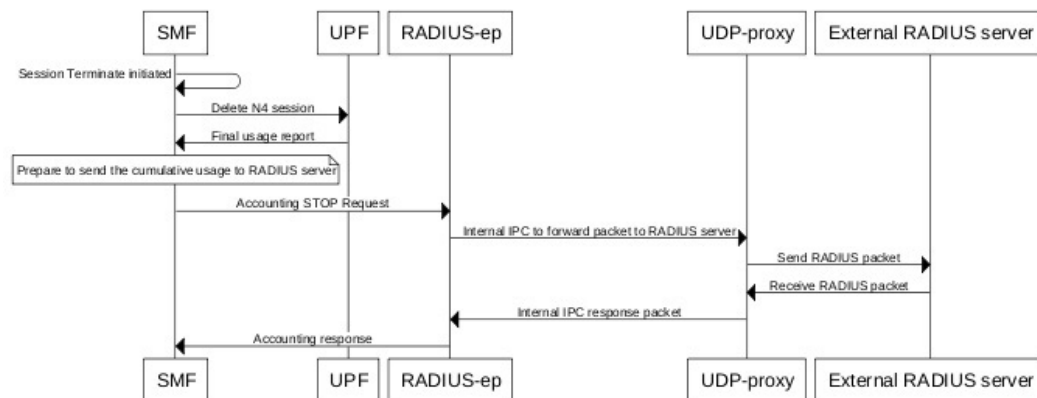
Figure 3: RADIUS Accounting Start Call Flow



## RADIUS Accounting Stop Call Flow

This section describes the call flow associated with the termination of RADIUS accounting procedure.

Figure 4: RADIUS Accounting Stop Call Flow

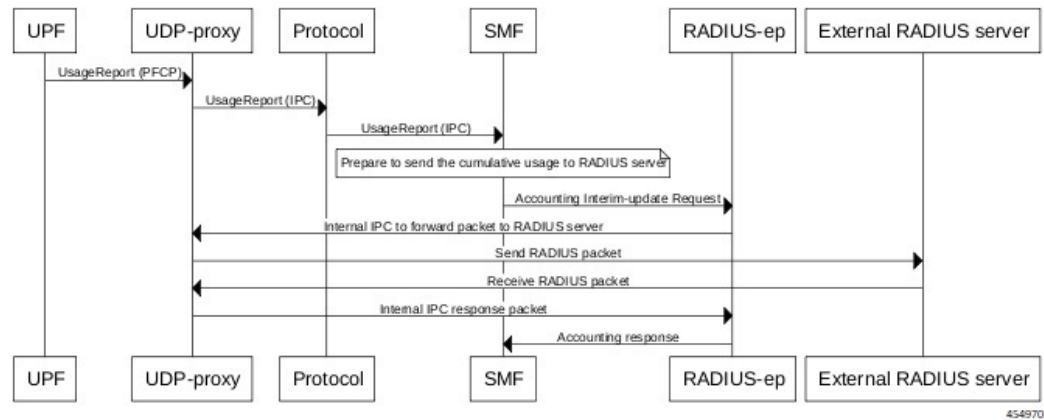


454969

## Asynchronous Accounting Interim-Update Call Flow

This section describes the call flow associated with the asynchronous interim-update request.

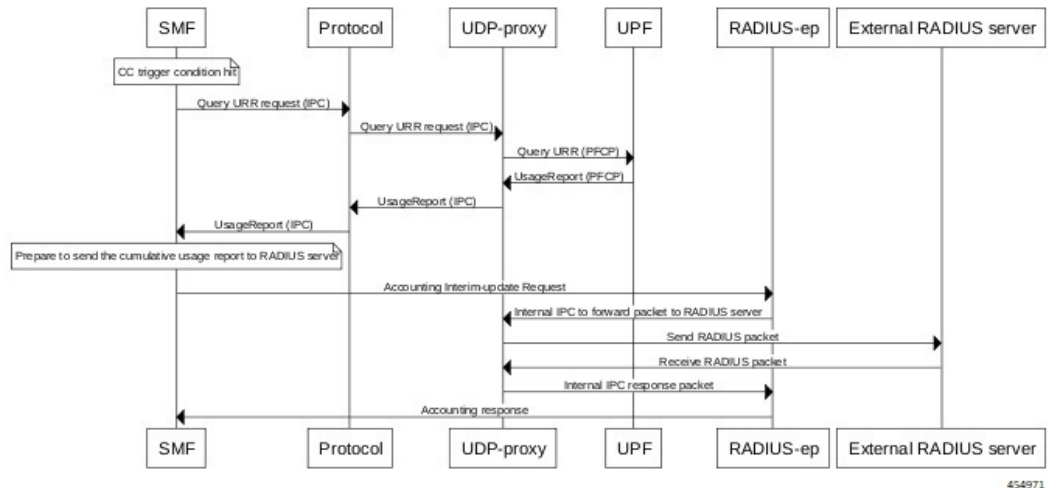
Figure 5: Asynchronous Accounting Interim-Update Call Flow



## Synchronous Accounting Interim-Update Call Flow

This section describes the call flow associated with the synchronous interim-update request.

Figure 6: Synchronous Accounting Interim-Update Call Flow



## Processing of Usage Reporting Rules

After enabling the RADIUS accounting, the SMF creates the Usage Reporting Rule (URR) and relays the rule to the UPF through the Create URR Information Element (IE). The Create URR IE is present in the N4 Session Establishment Request and it contains the volume and time limits as per the configuration.

The SMF associates the RADIUS URR only to the dynamic Packet Detection Rules (PDRs) and not for the static and predefined rules. With AAA group name in N4 session establishment request, the UPF associates the static and predefined PDRs with the RADIUS URR. The UPF sends the usage report for the RADIUS URR when the Volume limit or the Time limit is hit. Then, the SMF sends the usage in the Interim-Update Accounting-Request message to the RADIUS server.

The SMF receives the usage report for RADIUS URR in N4 Modification Response or N4 Deletion Response when any one of the following conditions are met:

- CC event condition is hit and the SMF performs Query URR
- Session Delete Response is sent

The SMF stores the values of Volume and Time thresholds reported for a previous session and reports the cumulative usage by adding the currently reported value to the stored value. The SMF sends the cumulative usage report in Accounting-Request Interim-Update and Accounting-Stop messages.

On receiving the usage report from UPF, the SMF identifies the URR IDs that are to be sent to the CHF server and to the RADIUS server. For example, if the URR ID is associated to “0x80 00 00 09”, then the SMF sends this URR ID to the RADIUS server, and the other URR IDs to the CHF server.

## Dynamic Configuration Update

The SMF allows you to change the RADIUS accounting configuration dynamically without impacting the existing sessions.

The following table identifies the impact of dynamic update to the various RADIUS accounting configurations.

**Table 5: Dynamic Update of RADIUS Accounting Configuration**

| Configuration                                                                                                                                                                            | Dynamic Change                     | Impact on Existing Sessions                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|----------------------------------------------------------------------------------------------------|
| Enabling and disabling of RADIUS accounting configuration                                                                                                                                | Allowed at the system level        | The existing sessions continue to use the old value.                                               |
| CC trigger updates                                                                                                                                                                       | Allowed as per current pod replica | The existing session uses the new value.                                                           |
| Volume and time limit changes                                                                                                                                                            | Allowed at the system level        | The existing sessions continue to use the old value.                                               |
| Global-level and group-level configurations<br><br><b>Note</b><br>If the group-level configuration is unavailable, then by default the system considers the global-level configurations. | Allowed at the system level        | The existing request continue to use the old value. New request takes the newly configured values. |

## RADIUS Attribute Definition

The following section provides a full description of each attribute. The majority of the attribute values are common for the ISE and 3GPP dictionaries. The values are included especially in the attribute description section for the attributes with different attribute values for ISE and 3GPP dictionary:

- USER-NAME

**Description:** String value encoded as per RFC 2865.

- 5G call: GPSI value is used, with stripped-off "msisdn-"
- 4G call: MSISDN value is used, with stripped-off "msisdn-"

- The attribute value for 3GPP dictionary is imsi@apn.




---

**Note** PAP, CHAP, and MSCHAP authentication methods are not supported.

---

- **PASSWORD**

**Description:** Encrypted string value encoded as per RFC 2865.

For both 5G and 4G calls, selected RADIUS server's "secret" is set as user-password.

- **CALLING-STATION-ID**

**Description:** String value encoded as per RFC 2865.

5G call: GPSI value is used, with stripped of "msisdn-"

4G call: MSISDN value is used, with stripped of "msisdn-"

- **CALLED-STATION-ID**

**Description:** String value encoded as per RFC 2865.

For both 5G and 4G calls, DNN value is set as called-station-id.

- **NAS-IP-ADDRESS**

**Description:** IPv4 address value encoded as per RFC 2865.

For both 5G and 4G calls, user-configured RADIUS Client interface-type's VIP-IP is used.

- **NAS-IDENTIFIER**

**Description:** String value encoded as per RFC 2865.

For both 5G and 4G calls, user-configured nas-identifier attribute value is used.

- **SERVICE-TYPE**

**Description:** 4-byte octet (int) value encoded as per RFC 2865.

For both 5G and 4G calls, "FRAMED (2)" value is set.

- **FRAMED-PROTOCOL**

**Description:** 4-byte octet (int) value encoded as per RFC 2865.

For both 5G and 4G calls, "GPRS-PDP-CONTEXT (7)" value is set.

- **NAS-PORT-TYPE**

**Description:** 4-byte octet (int) value encoded as per RFC 2865.

For both 5G and 4G calls, "WIRELESS-OTHER (18)" value is set.

- **NAS-PORT**

**Description:** 4-byte octet (int) value encoded as per RFC 2865.

For both 5G and 4G calls, the base value of respective instance is used. That is:

0x4000... 0x407F is set for replica-0

0x4080... 0x40FF is set for replica-1

- 3GPP-IMSI

**Description:** String value encoded as per *3GPP TS 29.061*.

5G call: SUPI value is used.

4G call: IMSI value is used.

- 3GPP-CHARGING-ID

**Description:** 4-byte octet (int) value encoded as per *3GPP TS 29.061*.

For both 5G and 4G calls, charging-ID is set.

- 3GPP-PDP-TYPE

**Description:** 4-byte octet (int) value encoded as per *3GPP TS 29.061*.

For both 5G and 4G calls, pdp-type is set as follows:

- 0 = IPv4
- 2 = IPv6
- 3 = IPv4v6

- 3GPP-CHARGING-GATEWAY-ADDR

**Description:** 4-byte octet (IPv4-address) value encoded as per *3GPP TS 29.061*.

For both 5G and 4G calls, charging gateway address is set.

- 3GPP-GPRS-NEG-QOS-PROFILE

**Description:** Octets (special encoding) value encoded as per *3GPP TS 29.061* and *29.274*.

For 5G call, the values from default-qos profile of the system are used and the encoding is performed as follows:

**Table 6: Non-GBR case**

|               |                                             |
|---------------|---------------------------------------------|
| 1-2           | <Release indicator>- = "15" (UTF-8 encoded) |
| 3             | "-" (UTF-8 encoded)                         |
| 4-5           | ARP (UTF-8 encoded)                         |
| 6-7           | 5QI (UTF-8 encoded)                         |
| 8-9           | UL Session-AMBR length (UTF-8 encoded)      |
| 10-m          | UL Session-AMBR (UTF-8 encoded)             |
| (m+1) - (m+2) | DL Session-AMBR length (UTF-8 encoded)      |
| (m+3) – n     | DL Session-AMBR (UTF-8 encoded)             |

**Table 7: GBR case**

|     |                                            |
|-----|--------------------------------------------|
| 1-2 | <Release indicator> = "15" (UTF-8 encoded) |
|-----|--------------------------------------------|

|               |                                |
|---------------|--------------------------------|
| 3             | "-" (UTF-8 encoded)            |
| 4-5           | ARP (UTF-8 encoded)            |
| 6-7           | 5QI (UTF-8 encoded)            |
| 8-9           | UL MFBR length (UTF-8 encoded) |
| 10-m          | UL MFBR (UTF-8 encoded)        |
| (m+1)-(m+2)   | DL MFBR length (UTF-8 encoded) |
| (m+3)-n       | DL MFBR (UTF-8 encoded)        |
| (n+1)-(n+2)   | UL GFBR length (UTF-8 encoded) |
| (n+3)-o       | UL GFBR (UTF-8 encoded)        |
| (o+1) – (o+2) | UL GFBR length (UTF-8 encoded) |
| (o+3) - p     | DL GFBR (UTF-8 encoded)        |

For 4G call, the values from the default-qos profile of the system are used and the encoding is performed as follows:

**Table 8: Non-GBR case**

|       |                                             |
|-------|---------------------------------------------|
| 1-2   | <Release indicator>- = "08" (UTF-8 encoded) |
| 3     | "-" (UTF-8 encoded)                         |
| 4-5   | ARP (UTF-8 encoded)                         |
| 6-7   | 5QI (UTF-8 encoded)                         |
| 8-11  | UL Session-AMBR (UTF-8 encoded)             |
| 12-15 | DL Session-AMBR (UTF-8 encoded)             |

**Table 9: GBR case**

|       |                                            |
|-------|--------------------------------------------|
| 1-2   | <Release indicator> = "08" (UTF-8 encoded) |
| 3     | "-" (UTF-8 encoded)                        |
| 4-5   | ARP (UTF-8 encoded)                        |
| 6-7   | 5QI (UTF-8 encoded)                        |
| 8-11  | UL MBR (UTF-8 encoded)                     |
| 12-15 | DL MBR (UTF-8 encoded)                     |
| 16-19 | UL GBR (UTF-8 encoded)                     |
| 20-23 | DL GBR (UTF-8 encoded)                     |

- 3GPP-SGSN-ADDRESS

**Description:** 4-byte octet (IPv4-address) value encoded as per 3GPP TS 29.061.

For 5G call, the AMF address is set.

