CoA, RADIUS DM, and Session Redirection (Hotlining)

This chapter describes Change of Authorization (CoA), Disconnect Message (DM), and Session Redirect (Hotlining) support in the system. RADIUS attributes, Access Control Lists (ACLs) and filters that are used to implement these features are discussed. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in this Administration Guide, before using the procedures in this chapter.

Important Not all functions, commands, and keywords/variables are available or supported for all network function or services. This depends on the platform type and the installed license(s).

- RADIUS Change of Authorization and Disconnect Message, on page 1
- Session Redirection (Hotlining), on page 6

RADIUS Change of Authorization and Disconnect Message

This section describes how the system implements CoA and DM RADIUS messages and how to configure the system to use and respond to CoA and DM messages.

CoA Overview

The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session. The filter-id attribute (attribute ID 11) contains the name of an Access Control List (ACL). For detailed information on configuring ACLs, refer to the *IP Access Control Lists* chapter in the *System Administration Guide*.

If the system successfully executes a CoA request, a CoA-ACK message is sent back to the RADIUS server and the data filter is applied to the subscriber session. Otherwise, a CoA-NAK message is sent with an error-cause attribute without making any changes to the subscriber session.

Important Changing ACL and rulebase together in a single CoA is not supported. For this, two separate CoA requests can be sent through AAA server requesting for one attribute change per request.

DM Overview

The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session. If the system successfully disconnects the subscriber session, a DM-ACK message is sent back to the RADIUS server, otherwise, a DM-NAK message is sent with proper error reasons.

License Requirements

The RADIUS Change of Authorization (CoA) and Disconnect Message (DM) are licensed Cisco features. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Enabling CoA and DM

To enable RADIUS Change of Authorization and Disconnect Message:

Step 1 Enable the system to listen for and respond to CoA and DM messages from the RADIUS server as described in Enabling CoA and DM, on page 2.

Step 2 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Step 3 View CoA and DM message statistics as described in Viewing CoA and DM Statistics, on page 5.

Important Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands. Not all commands and keywords/variables are available or supported. This depends on the platform type and the installed license(s).

Enabling CoA and DM

Use the following example to enable the system to listen for and respond to CoA and DM messages from the RADIUS server:

```
configure
   context <context_name>
      radius change-authorize-nas-ip <ipv4/ipv6_address>
      end
```

Notes:

- <*context_name*> must be the name of the AAA context where you want to enable CoA and DM.

  For more information on configuring the AAA context, if you are using StarOS 12.3 or an earlier release, refer to the *Configuring Context-Level AAA Functionality* section of the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

- A number of optional keywords and variables are available for the **radius change-authorize-nas-ip** command. For more information regarding this command please refer to the *Command Line Interface Reference*.

CoA and DM Attributes

For CoA and DM messages to be accepted and acted upon, the system and subscriber session to be affected must be identified correctly.

To identify the system, use any one of the following attributes:

- NAS-IP-Address: NAS IP address if present in the CoA/DM request should match with the NAS IP address.
- NAS-Identifier: If this attribute is present, its value should match to the nas-identifier generated for the subscriber session

To identify the subscriber session, use any one of the following attributes.

- If 3GPP2 service is configured the following attribute is used for correlation identifier:
  - 3GPP2-Correlation-ID: The values should exactly match the 3GPP2-correlation-id of the subscriber session. This is one of the preferred methods of subscriber session identification.
- If 3GPP service is configured the following attributes are used for different identifiers:
  - 3GPP-IMSI: International Mobile Subscriber Identification (IMSI) number should be validated and matched with the specified IMSI for specific PDP context.
  - 3GPP-NSAPI: Network Service Access Point Identifier (NSAPI) should match to the NSAPI specified for specific PDP context.
- User-Name: The value should exactly match the subscriber name of the session. This is one of the preferred methods of subscriber session identification.
- Framed-IP-Address: The