For 4G call, the S-GW address is set.

- 3GPP-GGSN-ADDRESS

**Description:** 4-byte octet (IPv4-address) value encoded as per *3GPP TS 29.061*.

For both 5G and 4G calls, the SMF-Service IP is set.

For 3GPP dictionary, PGW control IP address as sent in CSRs.

- 3GPP-IMSI-MCC-MNC

**Description:** String value encoded as per *3GPP TS 29.061*.

For 5G call, SUPIs MCC and MNC values are set.

For 4G call, IMSIs MCC and MNC values are set.

MCC is first 3 bytes, MNC is next 2 or 3 bytes.

If MCC value is any of the following, then MNC will be of 3 bytes, else MNC will be of 2 bytes.

300 302 310 311 312 313 316 334 338 342 344 346 348 354 356 358 360 365 376 405 708 722 732

- 3GPP-GGSN-MCC-MNC

**Description:** String value encoded as per *3GPP TS 29.061*.

For both 5G and 4G calls, configured MCC and MNC value of SMF is used.

MCC is first 3 bytes, and MNC is next 2 or 3 bytes.

- 3GPP-SGSN-MCC-MNC

**Description:** String value encoded as per *3GPP TS 29.061*.

For 5G call, AMFs MCC and MNC values are set.

For 4G call, SGWs MCC and MNC values are set.

MCC is first 3 bytes, and MNC is next 2 or 3 bytes.

- 3GPP-NSAPI

**Description:** String value encoded as per *3GPP TS 29.061*.

For 5G call, QFI value from the defaultQos profile is set.

For 4G call, EPS bearer ID is set.

- 3GPP-SELECTION-MODE

**Description:** String value encoded as per *3GPP TS 29.061*.

For both 4G and 5G calls, the value is set to "0".

For 3GPP dictionary, the selection mode value is received in CSReq.

- 3GPP-CHARGING-CHARACTERISTICS

**Description:** String value encoded as per *3GPP TS 29.061*.

For both 4G and 5G calls, generic charging character is set.

- 3GPP-IMEISV

**Description:** String value encoded as per *3GPP TS 29.061*.

For 5G call, PEI value is set.

For 4G call, IMEI value is set.

- 3GPP-RAT-TYPE

**Description:** 1-byte octet encoded as per *3GPP TS 29.061*.

For 5G call, value "NR (51)" is set.

For 4G call, value "EUTRAN (6)" is set.

For WLAN call, value "WLAN (3)" is set.

- 3GPP-USER-LOCATION

**Description:** Special octet value encoded as per *3GPP TS 29.061*.

For 5G call, the following encoding logic is used:

|      |                                                                            |
|------|----------------------------------------------------------------------------|
| 1    | Location-Type<br>Only TAI = 136<br>Only NCGI = 135<br>Both TAI + NCGI =137 |
| 2-7  | TAI-Encoding (if present)                                                  |
| 8-15 | NCGI-Encoding (if present)                                                 |

TAI Encoding header:

|     |             |             |
|-----|-------------|-------------|
| 1   | MCC digit 2 | MCC digit 1 |
| 2   | MNC digit 3 | MCC digit 3 |
| 3   | MNC digit 2 | MNC digit 1 |
| 4-6 | TAC value   |             |

NCGI Encoding header:

|     |                          |             |
|-----|--------------------------|-------------|
| 1   | MCC digit 2              | MCC digit 1 |
| 2   | MNC digit 3              | MCC digit 3 |
| 3   | MNC digit 2              | MNC digit 1 |
| 4   | SPARE                    | NCI         |
| 5-8 | NR Cell Identifier (NCI) |             |

For 4G call, the following encoding logic is used:

|   |                      |
|---|----------------------|
| 1 | Location-Type        |
|   | Only TAI = 128       |
|   | Only ECGI = 129      |
|   | Both TAI + ECGI =130 |

|      |                            |
|------|----------------------------|
| 2-6  | TAI-Encoding (if present)  |
| 7-13 | ECGI-Encoding (if present) |

TAI Encoding header:

|     |             |             |
|-----|-------------|-------------|
| 1   | MCC digit 2 | MCC digit 1 |
| 2   | MNC digit 3 | MCC digit 3 |
| 3   | MNC digit 2 | MNC digit 1 |
| 4-5 | TAC value   |             |

ECGI Encoding header:

|     |                              |             |
|-----|------------------------------|-------------|
| 1   | MCC digit 2                  | MCC digit 1 |
| 2   | MNC digit 3                  | MCC digit 3 |
| 3   | MNC digit 2                  | MNC digit 1 |
| 4   | Spare                        | ECI         |
| 5-7 | EUTRAN Cell Identifier (ECI) |             |

- 3GPP-MS-TIMEZONE

**Description:** Special octet value encoded as per *3GPP TS 29.061*.

Timezone string (for example: -07:00+1) is encoded as two-byte value as mentioned in the following table.

|   |                                                                                                                                  |
|---|----------------------------------------------------------------------------------------------------------------------------------|
| 1 | TIMEZONE<br>The first byte timezone is encoded as per 3GPP 29.061, 3GPP 29.274, 3GPP 24.008, and 3GPP 23.040 (section 9.2.3.11). |
| 2 | DAYLIGHT SAVING 0, or +1 or +2<br>The second byte daylight consists of two bits used (00-0, 01-+1, 10-+2, 11 – Unused).          |

- 3GPP-NEGOTIATED-DSCP

**Description:** 1-byte octet encoded as per *3GPP TS 29.061*

For both 5G and 4G calls, DSCP configuration from DNN qos-profile configuration is used.

Sub -> DNN profile -> QosProfile -> DSCPMap -> Qi5 value check -> ARP priority check

- FRAMED-IP

The IPv4 address value decoded as per RFC 2865.

For both 4G and 5G calls, the received value is set as the IPv4 address for the subscriber.

- FRAMED-IPv6-PREFIX

The IPv6 Prefix + Length value decoded as per RFC 3162.

For both 4G and 5G calls, the received value is set as the IPv6 prefix for the subscriber.




---

**Important** If the received prefix-length is !=64, the SMF overrides to 64.

---

- IDLE-TIMEOUT

The 4-byte octet (integer) value encoded as per RFC 2865. This attribute is supported in the inbound RADIUS packet.

For both 4G and 5G calls, the received value is used as the maximum number of consecutive seconds of idle time that the user is permitted before being disconnected by the NAS.

- SESSION-TIMEOUT

The 4-byte octet (integer) value encoded as per RFC 2865. This attribute is supported in the inbound RADIUS packet.

For both 4G and 5G calls, the received value is used as the maximum number of seconds that the user is allowed to remain connected by the NAS.

- 3GPP-Negotiated-QoS-Profile

- Access-request

For ISE or default dictionary: ARP PCI and ARP PVI were sent out incorrectly and did not match value received in CSReq. Also APN AMBR was sent out in bps instead of Kbps.

For 3GPP dictionary: ARP PCI and ARP PVI values are fixed and in sync with what is received in CSReq. Also APN AMBR is sent out in Kbps.

- Accounting-request

For ISE or default dictionary: ARP PCI and ARP PVI were sent out incorrectly and did not match value received in CSReq/Gx CCA-I. Also APN AMBR was sent out in bps instead of Kbps.

- For 3GPP dictionary: ARP PCI and ARP PVI values are fixed and in sync with what is received in CSReq/Gx-CCA-I. Also APN AMBR is sent out in Kbps.

- 3GPP-IMEI-SV

- Access-request

For ISE or default dictionary: For 16 bit IMEI: imeisv-1122334455667788 and for 15 bit imei: 112233445566778.

For 3GPP dictionary: For 16 bit IMEI: 1122334455667788 and for 15 bit IMEI: 112233445566778.

- Accounting-request

For ISE or default dictionary: For 16 bit IMEI: imeisv-1122334455667788 and for 15 bit IMEI: 112233445566778.

- For 3GPP dictionary: For 16 bit IMEI: 1122334455667788 and for 15 bit IMEI: 112233445566778.

- 3GPP-UE-Location

- Access-request

For ISE or default dictionary: ECI value is going as 0.

For 3GPP dictionary: the value is received in CSReq.

- Accounting-request

For ISE or default dictionary: For 16 bit IMEI: imeisv-1122334455667788 and for 15 bit IMEI: 112233445566778.

- For 3GPP dictionary: For 16 bit IMEI: 1122334455667788 and for 15 bit IMEI: 112233445566778



**Note** The WiFi call attributes are the same as the 4G call.

## Standards Compliance

The RADIUS Client feature complies with the following standards:

- RFC 2865: RADIUS
- RFC 2866: RADIUS Accounting
- RFC 3162: RADIUS and IPv6
- 3GPP TS 29.061
- 3GPP TS 29.274
- 3GPP TS 29.561, version 16.4.0

## Limitations and Restrictions

The SMF has the following limitations:

- The SMF supports only single RADIUS attribute profile, and does not support dictionary selection.
- If RADIUS accounting is enabled and server-group is configured within DNN profile, the SMF sends server-group as AAA group in charging-params in N4 session establishment. The UPF displays an error if there is a server group mismatch between SMF and UPF.

In this scenario, static and predefined usage are not accounted in the RADIUS URR. However, the dynamic rules traffic is accounted in the RADIUS URR.

## Configuring the RADIUS Client

The RADIUS client provides both RADIUS authentication and accounting functionalities. For using these functionalities, it is important to enable the RADIUS authentication and accounting framework through the associated CLI configuration.

This section describes how to configure the RADIUS client.



**Important** Configuring the VIP-IP of the RADIUS client interface is mandatory for the RADIUS client to work. Also, the VIP-IP must be the same as the IP of the UDP proxy pod.

Configuring the RADIUS Client involves the following:

- [Configuring RADIUS Server, on page 27](#)
- [Configuring RADIUS Server Selection Logic, on page 29](#)
- [Configuring RADIUS Attributes, on page 29](#)
- [Configuring RADIUS Detect Dead Server, on page 32](#)
- [Configuring RADIUS Dead Time, on page 32](#)
- [Configuring RADIUS Retries, on page 34](#)
- [Configuring RADIUS Dictionary](#)
- [Configuring RADIUS dictionary at server-group, on page 33](#)
- [Configuring RADIUS Timeout, on page 36](#)
- [Configuring RADIUS Pod, on page 36](#)
- [Configuring Secondary Authentication Method, on page 39](#)
- [Configuring PAP, CHAP, or MSCHAP-based Authentication, on page 40](#)
- [Enabling RADIUS Accounting, on page 41](#)
- [Defining RADIUS Server Group in DNN Profile, on page 42](#)
- [Configuring RADIUS Accounting Options, on page 42](#)
- [Configuring RADIUS Accounting Server Group, on page 43](#)
- [Configuring the Session Disconnect Feature, on page 44](#)
- [Enabling RADIUS Authentication Allow Parameter, on page 30](#)
- [Configuring Consecutive Failure, on page 31](#)
- [Configuring Max Transmissions, on page 35](#)
- [Configuring Internal Virtual IP for Protocol Endpoint, on page 31](#)

## Configuring RADIUS Server

Use the following sample configuration to configure the RADIUS server.

```
config
  profile radius
    server ipv4_address port_num
      secret secret_key
      priority priority_value
```

```
type { acct | auth }
commit
```

**NOTES:**

- **profile radius:** Enter the RADIUS configuration mode.
- **server *ipv4\_address port\_num*:** Specify the IPv4 address and port of the RADIUS server.
- **secret *secret\_key*:** Specify the secret key.
- **priority *priority\_value*:** Specify the server priority.
- **type { acct | auth }:** Specify the type of the RADIUS server. The server can be one of the following:
  - **acct:** RADIUS server used for the accounting requests
  - **auth:** RADIUS server used for the authentication requests
- **commit:** Commit the configuration.

**Example**

The following is an example of the RADIUS server configuration.

```
profile radius
server 209.165.200.238 1812
secret $8$73a0i4G3ILj0Np+8tn2QOoWDj3QkB+oefPc2ZK6RE6A=
priority 1
exit
server 209.165.200.240 1812
secret $8$VccEEUVou7m5ptA9WZRPR7KDmxQ/L3KlJ3QqgHjexkk=
priority 2
exit
exit
```

**Verifying the RADIUS Configuration**

Use the **show radius** command to display information about the RADIUS servers (both accounting and authentication) that are configured in the system.

The following configuration is a sample output of the **show radius** command:

```
bng# show radius
radius
-----
Server: 209.165.200.231, port: 1812, status: up, port-type: Auth
2 requests, 0 pending, 0 retransmits
1 accepts, 1 rejects, 0 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 4 ms latest rtt
-----
Server: 209.165.200.231, port: 1813, status: up, port-type: Acct
3 requests, 0 pending, 0 retransmits
3 responses, 0 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 1 ms latest rtt
-----
```

## Configuring RADIUS Server Selection Logic

Use the following sample configuration to configure the RADIUS server selection logic.

```
config
  profile radius
    algorithm { first-server | round-robin }
  commit
```

### NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **algorithm { first-server | round-robin }**: Define the algorithm for selecting the RADIUS server.
  - **first-server**: Set the selection logic as highest priority first. This is the default behavior.
  - **round-robin**: Set the selection logic as round-robin order of servers.
- **commit**: Commit the configuration.

### Example

The following is an example of the RADIUS server selection logic configuration.

```
config
  profile radius
    algorithm round-robin
  exit
```

## Configuring RADIUS Attributes

To configure the RADIUS attributes for authentication and accounting, use the following sample configuration:

```
config
  profile radius
    attribute [ [ instance gr_instance_id ] [ nas-identifier nas_id ] [
nas-ip ipv4_address ] ]
  end
```

### NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **attribute [ [ instance gr\_instance\_id ] [ nas-identifier nas\_id ] [ nas-ip ipv4\_address ] ]**: Configure the RADIUS identification parameters.
  - **instance gr\_instance\_id**: Specify the Geographic Redundancy (GR) instance ID. *gr\_instance\_id* must be an integer.
  - **nas-identifier nas\_id**: Specify the attribute name by which the system will be identified in Accounting-Request messages. *nas\_id* must be an alphanumeric string.
  - **nas-ip ipv4\_address**: Specify the NAS IPv4 address. *ipv4\_address* must be an IPv4 address in dotted decimal notation.

- The NAS-IP-Address and NAS-Identifier attributes can be configured per instance-id in RADIUS profile configuration. In this case, NAS-IP-Address and NAS-Identifier attributes under instance configuration are treated as high priority over the non-instance based attribute configuration.

### Example

The following is an example of the RADIUS attributes configuration.

```
config
  profile radius
    attribute
      instance 1
        nas-identifier CiscoSmf
      exit
    exit
  exit
exit
```

## Enabling RADIUS Authentication Allow Parameter

Use the following configuration to enable allow-auth in the RADIUS server.

```
config
  profile radius
    enable-allow-auth
  end
```

### NOTES:

- **profile radius:** Enter the RADIUS configuration mode.
- **enable-allow-auth :** If allow-auth is enabled in the configuration, it allows the ongoing call to continue irrespective of authentication being successful, timed out, or any error message received. The default value is false, configuration is required to enable the allow-auth.

Use the following configuration to enable allow-auth in the RADIUS server group.

```
config
  profile radius
    server-group group_name
      enable-allow-auth
    end
```

### NOTES:

- **profile radius:** Enter the RADIUS configuration mode.
- **server-group group\_name:** Enter the server group on which you want to enable the allow-auth.
- **enable-allow-auth :** If allow-auth is enabled in the configuration, it allows the ongoing call to continue irrespective of authentication being successful, timed out, or any error message received. The default value is false, configuration is required to enable the allow-auth..

## Configuring Consecutive Failure

Use the following configuration to configure consecutive failure in the RADIUS server. Even if there is no option for dead-server-detection, consecutive-failure is enabled by default and its default value is 10. To turn it off, the user must set the value to 0.

```
config
  profile radius
    detect-dead-server consecutive-failures value
  end
```

### NOTES:

- **profile radius:** Enter the RADIUS configuration mode.
- **detect-dead-server consecutive-failures value:** When a server's failure count reaches the threshold for consecutive failures, the server is declared as dead server.  
*value:* must be an integer in the range of 1–1000. Default: 10.

- It is recommended to configure the consecutive failure value more than the request maxTransmissions value in the setup.

**Example:** The consecutive failure count may be greater than 6 if maxRetry = 2 and maxTransmissions = 6, so as not to affect the server switch caused by maxtransmissions. Moreover, a server level value called consecutive-failure is increased when successive requests are made to the same server.

## Configuring Internal Virtual IP for Protocol Endpoint

The protocol endpoint is the configuration for the UDP-Proxy pod. The UDP-Proxy pod receives the IPC request to send the UDP message from the RADIUS-EP pod. The UDP-Proxy pod then converts the message to a proper UDP packet and sends it to the radius server. When radius server is sending UDP packet to the SMF, the UDP-Proxy pod receives and forwards the packet on the TCP connection to the RADIUS-EP pod.

```
config
  instance instance-id gr_instance_id
    endpoint protocol
      replicas replica_id
      nodes node_id
      internal-vip { SMF_UDP_PROXY_INTERNAL_VIP }
      vip-ip { client_ipv4_address }
    exit
  exit
```

### NOTES:

- **instance instance-id gr\_instance\_id:** Specify GR Instance ID.
- **endpoint protocol:** Enter the endpoint configuration mode.
- **replicas replica\_id:** Specifies the replica server's ID.
- **nodes node\_id:** Specify the node ID for the SMF peer node. The value must be a string.

- **internal-vip**{ *SMF\_UDP\_PROXY\_INTERNAL\_VIP* }: Specify the IP address of the UDP-Proxy for internal SMF communication, Radius-ep uses this IP address to reach the UDP proxy for outgoing AAA messages.
- **VIP-ip**{ *client\_ipv4\_address* }: Specify the IP address of the dynamic authorization client. *ipv4\_address* must be in standard IPv4 dotted decimal notation.

### Example

The following is an example configuration.

```
config
  instance instance-id 1
    endpoint protocol
      replicas 1
      nodes 2
      internal-vip {SMF_UDP_PROXY_INTERNAL_VIP}
      vip-ip { client_ipv4_address}
    exit
  exit
```

## Configuring RADIUS Detect Dead Server

Use the following sample configuration to configure the RADIUS detect dead server.

```
config
  profile radius
    detect-dead-server response-timeout value
  commit
```

### NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **detect-dead-server response-timeout value**: Set the timeout value that marks a server as "dead" when a packet is not received for the specified number of seconds.  
*value* must be an integer in the range of 1–65535. Default: 10 seconds.
- **commit**: Commit the configuration.

### Example

The following is an example of the RADIUS detect dead server configuration.

```
config
  profile radius
    detect-dead-server response-timeout 100
  exit
```

## Configuring RADIUS Dead Time

Use the following sample configuration to configure the RADIUS dead time.

```
config
  profile radius
```

```

deadtime value
commit

```

#### NOTES:

- **profile radius:** Enter the RADIUS configuration mode.
- **deadtime value:** Set the time to elapse between RADIUS server marked unreachable and when we can reattempt to connect.  
*value* must be an integer in the range of 1–65535. Default: 10 minutes.
- **commit:** Commit the configuration.

#### Example

The following is an example of the RADIUS dead time configuration.

```

config
  profile radius
    deadtime 15
  exit

```

## Configuring RADIUS Dictionary

Use the following sample configuration to configure the RADIUS dictionary.

```

config
  profile radius
    dictionary { ISE dictionary | 3GPP dictionary | custom1 dictionary }
  commit

```



#### Note

- **profile radius:** Enter the RADIUS configuration mode.
- **dictionary { ISE dictionary | 3GPP dictionary | custom1 dictionary }:** Configures the dictionary to be used for RADIUS message processing. When configured, the SMF service populates RADIUS request messages using the selected dictionary format.
- **commit:** Commit the configuration.

The following is an example of the RADIUS dictionary configuration.

```

config
  profile radius
    dictionary { ISE dictionary | 3GPP dictionary | custom1 dictionary }
  exit

```

## Configuring RADIUS dictionary at server-group

Use the following sample configuration to configure the RADIUS dictionary at server-group level,

```

config
  profile radius
    server group <server-group-name>
      dictionary { ISE dictionary | 3GPP dictionary | custom1 dictionary
    }
  commit

```

**NOTES:**

- **profile radius:** Enter the RADIUS configuration mode.
- **server-group <server-group-name>:** Specifies the RADIUS server group.
- **dictionary { ISE dictionary | 3GPP dictionary | custom1 dictionary }:** Configures the dictionary to be used by the specified server-group. When configured, the SMF service populates RADIUS request messages using the selected dictionary format.
- **commit:** Commits the configuration.
- The dictionary configured under a RADIUS server group takes precedence over the globally configured dictionary.

**Example**

The following is an example of the RADIUS dictionary at server-group.

```

config
  profile radius
    dictionary { ISE dictionary | 3GPP dictionary | custom1 dictionary }
    server-group b2b.static_AAA
    dictionary { ISE dictionary | 3GPP dictionary | custom1 dictionary }
  exit

```

## Configuring RADIUS Retries

Use the following sample configuration to configure the maximum RADIUS retries.

```

config
  profile radius
    max-retry value
  commit

```

**NOTES:**

- **profile radius:** Enter the RADIUS configuration mode.
- **max-retry value:** Set the maximum number of times that the system will attempt retry with the RADIUS server.  
*value* must be an integer in the range of 0–65535. Default: 2
- **commit:** Commit the configuration.

**Example**

The following is an example of the RADIUS retries configuration.

```
config
  profile radius
    max-retry 2
  exit
```

## Configuring Max Transmissions

Use the following configuration to configure max transmissions in the RADIUS server.

```
config
  profile radius
    max-transmissions value
  end
```

### NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **max-transmissions value**: Max transmission allows you to configure the transmission parameters for all the available servers. This feature helps to cross-check if the number of transmissions exceeds the number of retries once the retry cycle for a request is finished, and if so, it begins the subsequent retry cycle on a different server if one is available. If no server is available or if maxtransmissions limit is reached, then the server database sends out the timeout response.  
*value*: must be an integer in the range of 0–65535. Default: 6.
- Max transmission value should always be higher value than the max retries +1. It is recommended to use maxTransmissions number as multiples of (maxRetries +1).
- Based on the maxTransmissions, time spent on a single request increases and remains in the system without providing a response by retrying on other servers. As a result, system resources are used up, which may lead to performance degradation.

Use the following configuration to configure max transmissions in the RADIUS server group.

```
config
  profile radius
    server-group group_name
      max-transmissions value
    end
```

### NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **server-group group\_name**: Enter the server group on which you want to configure the max-transmissions.
- **max-transmissions value**: Max transmission allows you to configure the transmission parameters for all the available servers. This feature helps to cross-check if the number of transmissions exceeds the number of retries once the retry cycle for a request is finished, and if so, it begins the subsequent retry cycle on a different server if one is available. If no server is available or if maxtransmissions limit is reached, then the server database sends out the timeout response.  
*value*: must be an integer in the range of 0–65535. Default: 6.
- Max transmission value should always be higher value than the max retries +1. It is recommended to use maxTransmissions number as multiples of (maxRetries +1).

- Based on the maxTransmissions, time spent on a single request increases and remains in the system without providing a response by retrying on other servers. As a result, system resources are used up, which may lead to performance degradation.

## Configuring RADIUS Timeout

Use the following sample configuration to configure the RADIUS timeout.

```
config
  profile radius
    timeout value_in_seconds
  commit
```

### NOTES:

- **profile radius:** Enter the RADIUS configuration mode.
- **timeout *value\_in\_seconds*:** Set the time to wait for response from the RADIUS server before retransmitting.  
*value\_in\_seconds* must be an integer in the range of 1–65535. Default: 2 seconds.
- **commit:** Commit the configuration.

### Example

The following is an example of the RADIUS timeout configuration.

```
config
  profile radius
    timeout 4
  exit
```

## Configuring RADIUS Pod

Use the following sample configuration to configure the RADIUS pod.

```
config
  instance instance-id gr_instance_id
    endpoint radius
      replicas number_of_replicas
    commit
```

### NOTES:

- **endpoint radius:** Enter the RADIUS endpoint configuration mode.
- **replicas *number\_of\_replicas*:** Set the number of replicas required.
- **commit:** Commit the configuration.

### Example

The following is an example of the RADIUS pod configuration.

```

config
  instance instance-id 1
  endpoint radius
    replicas 3
  exit

```

## Configuring RADIUS NAS-IP

This section describes how to configure the RADIUS NAS-IP.

### Multiple RADIUS NAS-IP Configuration



**Note** The NAS-Identifier attribute configuration can be defined per instance-id in RADIUS profile configuration. In this case, NAS-Identifier attribute under instance configuration is treated as high priority over the non-instance based NAS-Identifier attribute configuration.

To configure multiple RADIUS NAS-IP addresses at various levels, use the following sample configuration:

```

config
  profile radius
    attribute [[ instance gr_instance_id ] [ nas-ip ipv4_address ] ]
    accounting attribute [[ instance gr_instance_id ] [ nas-ip ipv4_address ] ]
  ]
  server-group group_name attribute [[ instance gr_instance_id ] [ nas-ip
ipv4_address ] ]
  server-group group_name accounting attribute [[ instance gr_instance_id
] [ nas-ip ipv4_address ] ]
end

```

#### NOTES:

- **profile radius:** Enter the RADIUS configuration mode.
- **attribute [[ instance gr\_instance\_id ] [ nas-ip ipv4\_address ] ]:** Set the global NAS-IP address value.
  - **instance gr\_instance\_id:** Specify the Geographic Redundancy (GR) instance ID. *gr\_instance\_id* must be an integer.
  - **nas-ip ipv4\_address:** Specify the NAS IPv4 address. *ipv4\_address* must be an IPv4 address in dotted decimal notation.
- **accounting attribute [[ instance gr\_instance\_id ] [ nas-ip ipv4\_address ] ]:** Set the global accounting NAS-IP address value.
  - **instance gr\_instance\_id:** Specify the Geographic Redundancy (GR) instance ID. *gr\_instance\_id* must be an integer.
  - **nas-ip ipv4\_address:** Specify the NAS IPv4 address. *ipv4\_address* must be an IPv4 address in dotted decimal notation.
- **server-group group\_name attribute [[ instance gr\_instance\_id ] [ nas-ip ipv4\_address ] ]:** Set the per server-group common NAS-IP address value.

- **instance** *gr\_instance\_id*: Specify the Geographic Redundancy (GR) instance ID. *gr\_instance\_id* must be an integer.
- **nas-ip** *ipv4\_address*: Specify the NAS IPv4 address. *ipv4\_address* must be an IPv4 address in dotted decimal notation.
- **server-group** *group\_name* **accounting attribute** [**instance** *gr\_instance\_id*] [**nas-ip** *ipv4\_address* ]: Set the per server-group accounting NAS-IP address value.
  - **instance** *gr\_instance\_id*: Specify the Geographic Redundancy (GR) instance ID. *gr\_instance\_id* must be an integer.
  - **nas-ip** *ipv4\_address*: Specify the NAS IPv4 address. *ipv4\_address* must be an IPv4 address in dotted decimal notation.

### Example:

The following is an example of the multiple RADIUS NAS-IP configuration.

```

config
profile radius
attribute
instance 1
nas-ip 209.165.200.225
nas-identifier smf1
exit
instance 2
nas-ip 209.165.201.2

nas-identifier smf2
exit
exit
accounting
attribute
instance 1
nas-ip 209.165.200.225
nas-identifier smf1
exit
instance 2
nas-ip 209.165.201.2

nas-identifier smf2
exit
exit
exit
server-group g1
attribute
instance 1
nas-ip 209.165.200.225
nas-identifier smf1
exit
instance 2
nas-ip 209.165.201.2

nas-identifier smf2
exit
exit
exit
accounting
attribute

```

```

instance 1
  nas-ip 209.165.200.225
  nas-identifier smf1
exit
instance 2
  nas-ip 209.165.201.2

  nas-identifier smf2
exit
exit
exit
exit

```

## Configuring Secondary Authentication Method

Use the following sample configuration to configure the secondary authentication method.

```

config
  profile dnn dnn_name
    authentication secondary radius [ group group_name ]
  commit

```

### NOTES:

- **profile dnn *dnn\_name***: Enter the DNN Profile configuration mode.
- **authentication secondary radius [ group *group\_name* ]**: Enable secondary authentication under the DNN profile and sets method as RADIUS.  
**group *group\_name***: This keyword is optional. This keyword defines the RADIUS server group name.
- **commit**: Commit the configuration.

### Example

The following is a configuration example of the secondary authentication method.

```

config
  profile dnn intershat
  ...
  authentication secondary radius
exit

```

## Verifying the RADIUS Authentication Configuration

Use the **show radius auth-server** command to display detailed statistics for RADIUS authentication server and port.

The following configuration is a sample output of the **show radius auth-server** command:

```

bng# show radius auth-server
-----
Server: 209.165.200.232, port: 1812, status: up, port-type: Auth
2 requests, 0 pending, 0 retransmits
1 accepts, 1 rejects, 0 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 4 ms latest rtt
-----

```

## Configuring PAP, CHAP, or MSCHAP-based Authentication

This section provides the configuration to enable the PAP, CHAP, and MSCHAP-based RADIUS authentication. This configuration aids in converting the CHAP Challenge and Response received in PCO IE as MSCHAP Challenge and Response.

### Defining Priority for Authentication Algorithm

Use the following sample configuration to define the priority for different authentication algorithms (PAP or CHAP or MSCHAP) for RADIUS-based authentication in SMF.

```
config
  profile dnn profile_name
    authentication { { secondary radius [ group group_name ] | { algorithm
  { pap priority_value [ password-use-pco ] | chap priority_value [
convert-to-mschap ] | mschap priority_value } }
    end
```

#### NOTES:

- **password-use-pco**: This keyword overrides the DNN configured password with PCO password. The default setting is disabled.  
If the host level password is not configured at DNN, then the SMF uses the UE given password for PAP-based authentication even though this configuration is disabled.
- **convert-to-mschap**: This keyword converts the received CHAP Challenge and Response to MSCHAP if the CHAP Response length is 49 bytes. Otherwise, the SMF sends as CHAP only even though this configuration is explicitly enabled.
- The default priority for PAP, CHAP, and MSCHAP algorithms is 0 which means that the configuration is disabled. The valid values are 1, 2, and 3. Lower the value, higher is the priority. It is used to resolve conflicts if the UE sends multiple authentication parameters in the PCO, EPCO, or APCO IE.

### Configuring Host Password

Use the following sample configuration to specify the host password at DNN level which is used as a password for PAP-based authentication.

```
config
  profile dnn profile_name
    outbound password password
    end
```

#### NOTES:

- **profile dnn *profile\_name***: Specify the DNN profile name as an alphanumeric string to enter the DNN configuration mode.
- **outbound password *password***: Specify the DNN host password for authentication. By default, the SMF sends this password in PAP user-password if it is not explicitly overridden using the **password-use-pco** option.

By default, the SMF encrypts the given password using AES-128-CFB encryption algorithm.

## Enabling RADIUS Accounting

Use the following sample configuration to enable RADIUS accounting on SMF and configure the RADIUS accounting specific parameters.

```
config
  profile charging charging_profile_name
    accounting limit { duration value | volume { downlink value | total
value | uplink value } }
    accounting triggers [ ambr-change | plmn-change | qos-change |
rat-change | serv-node-change | tft-change | ue-time-change |
user-loc-change ]
  commit
```

### NOTES:

- **profile charging *charging\_profile\_name***: Specify the charging profile name. *charging\_profile\_name* must be an alphanumeric string.
- **accounting**: Specify this option to enable RADIUS accounting on SMF for the subscribers.
- **limit { duration *value* | volume { downlink *value* | total *value* | uplink *value* } }**: Specify the volume and time limits for RADIUS accounting.
  - duration *value***: Specify the time duration value as an integer in the range of 0–2147483647.
  - downlink *value***: Specify the downlink volume limit for interim generation in bytes, as an integer in the range of 100000–4000000000.
  - total *value***: Specify the total volume limit for interim generation in bytes, as an integer in the range of 100000–4000000000.
  - uplink *value***: Specify the uplink volume limit for interim generation in bytes, as an integer in the range of 100000–4000000000.
- **accounting triggers [ ambr-change | plmn-change | qos-change | rat-change | serv-node-change | tft-change | ue-time-change | user-loc-change ]**: Enable the appropriate RADIUS accounting triggers according to the following conditions:
  - AMBR change
  - PLMN change
  - Quality of Service change
  - Routing Area Information change
  - Serving node change
  - Traffic Flow Template (TFT) change
  - UE time change
  - User Location Information change - applicable only for PGW-C and GGSN.



### Important

Enabling any one of these triggers turns off the remaining triggers.

- **commit**: Commit the configuration.

## Defining RADIUS Server Group in DNN Profile

Use the following sample configuration to set RADIUS server-group to use for accounting in DNN profile. All subscribers under the specified DNN will have RADIUS accounting enabled.

```
config
  profile dnn dnn_profile_name
    accounting server-group group_name
  commit
```

### NOTES:

- **profile dnn dnn\_profile\_name**: Specify the DNN profile name to enter the DNN configuration mode. *dnn\_profile\_name* must be an alphanumeric string.
- **accounting server-group group\_name**: Specify the RADIUS server-group to use for accounting in the configured DNN profile. *group\_name* must be an alphanumeric string.
- **commit**: Commit the configuration.

## Configuring RADIUS Accounting Options

To configure the RADIUS accounting options, use the following sample configuration:

```
config
  profile radius accounting
    algorithm { first-server | round-robin }
    attribute [ [ instance gr_instance_id ] [ nas-identifier nas_id ] [
nas-ip ipv4_address ] ]
    deadtime value
    detect-dead-server response-timeout value
    max-retry value
    timeout value
  end
```

### NOTES:

- **profile radius accounting**: Enter the RADIUS accounting configuration mode.
- **algorithm { first-server | round-robin }**: Define the algorithm for selecting the RADIUS server.
  - **first-server**: Set the selection logic as highest priority first. This is the default behavior.
  - **round-robin**: Set the selection logic as round-robin order of servers.
- **attribute [ [ instance gr\_instance\_id ] [ nas-identifier nas\_id ] [ nas-ip ipv4\_address ] ]**: Configure the RADIUS identification parameters.
  - **instance gr\_instance\_id**: Specify the Geographic Redundancy (GR) instance ID. *gr\_instance\_id* must be an integer.

- **nas-identifier** *nas\_id*: Specify the attribute name by which the system will be identified in Accounting-Request messages. *nas\_id* must be an alphanumeric string.
- **nas-ip** *ipv4\_address*: Specify the NAS IPv4 address. *ipv4\_address* must be an IPv4 address in dotted decimal notation.
- **deadtime** *value*: Set the time to elapse between RADIUS server marked unreachable and when we can re-attempt to connect.  
*value* must be an integer from 0 through 65535. Default: 10 minutes.
- **detect-dead-server response-timeout** *value*: Set the timeout value that marks a server as "dead" when a packet is not received for the specified number of seconds.  
*value* must be an integer from 1 through 65535. Default: 10 seconds.
- **max-retry** *value*: Set the maximum number of times that the system will attempt retry with the RADIUS server.  
*value* must be an integer in the range of 0–65535. Default: 2
- **timeout** *value*: Set the time to wait for response from the RADIUS server before retransmitting.  
*value* must be an integer in the range of 1–65535. Default: 2 seconds.
- All the keyword options under the RADIUS accounting configuration mode are also available within the RADIUS configuration mode.

## Configuring RADIUS Accounting Server Group

Use the following sample configuration to configure the RADIUS server group.

```
config
  profile radius
    server-group group_name
  commit
```

### NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **server group** *group\_name*: Specify the name of server group for use in RADIUS accounting. *group\_name* must be an alphanumeric string.
- **commit**: Commit the configuration.

## Verifying the RADIUS Accounting Configuration

Use the **show radius acct-server** command to display statistics for RADIUS accounting server and port.

The following configuration is a sample output of the **show radius acct-server** command:

```
bng# show radius acct-server
-----
Server: 209.165.200.228, port: 1813, status: up, port-type: Acct
3 requests, 0 pending, 0 retransmits
3 responses, 0 timeouts
0 bad responses, 0 bad authenticators
```

```
0 unknown types, 0 dropped, 1 ms latest rtt
```

## Configuring the Session Disconnect Feature

This section describes how to configure the Session Disconnect feature.

Configuring the Session Disconnect feature in SMF involves the following steps:

- [Configuring the Dynamic Authorization Service, on page 44](#)
- [Configuring the CoA-NAS Interface, on page 45](#)

## Configuring the Dynamic Authorization Service

Use the following sample configuration to enable the NAS as an authentication, authorization, and accounting (AAA) server for the dynamic authorization service. This service supports the RADIUS Disconnect and Change of Authorization (CoA) functionality.

```
config
  profile radius-dynamic-author
    client ipv4_address [ secret shared_secret ]
    nas-identifier value
    secret shared_secret
  end
```

### NOTES:

- **profile radius-dynamic-author:** Enter the dynamic authorization configuration mode.
- **client ipv4\_address [ secret shared\_secret ]:** Specify the IP address of the Dynamic Authorization Client. *ipv4\_address* must be in standard IPv4 dotted decimal notation.  
You can add a list of client IPs from which the Disconnect message is accepted.  
**secret shared\_secret:** This is an optional keyword. Specify the secret key at the client level.



### Important

Configuring the server key at the client level overrides the server key configured at the global level.

- **nas-identifier value:** Specify the dynamic authorization specific NAS-Identifier value. *value* must be an alphanumeric string of 1 to 64 characters.

If this keyword is configured, it is validated against the value received in DM request. If this keyword is not configured, the input value is silently ignored. That is, the DM requests from unlisted or unauthenticated clients are silently discarded.

- **secret shared\_secret:** Specify the global shared secret key of the server.

## Verifying the Session Disconnect Feature Configuration

This section describes how to verify the configuration associated with the Session Disconnect feature.

To view the information about the RADIUS Dynamic Authorization Clients that are configured in the system, use the **show radius-dyn-auth** command.

The following is a sample output of the **show radius-dyn-auth** command.

```
[unknown] smf# show radius-dyn-auth
radius-dyn-auth
-----
IP: 209.165.200.227
-----
COA:
0 total-requests      0 inprocess-requests
  0 retry-request-drops 0 invalid-requests
  0 bad-authenticators  0 internal-errors
0 ack-sent            0 nak-sent
-----
DISCONNECT:
0 total-requests      0 inprocess-requests
  0 retry-request-drops 0 invalid-requests
  0 bad-authenticators  0 internal-errors
0 ack-sent            0 nak-sent
-----
UnknownTypesRcvd: 0
-----
```

## Configuring the CoA-NAS Interface

Use the following sample configuration to define Change of Authorization (CoA) NAS interface in the RADIUS endpoint.

```
config
  instance instance-id gr_instance_id
  endpoint radius
    interface coa-nas
      vip-ip ipv4_address vip-port port_number
    end
```

### NOTES:

- **endpoint radius:** Enter the RADIUS endpoint configuration mode.
- **interface coa-nas:** Enter the CoA NAS interface configuration mode. This keyword defines a new interface "coa-nas".
- **vip-ip ipv4\_address vip-port port\_number:** Specify the IP address of the host. *ipv4\_address* must be in standard IPv4 dotted decimal notation.

You can configure a list of VIP-IPs to listen to the inbound CoA or DM requests.

**vip-port port\_number:** Specify the port number of the UDP proxy. By default, the port number is 3799. This default value is used only when the VIP-IP is specified.




---

**Important** This configuration allows only port to be specified per IP.

---

The SMF (udp-pxy) listens to the inbound CoA or DM request messages on these ports, and ACK or NAK messages sent with the respective source IP and port.

# RADIUS Client OA&M Support

This section describes operations, administration, and maintenance information for this feature.

## Statistics Support

### RADIUS Authentication Statistics

This feature supports the following statistics related to RADIUS Authentication:

- SMF-Service:
  - Number of Secondary-Authentication requests sent
  - Number of Secondary-Authentication response received
- RADIUS-EP:
  - Number of Secondary-Authentication requests sent
  - Number of Secondary-Authentication response received
  - Number of RADIUS packets sent
  - Number of RADIUS packets received

## Troubleshooting Information

This section provides information on using the command line interface (CLI) commands, alerts, logs, and metrics for troubleshooting any RADIUS related issues that may arise during system operation.

## RADIUS Bulk Statistics

Use the following bulk statistics to monitor the failures or issues associated with RADIUS authentication, RADIUS accounting, and Disconnect Message requests.

[illegible]

1996  
 1997  
 1998  
 1999  
 2000  
 2001  
 2002  
 2003  
 2004  
 2005  
 2006  
 2007  
 2008  
 2009  
 2010  
 2011  
 2012  
 2013  
 2014  
 2015  
 2016  
 2017  
 2018  
 2019  
 2020  
 2021  
 2022  
 2023  
 2024  
 2025  
 2026  
 2027  
 2028  
 2029  
 2030  
 2031  
 2032  
 2033  
 2034  
 2035  
 2036  
 2037  
 2038  
 2039  
 2040  
 2041  
 2042  
 2043  
 2044  
 2045  
 2046  
 2047  
 2048  
 2049  
 2050  
 2051  
 2052  
 2053  
 2054  
 2055  
 2056  
 2057  
 2058  
 2059  
 2060  
 2061  
 2062  
 2063  
 2064  
 2065  
 2066  
 2067  
 2068  
 2069  
 2070  
 2071  
 2072  
 2073  
 2074  
 2075  
 2076  
 2077  
 2078  
 2079  
 2080  
 2081  
 2082  
 2083  
 2084  
 2085  
 2086  
 2087  
 2088  
 2089  
 2090  
 2091  
 2092  
 2093  
 2094  
 2095  
 2096  
 2097  
 2098  
 2099  
 2100  
 2101  
 2102  
 2103  
 2104  
 2105  
 2106  
 2107  
 2108  
 2109  
 2110  
 2111  
 2112  
 2113  
 2114  
 2115  
 2116  
 2117  
 2118  
 2119  
 2120  
 2121  
 2122  
 2123  
 2124  
 2125  
 2126  
 2127  
 2128  
 2129  
 2130  
 2131  
 2132  
 2133  
 2134  
 2135  
 2136  
 2137  
 2138  
 2139  
 2140  
 2141  
 2142  
 2143  
 2144  
 2145  
 2146  
 2147  
 2148  
 2149  
 2150  
 2151  
 2152  
 2153  
 2154  
 2155  
 2156  
 2157  
 2158  
 2159  
 2160  
 2161  
 2162  
 2163  
 2164  
 2165  
 2166  
 2167  
 2168  
 2169  
 2170  
 2171  
 2172  
 2173  
 2174  
 2175  
 2176  
 2177  
 2178  
 2179  
 2180  
 2181  
 2182  
 2183  
 2184  
 2185  
 2186  
 2187  
 2188  
 2189  
 2190  
 2191  
 2192  
 2193  
 2194  
 2195  
 2196  
 2197  
 2198  
 2199  
 2200  
 2201  
 2202  
 2203  
 2204  
 2205  
 2206  
 2207  
 2208  
 2209  
 2210  
 2211  
 2212  
 2213  
 2214  
 2215  
 2216  
 2217  
 2218  
 2219  
 2220  
 2221  
 2222  
 2223  
 2224  
 2225  
 2226  
 2227  
 2228  
 2229  
 2230  
 2231  
 2232  
 2233  
 2234  
 2235  
 2236  
 2237  
 2238  
 2239  
 2240  
 2241  
 2242  
 2243  
 2244  
 2245  
 2246  
 2247  
 2248  
 2249  
 2250  
 2251  
 2252  
 2253  
 2254  
 2255  
 2256  
 2257  
 2258  
 2259  
 2260  
 2261  
 2262  
 2263  
 2264  
 2265  
 2266  
 2267  
 2268  
 2269  
 2270  
 2271  
 2272  
 2273  
 2274  
 2275  
 2276  
 2277  
 2278  
 2279  
 2280  
 2281  
 2282  
 2283  
 2284  
 2285  
 2286  
 2287  
 2288  
 2289  
 2290  
 2291  
 2292  
 2293  
 2294  
 2295  
 2296  
 2297  
 2298  
 2299  
 2300  
 2301  
 2302  
 2303  
 2304  
 2305  
 2306  
 2307  
 2308  
 2309  
 2310  
 2311  
 2312  
 2313  
 2314  
 2315  
 2316  
 2317  
 2318  
 2319  
 2320  
 2321  
 2322  
 2323  
 2324  
 2325  
 2326  
 2327  
 2328  
 2329  
 2330  
 2331  
 2332  
 2333  
 2334  
 2335  
 2336  
 2337  
 2338  
 2339  
 2340  
 2341  
 2342  
 2343  
 2344  
 2345  
 2346  
 2347  
 2348  
 2349  
 2350  
 2351  
 2352  
 2353  
 2354  
 2355  
 2356  
 2357  
 2358  
 2359  
 2360  
 2361  
 2362  
 2363  
 2364  
 2365  
 2366  
 2367  
 2368  
 2369  
 2370  
 2371  
 2372  
 2373  
 2374  
 2375  
 2376  
 2377  
 2378  
 2379  
 2380  
 2381  
 2382  
 2383  
 2384  
 2385  
 2386  
 2387  
 2388  
 2389  
 2390  
 2391  
 2392  
 2393  
 2394  
 2395  
 2396  
 2397  
 2398  
 2399  
 2400  
 2401  
 2402  
 2403  
 2404  
 2405  
 2406  
 2407  
 2408  
 2409  
 2410  
 2411  
 2412  
 2413  
 2414  
 2415  
 2416  
 2417  
 2418  
 2419  
 2420  
 2421  
 2422  
 2423  
 2424  
 2425  
 2426  
 2427  
 2428  
 2429  
 2430  
 2431  
 2432  
 2433  
 2434  
 2435  
 2436  
 2437  
 2438  
 2439  
 2440  
 2441  
 2442  
 2443  
 2444  
 2445  
 2446  
 2447  
 2448  
 2449  
 2450

[illegible]

1. **Introduction**  
 2. **Background**  
 3. **Methodology**  
 4. **Results**  
 5. **Discussion**  
 6. **Conclusion**  
 7. **References**  
 8. **Appendix**  
 9. **Index**  
 10. **Table of Contents**  
 11. **Figure 1**  
 12. **Figure 2**  
 13. **Figure 3**  
 14. **Figure 4**  
 15. **Figure 5**  
 16. **Figure 6**  
 17. **Figure 7**  
 18. **Figure 8**  
 19. **Figure 9**  
 20. **Figure 10**  
 21. **Figure 11**  
 22. **Figure 12**  
 23. **Figure 13**  
 24. **Figure 14**  
 25. **Figure 15**  
 26. **Figure 16**  
 27. **Figure 17**  
 28. **Figure 18**  
 29. **Figure 19**  
 30. **Figure 20**  
 31. **Figure 21**  
 32. **Figure 22**  
 33. **Figure 23**  
 34. **Figure 24**  
 35. **Figure 25**  
 36. **Figure 26**  
 37. **Figure 27**  
 38. **Figure 28**  
 39. **Figure 29**  
 40. **Figure 30**  
 41. **Figure 31**  
 42. **Figure 32**  
 43. **Figure 33**  
 44. **Figure 34**  
 45. **Figure 35**  
 46. **Figure 36**  
 47. **Figure 37**  
 48. **Figure 38**  
 49. **Figure 39**  
 50. **Figure 40**  
 51. **Figure 41**  
 52. **Figure 42**  
 53. **Figure 43**  
 54. **Figure 44**  
 55. **Figure 45**  
 56. **Figure 46**  
 57. **Figure 47**  
 58. **Figure 48**  
 59. **Figure 49**  
 60. **Figure 50**  
 61. **Figure 51**  
 62. **Figure 52**  
 63. **Figure 53**  
 64. **Figure 54**  
 65. **Figure 55**  
 66. **Figure 56**  
 67. **Figure 57**  
 68. **Figure 58**  
 69. **Figure 59**  
 70. **Figure 60**  
 71. **Figure 61**  
 72. **Figure 62**  
 73. **Figure 63**  
 74. **Figure 64**  
 75. **Figure 65**  
 76. **Figure 66**  
 77. **Figure 67**  
 78. **Figure 68**  
 79. **Figure 69**  
 80. **Figure 70**  
 81. **Figure 71**  
 82. **Figure 72**  
 83. **Figure 73**  
 84. **Figure 74**  
 85. **Figure 75**  
 86. **Figure 76**  
 87. **Figure 77**  
 88. **Figure 78**  
 89. **Figure 79**  
 90. **Figure 80**  
 91. **Figure 81**  
 92. **Figure 82**  
 93. **Figure 83**  
 94. **Figure 84**  
 95. **Figure 85**  
 96. **Figure 86**  
 97. **Figure 87**  
 98. **Figure 88**  
 99. **Figure 89**  
 100. **Figure 90**  
 101. **Figure 91**  
 102. **Figure 92**  
 103. **Figure 93**  
 104. **Figure 94**  
 105. **Figure 95**  
 106. **Figure 96**  
 107. **Figure 97**  
 108. **Figure 98**  
 109. **Figure 99**  
 110. **Figure 100**  
 111. **Figure 101**  
 112. **Figure 102**  
 113. **Figure 103**  
 114. **Figure 104**  
 115. **Figure 105**  
 116. **Figure 106**  
 117. **Figure 107**  
 118. **Figure 108**  
 119. **Figure 109**  
 120. **Figure 110**  
 121. **Figure 111**  
 122. **Figure 112**  
 123. **Figure 113**  
 124. **Figure 114**  
 125. **Figure 115**  
 126. **Figure 116**  
 127. **Figure 117**  
 128. **Figure 118**  
 129. **Figure 119**  
 130. **Figure 120**  
 131. **Figure 121**  
 132. **Figure 122**  
 133. **Figure 123**  
 134. **Figure 124**  
 135. **Figure 125**  
 136. **Figure 126**  
 137. **Figure 127**  
 138. **Figure 128**  
 139. **Figure 129**  
 140. **Figure 130**  
 141. **Figure 131**  
 142. **Figure 132**  
 143. **Figure 133**  
 144. **Figure 134**  
 145. **Figure 135**  
 146. **Figure 136**  
 147. **Figure 137**  
 148. **Figure 138**  
 149. **Figure 139**  
 150. **Figure 140**  
 151. **Figure 141**  
 152. **Figure 142**  
 153. **Figure 143**  
 154. **Figure 144**  
 155. **Figure 145**  
 156. **Figure 146**  
 157. **Figure 147**  
 158. **Figure 148**  
 159. **Figure 149**  
 160. **Figure 150**  
 161. **Figure 151**  
 162. **Figure 152**  
 163. **Figure 153**  
 164. **Figure 154**  
 165. **Figure 155**  
 166. **Figure 156**  
 167. **Figure 157**  
 168. **Figure 158**  
 169. **Figure 159**  
 170. **Figure 160**  
 171. **Figure 161**  
 172. **Figure 162**  
 173. **Figure 163**  
 174. **Figure 164**  
 175. **Figure 165**  
 176. **Figure 166**  
 177. **Figure 167**  
 178. **Figure 168**  
 179. **Figure 169**  
 180. **Figure 170**  
 181. **Figure 171**  
 182. **Figure 172**  
 183. **Figure 173**  
 184. **Figure 174**  
 185. **Figure 175**  
 186. **Figure 176**  
 187. **Figure 177**  
 188. **Figure 178**  
 189. **Figure 179**  
 190. **Figure 180**  
 191. **Figure 181**  
 192. **Figure 182**  
 193. **Figure 183**  
 194. **Figure 184**  
 195. **Figure 185**  
 196. **Figure 186**  
 197. **Figure 187**  
 198. **Figure 188**  
 199. **Figure 189**  
 200. **Figure 190**  
 201. **Figure 191**  
 202. **Figure 192**  
 203. **Figure 193**  
 204. **Figure 194**  
 205. **Figure 195**  
 206. **Figure 196**  
 207. **Figure 197**  
 208. **Figure 198**  
 209. **Figure 199**  
 210. **Figure 200**  
 211. **Figure 201**  
 212. **Figure 202**  
 213. **Figure 203**  
 214. **Figure 204**  
 215. **Figure 205**  
 216. **Figure 206**  
 217. **Figure 207**  
 218

1. **1998**  
 2. **as**  
 3. **an**  
 4. **and**  
 5. **at**  
 6. **from**  
 7. **in**  
 8. **of**  
 9. **off**  
 10. **on**  
 11. **over**  
 12. **per**  
 13. **to**  
 14. **with**  
 15. **without**  
 16. **by**  
 17. **for**  
 18. **in**  
 19. **of**  
 20. **a**  
 21. **the**  
 22. **your**  
 23. **not**  
 24. **to**  
 25. **in**  
 26. **to**  
 27. **&**  
 28. **and**  
 29. **from**  
 30. **to**  
 31. **in**  
 32. **of**  
 33. **on**  
 34. **over**  
 35. **per**  
 36. **to**  
 37. **with**  
 38. **without**  
 39. **by**  
 40. **for**  
 41. **in**  
 42. **of**  
 43. **a**  
 44. **the**  
 45. **your**  
 46. **not**  
 47. **to**  
 48. **in**  
 49. **to**  
 50. **&**

**Abstract**

**Table 11: RADIUS Accounting Message (Per SMF service)**

1. **Introduction**  
 2. **Background**  
 3. **Methodology**  
 4. **Results**  
 5. **Discussion**  
 6. **Conclusion**  
 7. **References**  
 8. **Appendix**  
 9. **Index**  
 10. **Table of Contents**  
 11. **Abstract**  
 12. **Summary**  
 13. **Key Words**  
 14. **Keywords**  
 15. **Subject Headings**  
 16. **Classification**  
 17. **Indexing**  
 18. **References**  
 19. **Appendix**  
 20. **Index**  
 21. **Table of Contents**  
 22. **Abstract**  
 23. **Summary**  
 24. **Key Words**  
 25. **Keywords**  
 26. **Subject Headings**  
 27. **Classification**  
 28. **Indexing**  
 29. **References**  
 30. **Appendix**  
 31. **Index**  
 32. **Table of Contents**  
 33. **Abstract**  
 34. **Summary**  
 35. **Key Words**  
 36. **Keywords**  
 37. **Subject Headings**  
 38. **Classification**  
 39. **Indexing**  
 40. **References**  
 41. **Appendix**  
 42. **Index**  
 43. **Table of Contents**  
 44. **Abstract**  
 45. **Summary**  
 46. **Key Words**  
 47. **Keywords**  
 48. **Subject Headings**  
 49. **Classification**  
 50. **Indexing**  
 51. **References**  
 52. **Appendix**  
 53. **Index**  
 54. **Table of Contents**  
 55. **Abstract**  
 56. **Summary**  
 57. **Key Words**  
 58. **Keywords**  
 59. **Subject Headings**  
 60. **Classification**  
 61. **Indexing**  
 62. **References**  
 63. **Appendix**  
 64. **Index**  
 65. **Table of Contents**  
 66. **Abstract**  
 67. **Summary**  
 68. **Key Words**  
 69. **Keywords**  
 70. **Subject Headings**  
 71. **Classification**  
 72. **Indexing**  
 73. **References**  
 74. **Appendix**  
 75. **Index**  
 76. **Table of Contents**  
 77. **Abstract**  
 78. **Summary**  
 79. **Key Words**  
 80. **Keywords**  
 81. **Subject Headings**  
 82. **Classification**  
 83. **Indexing**  
 84. **References**  
 85. **Appendix**  
 86. **Index**  
 87. **Table of Contents**  
 88. **Abstract**  
 89. **Summary**  
 90. **Key Words**  
 91. **Keywords**  
 92. **Subject Headings**  
 93. **Classification**  
 94. **Indexing**  
 95. **References**  
 96. **Appendix**  
 97. **Index**  
 98. **Table of Contents**  
 99. **Abstract**  
 100. **Summary**  
 101. **Key Words**  
 102. **Keywords**  
 103. **Subject Headings**  
 104. **Classification**  
 105. **Indexing**  
 106. **References**  
 107. **Appendix**  
 108. **Index**  
 109. **Table of Contents**  
 110. **Abstract**  
 111. **Summary**  
 112. **Key Words**  
 113. **Keywords**  
 114. **Subject Headings**  
 115. **Classification**  
 116. **Indexing**  
 117. **References**  
 118. **Appendix**  
 119. **Index**  
 120. **Table of Contents**  
 121. **Abstract**  
 122. **Summary**  
 123. **Key Words**  
 124. **Keywords**  
 125. **Subject Headings**  
 126. **Classification**  
 127. **Indexing**  
 128. **References**  
 129. **Appendix**  
 130. **Index**  
 131. **Table of Contents**  
 132. **Abstract**  
 133. **Summary**  
 134. **Key Words**  
 135. **Keywords**  
 136. **Subject Headings**  
 137. **Classification**  
 138. **Indexing**  
 139. **References**  
 140. **Appendix**  
 141. **Index**  
 142. **Table of Contents**  
 143. **Abstract**  
 144. **Summary**  
 145. **Key Words**  
 146. **Keywords**  
 147. **Subject Headings**  
 148. **Classification**  
 149. **Indexing**  
 150. **References**  
 151. **Appendix**  
 152. **Index**  
 153. **Table of Contents**  
 154. **Abstract**  
 155. **Summary**  
 156. **Key Words**  
 157. **Keywords**  
 158. **Subject Headings**  
 159. **Classification**  
 160. **Indexing**  
 161. **References**  
 162. **Appendix**  
 163. **Index**  
 164. **Table of Contents**  
 165. **Abstract**  
 166. **Summary**  
 167. **Key Words**  
 168. **Keywords**  
 169. **Subject Headings**  
 170. **Classification**  
 171. **Indexing**  
 172. **References**  
 173. **Appendix**  
 174. **Index**  
 175. **Table of Contents**  
 176. **Abstract**  
 177. **Summary**  
 178. **Key Words**  
 179. **Keywords**  
 180. **Subject Headings**  
 181. **Classification**  
 182. **Indexing**  
 183. **References**  
 184. **Appendix**  
 185. **Index**  
 186. **Table of Contents**  
 187. **Abstract**  
 188. **Summary**  
 189. **Key Words**  
 190. **Keywords**  
 191. **Subject Headings**  
 192. **Classification**  
 193. **Indexing**  
 194. **References**  
 195. **Appendix**  
 196. **Index**  
 197. **Table of Contents**  
 198. **Abstract**  
 199. **Summary**  
 200. **Key Words**  
 201. **Keywords**  
 202. **Subject Headings**  
 203. **Classification**  
 204. **Indexing**  
 205. **References**  
 206. **Appendix**  
 207. **Index**  
 208. **Table of Contents**  
 209. **Abstract**  
 210. **Summary**  
 211. **Key Words**  
 212. **Keywords**  
 213. **Subject Headings**  
 214. **Classification**  
 215. **Indexing**  
 216. **References**  
 217. **Appendix**  
 218. **Index**  
 219. **Table of Contents**  
 220. **Abstract**  
 221. **Summary**  
 222. **Key Words**  
 223. **Keywords**  
 224. **Subject Headings**  
 225. **Classification**  
 226. **Indexing**  
 227. **References**  
 228. **Appendix**  
 229. **Index**  
 230. **Table of Contents**  
 231. **Abstract**  
 232. **Summary**  
 233. **Key Words**  
 234. **Keywords**  
 235. **Subject Headings**  
 236. **Classification**  
 237. **Indexing**  
 238. **References**  
 239. **Appendix**  
 240. **Index**  
 241. **Table of Contents**  
 242. **Abstract**  
 243. **Summary**  
 244. **Key Words**  
 245. **Keywords**  
 246. **Subject Headings**  
 247. **Classification**  
 248. **Indexing**  
 249. **References**  
 250. **Appendix**  
 251. **Index**  
 252. **Table of Contents**  
 253. **Abstract</**

[illegible]

[illegible]

[illegible]**Table 12: Disconnect Message**[illegible]

[illegible]

|     |     |
|-----|-----|
| IBQ | IBQ |
| IBQ | IBQ |
| IBQ | IBQ |

| Category               | Item                | Value                                                  |
|------------------------|---------------------|--------------------------------------------------------|
| 1. General Information | Name                | John Doe                                               |
|                        | Age                 | 35                                                     |
|                        | Gender              | Male                                                   |
|                        | Occupation          | Software Engineer                                      |
|                        | Education           | Master's Degree                                        |
|                        | Marital Status      | Single                                                 |
|                        | Address             | 123 Main St, New York, NY 10001                        |
|                        | Phone Number        | (212) 555-1234                                         |
|                        | Email Address       | john.doe@example.com                                   |
|                        | Emergency Contact   | John Doe (212) 555-1234                                |
| 2. Employment History  | Company Name        | ABC Corporation                                        |
|                        | Position            | Senior Software Engineer                               |
|                        | Start Date          | 2018-01-15                                             |
|                        | End Date            | 2023-06-30                                             |
|                        | Reason for Leaving  | Seeking new challenges                                 |
|                        | Supervisor          | Jane Smith                                             |
|                        | Key Projects        | Developed new web application                          |
|                        | Performance Rating  | Excellent                                              |
|                        | References          | John Doe (212) 555-1234                                |
|                        | Additional Comments | Strong team player, excellent communication skills     |
| 3. Education Details   | Institution         | University of California, Berkeley                     |
|                        | Degree              | Master of Science in Computer Science                  |
|                        | Year Graduated      | 2015                                                   |
|                        | Thesis Topic        | Advanced Algorithms for Data Structures                |
|                        | Advisor             | Prof. Dr. Jane Smith                                   |
|                        | Grade               | A                                                      |
|                        | Relevant Courses    | Algorithms, Data Structures, Operating Systems         |
|                        | Publications        | Published research paper on data structures            |
|                        | Recommendations     | John Doe (212) 555-1234                                |
|                        | Additional Comments | Excellent academic performance, strong research skills |

## Subscriber Details for RADIUS-specific Information

The **show subscriber supi supi\_id nf-service smf full** CLI command displays the subscriber details for RADIUS-specific use cases.

```
[unknown] smf# show subscriber supi imsi-123456789012345 nf-service smf
full
subscriber-details
{
...
"alwaysOn": "None",
  "dcnr": "None",
  "wps": "Wps Session",
  "ratType": "NR",
  "idleTimeout": 600,          << can be overwritten from Radius in Auth Resp
  "sessTimeout": 1200,       << can be overwritten from Radius in Auth Resp
  "radiusEpInfo": "209.165.200.228:1812",
  "authAlg": "pap-default",
  "authStatus": "Authenticated"
...
...
  "accountingEnabled": "true",
  "n40ChargingEnabled": "true",
  "acctSessId": "198.15.1.40016777221"
...
...
"upfServData": {
  "numberOfTunnels": 2,
  "smfSeid": 72057615828912656,
  "UPState": "Activated",
  "urrInfo": [
    {
      "id": 2147483657,
      "chgName": "radiusurr",
      "method": {
        "duration": "false",
        "volume": "true",
        "event": "false"
      }
    }
  ],
}
```

## RADIUS Endpoint Authentication and Accounting Statistics

The **show radius** CLI command displays statistics for RADIUS Authentication and Accounting from RADIUS endpoint.

```
[unknown] smf# show radius
radius
-----
Server: 209.165.200.240, port: 1812, status: up, port-type: Auth
3 requests, 0 pending, 0 retransmits
2 accepts, 0 rejects, 1 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 1 ms latest rtt
-----
Server: 209.165.200.234, port: 1813, status: up, port-type: Acct
3 requests, 0 pending, 6 retransmits
```

```

0 responses, 3 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt
-----
Server: 209.165.200.245, port: 1813, status: up, port-type: Acct
5 requests, 0 pending, 3 retransmits
3 responses, 2 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 6 ms latest rtt
-----
[unknown] smf#

[unknown] smf# show radius acct-server
-----
Server: 209.165.200.234, port: 1813, status: up, port-type: Acct
3 requests, 0 pending, 6 retransmits
0 responses, 3 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt
-----
Server: 209.165.200.240, port: 1813, status: up, port-type: Acct
5 requests, 0 pending, 3 retransmits
3 responses, 2 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 6 ms latest rtt
-----
[unknown] smf#

[unknown] smf# show radius auth-server
-----
Server: 209.165.200.243, port: 1812, status: up, port-type: Auth
3 requests, 0 pending, 0 retransmits
2 accepts, 0 rejects, 1 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 1 ms latest rtt
-----
[unknown] smf#

```

## RADIUS Endpoint Disconnect Message and CoA Statistics

The **show radius-dyn-auth** CLI command displays statistics for RADIUS Disconnect Message and CoA from RADIUS endpoint.

```

[unknown] smf# show radius-dyn-auth
radius-dyn-auth
-----
IP: 209.165.201.20
-----
COA:
0 total-requests      0 inprocess-requests
  0 retry-request-drops 0 invalid-requests
  0 bad-authenticators  0 internal-errors
0 ack-sent            0 nak-sent
-----
DISCONNECT:
2 total-requests      0 inprocess-requests
  0 retry-request-drops 0 invalid-requests
  0 bad-authenticators  0 internal-errors
1 ack-sent            1 nak-sent
-----
UnknownTypesRcvd: 0
-----
[unknown] smf#

```

## External Inbound and Outbound Connections

The **show peers all** CLI command fetches the list of external inbound and outbound connections established by the SMF.

```
[unknown] smf# show peers all | include radius
```

```
RadiusServer - 209.165.202.145:1813 Outbound radius-ep-0 Udp 18 hours Radius
Status: Active,Type: Acct 1
RadiusServer - 209.165.201.20:1812 Outbound radius-ep-0 Udp 17 hours Radius
Status: Active,Type: Auth 1
RadiusServer - 209.165.201.20:1813 Outbound radius-ep-0 Udp 17 hours Radius
Status: Active,Type: Acct 1
[unknown] smf#
```



### Important

During application startup or configuration updates, RADIUS endpoint sends test authentication and accounting requests to check the status of RADIUS server peer. The output of the **show peers** command displays the peer status result.

The results of these dummy requests will be overwritten by the outcomes of actual authentication and accounting requests.

## Internal and External Connections

The **show endpoint info** CLI command fetches the list of internal and external connections established by the SMF.

```
[unknown] smf# show endpoint all | include radius
```

```
Radius:209.165.201.4: 209.165.201.1:3799 Udp Started RADIUS false 18
hours <none> 1
[unknown] smf#
```

## Status of Pods

The **show running-status** CLI command fetches the current status of pods. This function is analogous to the K8 **kubectl get pods -n <>** CLI command.

```
[unknown] smf# show running-status | include radius
```

```
radius-ep-0 Started 19 hours
[unknown] smf#
```

## Configuration Errors

The **show config-error** CLI command displays the validation criteria — Pass or Failed. The Pass criteria appears when no entries exist.

```
[unknown] smf# show config-error | include radius
```

```
[unknown] smf#
```

## show alerts

This section provides the sample output for different variants of the **show alerts** CLI command.

**show alerts | include radius**

```

alerts history radius_test cfb253587397
alerts history radius_test 911f84aff47c
alerts history radius_test 3ed7a5112905
alerts history radius_test 292af807b299
  source      radius-ep-n0-0
  labels      [ "namespace: smf" "pod: radius-ep-n0-0" ]
  annotations [ "summary: Container:  of pod: radius-ep-n0-0 in namespace: smf has been
restarted." ]
  source      radius-ep-n0-0
  labels      [ "name: k8s_radius-ep_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0"
"namespace: smf" "pod: radius-ep-n0-0" ]
  annotations [ "summary: Container:
k8s_radius-ep_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
in namespace: smf has been restarted." ]
  source      radius-ep-n0-0
  labels      [ "name: k8s_POD_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0"
"namespace: smf" "pod: radius-ep-n0-0" ]
  annotations [ "summary: Container:
k8s_POD_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
in namespace: smf has been restarted." ]
alerts history radius_test 1c17e31c13f9
alerts history radius_test ffaabf0e0929
  source      radius-ep-n0-0
  labels      [ "name: k8s_POD_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0"
"namespace: smf" "pod: radius-ep-n0-0" ]
  annotations [ "summary: Container:
k8s_POD_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
in namespace: smf has been restarted." ]
  source      radius-ep-n0-0
  labels      [ "namespace: smf" "pod: radius-ep-n0-0" ]
  annotations [ "summary: Container:
k8s_radius-ep_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
in namespace: smf has been restarted." ]
[unknown] cee#

```

**show alerts active detail | include radius**

```

alerts active detail Radius_Server_Down 0fe030aba3ce
  summary "Radius Server: 209.165.201.20, Port: 1813 in namespace: smf is DOWN for more
than 15min."
alerts active detail Radius_Server_Down 6f41c340311c
  summary "Radius Server: 209.165.202.145, Port: 1813 in namespace: smf is DOWN for more
than 15min."
alerts active detail Radius_Server_Down 8a290c5ed1de
  summary "Radius Server: 209.165.201.20, Port: 1812 in namespace: smf is DOWN for more
than 15min."
[unknown] cee#
[unknown] cee#
alerts active detail Radius_Server_Down 0fe030aba3ce
  severity major
  type "Processing Error Alarm"
  startsAt 2020-12-11T13:30:16.874Z
  source System
  summary "Radius Server: 209.165.201.20, Port: 1813 in namespace: smf is DOWN for more
than 15min."
  labels [ "namespace: smf" "radSvrIP: 209.165.201.20" "radSvrPort: 1813" ]
alerts active detail Radius_Server_Down 6f41c340311c

```

```

severity major
type      "Processing Error Alarm"
startsAt  2020-12-11T13:30:16.874Z
source    System
summary   "Radius Server: 209.165.202.145, Port: 1813 in namespace: smf is DOWN for more
than 15min."
labels    [ "namespace: smf" "radSvrIP: 209.165.202.145" "radSvrPort: 1813" ]
alerts active detail Radius_Server_Down 8a290c5ed1de
severity major
type      "Processing Error Alarm"
startsAt  2020-12-11T13:30:16.874Z
source    System
summary   "Radius Server: 209.165.201.20, Port: 1812 in namespace: smf is DOWN for more
than 15min."
labels    [ "namespace: smf" "radSvrIP: 209.165.201.20" "radSvrPort: 1812" ]

[unknown] cee# show alerts active summary | include RTT
Radius_Server_RTT      1d0353b3db82 major      12-11T15:10:16 System RTT for Radius
Server: 209.165.201.20, Port: 1812 in namespace: smf is more than 5 ms.
[unknown] cee#

```

### show alerts active summary | include RTT

```

Radius_Server_RTT      1d0353b3db82 major      12-11T15:10:16 System RTT for Radius Server:
209.165.201.20, Port: 1812 in namespace: smf is more than 5 ms.
[unknown] cee#

```

### show alerts active summary | include radius

```

Radius_Server_RTT      1d0353b3db82 major      12-11T15:10:16 System RTT
for Radius Server: 209.165.201.20, Port: 1812 in namespace: smf is more than 5 ms.
Radius_Acct_Establish  520d9943d53f major      12-11T15:05:16 System This
alert is fired when the percentage of successful Radius Accounting Establish responses
received is lesser than threshold
Radius_Server_Down     0fe030aba3ce major      12-11T13:30:16 System Radius
Server: 209.165.201.20, Port: 1813 in namespace: smf is DOWN for more than 15min.
Radius_Server_Down     6f41c340311c major      12-11T13:30:16 System Radius
Server: 209.165.202.145, Port: 1813 in namespace: smf is DOWN for more than 15min.
Radius_Server_Down     8a290c5ed1de major      12-11T13:30:16 System Radius
Server: 209.165.201.20, Port: 1812 in namespace: smf is DOWN for more than 15min.

```

## RADIUS Alerts

The RADIUS endpoint for MVNO or PAPN flow supports new alerts. Following sections describe some basic alerts. These alerts can be enhanced based on RAT or as required by the users.




---

**Important** These alerts are configurable only through the CEE Ops-center CLI.

---

## RADIUS EP Down Alert

Use the following example to configure alerts related to RADIUS EP Down.

```

alerts rules group RadiusEP
  rule Radius_Server_Down
    expression "sum by (namespace, radSvrIP, radSvrPort)
(Radius_Server_Status{radSvrPortType=~\"Auth|Acct\"} < 1)"
    duration 15m

```

```

severity    major
type        "Processing Error Alarm"
annotation summary
value "\"Radius Server: {{ $labels.radSvrIP }}, Port: {{ $labels.radSvrPort }} in namespace:
{{ $labels.namespace }} is DOWN for more than 15min.\"""
exit
exit

```

## RADIUS Accounting Establishment Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Accounting Establishment Failure threshold.

```

alerts rules group RadiusEP
  rule Radius_Acct_Establish_SR
    expression "sum by (namespace)
    (increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
Establishment\", radPacketType=\"Rx\", radResult=\"Success\"}[5m])) / sum by (namespace)
    (increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
Establishment\", radPacketType=\"Tx\"}[5m])) < 0.80"
    severity    major
    type        "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of successful Radius Accounting Establish
responses received is lesser than threshold"
    exit
    exit

```

## RADIUS Accounting Release Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Accounting Release Failure threshold.

```

rule Radius_Acct_Release_SR
  expression "sum by (namespace)
  (increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
Release\", radPacketType=\"Rx\", radResult=\"Success\"}[5m])) / sum by (namespace)
  (increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
Release\", radPacketType=\"Tx\"}[5m])) < 0.80"
  severity    major
  type        "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of successful Radius Accounting Release
responses received is lesser than threshold"
  exit
  exit

```

## RADIUS Authentication Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Authentication Failure threshold.

```

rule Radius_Auth_SR
  expression "sum by (namespace)
  (increase(Radius_Requests_Statistics{radMsgCode=\"SecondaryAuthenReq\", procType=\"PDU
Session Establishment\", radPacketType=\"Rx\", radResult=\"Success\"}[5m])) / sum by
(namespace) (increase(Radius_Requests_Statistics{radMsgCode=\"SecondaryAuthenReq\",
procType=\"PDU Session Establishment\", radPacketType=\"Tx\"}[5m])) < 0.80"
  severity    major
  type        "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of successful Radius Authentication
Request responses received is lesser than threshold"

```

```
exit
exit
```

## RADIUS Disconnect Message Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Disconnect Message Failure threshold.

```
rule Radius_Disconnect_Message_SR
  expression "sum by (namespace)
(increase(Radius_CoaDM_Requests_Statistics{radMsgCode=\"DisconnectACK\", radPacketType=\"Tx\",
radResult=\"Success\"}[5m])) / sum by
(namespace) (increase(Radius_CoaDM_Requests_Statistics{radMsgCode=\"DisconnectRequest\",
radPacketType=\"Rx\"}[5m])) < 0.80"
  severity    major
  type        "Communications Alarm"
  annotation summary
    value "This alert is fired when the percentage of successful Disconnect Message (DM)
responses sent is lesser than threshold"
  exit
  exit
exit
```

## RADIUS Server RTT Alert

Use the following example to configure alerts related to RADIUS server RTT.

```
rule Radius_Server_RTT
  expression "sum by (namespace, radSvrIP, radSvrPort)
(Radius_Server_Rtt_ms{radSvrPortType=~\"Auth|Acct\"} > 5)"
  duration    15m
  severity    warning
  type        "Communications Alarm"
  annotation summary
    value "\"RTT for Radius Server: {{ $labels.radSvrIP }}, Port: {{ $labels.radSvrPort }}"
in namespace: {{ $labels.namespace }} is more than 5 ms.\""
  exit
  exit
exit
```

## RADIUS Accounting Start Initial Message Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Accounting Start Initial Message Failure threshold.

```
rule Radius_Acct_Start_SR
  expression "sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_initial\",
status=\"success\"}[5m])) / sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_initial\",
status=\"attempted\"}[5m])) < 0.80"
  severity    major
  type        "Processing Error Alarm"
  annotation summary
    value "This service based alert is fired when the percentage of successful Radius
Accounting Start successful response received is lesser than threshold"
  exit
  exit
exit
```

## RADIUS Accounting Interim/Update Message Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Accounting Interim/Update Message Failure threshold.

```

rule Radius_Acct_Interim_SR
    expression "sum by (namespace)
    (increase(radius_accounting_message_stats{procedure_type=\"radius_update\",
    status=\"success\"}[5m])) / sum by (namespace)
    (increase(radius_accounting_message_stats{procedure_type=\"radius_update\",
    status=\"attempted\"}[5m])) < 0.80"
    severity    major
    type        "Processing Error Alarm"
    annotation summary
    value "This service based alert is fired when the percentage of successful Radius
    Accounting Interim Update successful response received is lesser than threshold"
    exit
    exit

```

## RADIUS Accounting Stop/Terminate Message Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Accounting Stop/Terminate Message Failure threshold.

```

rule Radius_Acct_Stop_SR
    expression "sum by (namespace)
    (increase(radius_accounting_message_stats{procedure_type=\"radius_terminate\",
    status=\"success\"}[5m])) / sum by (namespace)
    (increase(radius_accounting_message_stats{procedure_type=\"radius_terminate\",
    status=\"attempted\"}[5m])) < 0.80"
    severity    major
    type        "Processing Error Alarm"
    annotation summary
    value "This service based alert is fired when the percentage of successful Radius
    Accounting Stop successful response received is lesser than threshold"
    exit
    exit

```

## RADIUS Authentication Type Message Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Authentication Type Message Failure threshold.

```

rule Radius_Auth_Type_SR
    expression "sum by (namespace, radius_auth_algorithm)
    (increase(radius_authentication_message_stats{radius_auth_algorithm=\"radius_auth_algorithm.*\",
    status=\"success\"}[1m])) / sum by (namespace)
    (increase(radius_authentication_message_stats{radius_auth_algorithm=\"radius_auth_algorithm.*\",
    status=\"attempted\"}[1m])) < 0.80"
    severity    major
    type        "Processing Error Alarm"
    annotation summary
    value "This alert is fired when the percentage of successful Radius Auth Type response
    received is lesser than threshold"
    exit
    exit

```

## Grafana Charts

The Grafana charts are used for monitoring based on the RADIUS endpoint or Service endpoint.

- RADIUS endpoint for call flows involving RADIUS Authentication, Accounting, and Disconnect Message.
- Service endpoint for accounting flows specific to Accounting Initial, Interim, or Terminate packets.

## Error Logs

This section explains the basic error conditions and the related logs to debug the failures.

### RADIUS Authentication

#### Authentication Request Not Responded by Server

The following is an error log for RADIUS Authentication Request not responded by the RADIUS server.

```
[smf-service-n0-0] 2020/09/17 07:14:52.921 smf-service [ERROR] [GenericAAA.go:786]
[smf-service0.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [16] Secondary
Authentication Failed: TIMEOUT
[smf-service-n0-0] *errors.errorString Secondary Authentication Failed: TIMEOUT
[smf-service-n0-0] /opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:621 (0xd89cae)
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/procedures/generic/GenericAAA.go:786 (0x144fa52)
```

#### Call Failure at Authentication Stage

The following is a sample error log for call failure at the RADIUS authentication stage.

```
[smf-service-n0-0]
[smf-service-n0-0] 2020/09/17 07:14:52.921 smf-service [ERROR] [idlestate.go:504]
[smf-service0.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [16]
USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED
[smf-service-n0-0] *errors.errorString USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED
[smf-service-n0-0] /opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:621 (0xd89cae)
[smf-service-n0-0] /opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:580 (0x15d7ddc)
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/procedures/4g/pdnsetup/idlestate.go:537 (0x15bc4f5)
```

#### Authentication Request Rejected by RADIUS Server

The following is an error log for RADIUS Authentication Request rejected by RADIUS server.

```
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [INFO] [idlestate.go:649]
[smf-service.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [1] Processing
Secondary Authentication Response
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [ERROR] [GenericAAA.go:1173]
[smf-service.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [1] Secondary
Authentication Failed: REJECT
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [DEBUG] [Genericutil.go:681]
[smf-service.smf-app.gen] Internal Transaction Submit with BP for MessageType: 118, SLA: 0

[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [DEBUG] [idlestate.go:169]
[smf-service.smf-app.gen] inCallStatus:9
```

```
*****
Transaction Log received from Instance: smf.radius-ep.ajay-smf1.smf.0
***** TRANSACTION: 00004 *****
TRANSACTION SUCCESS:
    Txn Type           : SecondaryAuthenReq(2004)
    Priority            : 1
    Session State       : No_Session
LOG MESSAGES:
    2020/12/09 09:20:13.756 [TRACE] [infra.message_log.core] >>>>>>>
```

```

2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Starting smf AccessRequest
2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Starting smf AccessRequest for User
[msisdn-9884886688]
2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Created new Radius Message for smf
AccessRequest
2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Selected server: 209.165.200.229:1812
, nasIP: 209.165.200.237 PID: 4194304
2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Sending an IPC Message to UDP proxy
[198.18.1.4]
2020/12/09 09:20:13.763 [DEBUG] [Radius.smf.AAA] PID: 4194304 - Response received on
channel
2020/12/09 09:20:13.763 [DEBUG] [Radius.smf.AAA] Authentication Result for user
[8899776655] = [REJECT]
2020/12/09 09:20:13.764 [TRACE] [infra.message_log.core] <<<<<<<<

*****

```

## Authentication Response with Incorrect Authenticator

The following is an error log for RADIUS Authentication Response with incorrect authenticator.

```

[radius-ep-n0-0] ***** TRANSACTION: 00044 *****
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0] Txn Type : RadiusUdpProxyMsg(2002)
[radius-ep-n0-0] Priority : 1
[radius-ep-n0-0] Session State : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0] 2020/12/09 13:20:38.874 [TRACE] [infra.message_log.core] >>>>>>>
[radius-ep-n0-0] 2020/12/09 13:20:38.874 [DEBUG] [Radius.smf.AAA] Response received
from udp proxy
[radius-ep-n0-0] 2020/12/09 13:20:38.874 [DEBUG] [Radius.smf.AAA] SrcIp: 209.165.201.20
SrcPort: 1812 DestIp: 209.165.201.4 DestPort: 16384
[radius-ep-n0-0] 2020/12/09 13:20:38.874 [ERROR] [Radius.smf.AAA] PID: 4194310 - Packet
dropped due to invalid authenticator
[radius-ep-n0-0] 2020/12/09 13:20:38.874 [TRACE] [infra.message_log.core] <<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] *****

```

## RADIUS Accounting

### Accounting Request Timeout

The following is an error log for RADIUS Accounting Request timeout.

```

[radius-ep-n0-0] ***** TRANSACTION: 00027 *****
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0] Txn Type : IntSmfAcctReqMsg(3)
[radius-ep-n0-0] Priority : 1
[radius-ep-n0-0] Session State : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0] 2020/12/09 13:09:10.247 [TRACE] [infra.message_log.core] >>>>>>>
[radius-ep-n0-0] 2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Starting smf
AccountingRequest
[radius-ep-n0-0] 2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Starting smf
AccountingRequest for User [msisdn-9884886688]
[radius-ep-n0-0] 2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Created new Radius
Message for smf AccountingRequest
[radius-ep-n0-0] 2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Selected server:
209.165.201.20:1813 , nasIP: 209.165.201.4 PID: 4194304
[radius-ep-n0-0] 2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Sending an IPC Message

```

```

to UDP proxy [209.165.201.4]
[radius-ep-n0-0] 2020/12/09 13:09:15.091 [DEBUG] [Radius.smf.AAA] PID: 4194304 - Response
received on channel
[radius-ep-n0-0] 2020/12/09 13:09:15.091 [ERROR] [Radius.smf.AAA] Retried MaxNumber of
times without success
[radius-ep-n0-0] 2020/12/09 13:09:15.092 [DEBUG] [Radius.smf.AAA] Int-txn Accounting
Result for user [9884886688] = [TIMEOUT]
[radius-ep-n0-0] 2020/12/09 13:09:15.092 [TRACE] [infra.message_log.core] <<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] *****

```

## Idle Timeout-based Release

### Idle Timeout Received from RADIUS

The following is a sample error log for idle timeout received from RADIUS.

```

[smf-service-n0-0] 2020/09/23 16:10:11.965 smf-service [DEBUG]
[Genericutil.go:7158] [smf-service.smf-app.gen] Idle timeout value received from Radius:
10
[smf-service-n0-0] 2020/09/23 16:10:11.965 smf-service [DEBUG]
[Genericutil.go:7168] [smf-service.smf-app.gen] Starting cp idle timer with timeout value:
10

```

### Absolute Session Timeout Received from RADIUS

The following is a sample error log for absolute session timeout received from RADIUS.

```

[smf-service-n0-0] 2020/09/23 16:10:11.964 smf-service [DEBUG]
[Genericutil.go:7200] [smf-service.smf-app.gen] Session absolute timeout value
received from Radius: 200

```

### Session Cleanup

The following is a sample error log for session cleanup.

```

[smf-service-n0-0] 2020/09/23 16:10:21.966 smf-service [WARN] [stateHandler.go:187]
[smf-service.smf-app.gen] [imsi-123456789012345:5] [imsi-123456789012345:5] [21]
TIMEOUT -- Cp Idle Session Timer Expired, Triggering release

```

## Disconnect Message

### Disconnect Message Received from Unknown Client

The following is a sample error log when disconnect message is received from an unknown client.

```

[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [INFO] [processor.go:157] [Radius.smf.Ipc]
Process continue - 2003
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [DEBUG] [coa.go:23] [Radius.smf.AAA] []
[] [11] Coa/Disconnect Req received from udp proxy
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [DEBUG] [coa.go:43] [Radius.smf.AAA] []
[] [11] SrcIp: 209.165.201.20 SrcPort: 3799 DestIp: 209.165.201.4 DestPort: 3799
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [ERROR] [coa.go:253] [Radius.smf.Ipc]
Bng Coa/Disconnect req failed - Invalid Coa Client 209.165.201.20
.
.
.
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [TRACE] [infra.message_log.core] >>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [DEBUG] [Radius.smf.AAA] Coa/Disconnect Req received
from udp proxy

```

```
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [DEBUG] [Radius.smf.AAA] SrcIp: 209.165.201.20
SrcPort: 3799 DestIp: 209.165.201.4 DestPort: 3799
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [ERROR] [Radius.smf.AAA] Unable to process
Coa/Disconnect request - Error during init of Radius Message Invalid Coa Client 209.165.201.20
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [TRACE] [infra.message_log.core] <<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] *****
```

### Disconnect Message Received with Invalid Session ID Key

The following is a sample error log when disconnect message is received with invalid session ID key.

```
[radius-ep-n0-0] ***** TRANSACTION: 00009 *****
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0] Txn Type : RadiusUdpProxyCoaMsg(2003)
[radius-ep-n0-0] Priority : 1
[radius-ep-n0-0] Session State : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0] 2020/11/25 10:49:43.942 [TRACE] [infra.message_log.core] >>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0] 2020/11/25 10:49:43.942 [DEBUG] [Radius.smf.AAA] Coa/Disconnect Req
received from udp proxy
[radius-ep-n0-0] 2020/11/25 10:49:43.942 [DEBUG] [Radius.smf.AAA] SrcIp: 209.165.201.20
SrcPort: 3799 DestIp: 209.165.201.4 DestPort: 3799
[radius-ep-n0-0] 2020/11/25 10:49:43.942 [DEBUG] [Radius.smf.AAA] Decoded coa message
type is DisconnectRequest
[radius-ep-n0-0] 2020/11/25 10:49:43.942 [ERROR] [Radius.smf.AAA] Unable to process
DisconnectRequest - Error during construct Invalid DNN/IPv4Addr/IPv6Pfx value
[radius-ep-n0-0] 2020/11/25 10:49:43.942 [TRACE] [infra.message_log.core] <<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] *****
```

## RADIUS Test CLI support

The **RADIUS test** CLI provides a mechanism for testing network connectivity with and configuration of RADIUS authentication and accounting servers.

This functionality is useful in determining the accuracy of the system RADIUS configuration, the configuration of the subscriber profile on the RADIUS server and troubleshooting the server response time.

### Testing a RADIUS Accounting Server

When used to test a RADIUS accounting server, the tool generates an accounting request message for a specific username.



**Note** The user name must already be configured on the RADIUS authentication server prior to executing the test.

To execute the RADIUS authentication test tool, enter the following command:

```
test-radius accounting { all | server-group group_name | server
server_ip_address port server_port } { client-nas client_nas_ip_address | grinstanceid
gr_instanceID | username user_name }
```

#### NOTES:

- **all**: Specify that all configured RADIUS accounting servers be tested.

- **server-group** *group\_name*: Specify the configured RADIUS authentication servers in a RADIUS server group named *group\_name* for server group functionality.
- **server** *server\_ip\_address*: Specify the IP address of a specific RADIUS accounting server to test.
- *server\_port*: Specify the TCP port over that the system must use when communicating with the RADIUS accounting server to test.
- **username** *user\_name*: Specify a username that is supplied to the RADIUS server for accounting.
- **client-nas** *client\_nas\_ip\_address*: Specify the IP address of the source NAS that is supplied to the RADIUS server for accounting.
- **grinstanceid** *gr\_instanceID*: Specify the GR instance ID. The default value is local instance ID.



**Important** **grinstanceid** is mandatory for non-native instances.

### Example

The following command verifies all the RADIUS servers.

```
test-radius accounting all
```

The following command verifies the RADIUS accounting for user *user1* for the RADIUS server with the IP address *192.0.2.0*.

```
test-radius accounting server 192.0.2.0 port 5000 username user1
```

The following command verifies the RADIUS accounting server group *star1* for user *user1*.

```
test-radius accounting server-group star1 username user1
```

## Testing a RADIUS Authentication Server

When used to test a RADIUS authentication server, the tool generates an authentication request message for a specific user name.



**Note** The user name must already be configured on the RADIUS authentication server prior to executing the test.

To execute the RADIUS authentication test tool, in the Exec mode, use the following command:

```
test-radius authentication { all | server-group group_name | server
server_ip_address port server_port } { client-nas client_nas_ip_address | grinstanceid
gr_instanceID | username user_name | password password }
```

### NOTES:

- **all**: Specify that all configured RADIUS authentication servers be tested.
- **server-group** *group\_name*: Specify the configured RADIUS authentication servers in a RADIUS server group named *group\_name* for server group functionality.

- **server** *server\_ip\_address*: Specify the IP address of a specific RADIUS authentication server to test.
- *server\_port*: Specify the TCP port over that the system must use when communicating with the RADIUS authentication server to test.
- **username** *user\_name*: Specify a username that is supplied to the RADIUS server for authentication. The default user name is *test*.
- **password** *password*: Specify the password associated with the username that is supplied to the RADIUS server for authentication. The default password is *test*.
- **client-nas** *client\_nas\_ip\_address*: Specify the IP address of the source NAS that is supplied to the RADIUS server for accounting.
- **grinstanceid** *gr\_instanceID*: Specify the GR instance ID. The default value is local instance ID.



---

**Important** **grinstanceid** is mandatory for non-native instances.

---

### Example

The following command verifies all the RADIUS servers.

```
test-radius authentication all
```

The following command verifies the RADIUS authentication for user *user1* for the RADIUS server with the IP address *192.0.2.0*.

```
test-radius authentication server 192.0.2.0 port 5000 username user1  
password dummyPwd
```

The following command verifies the RADIUS authentication server group *star1* for user *user1*.

```
test-radius authentication server-group star1 username user1
```

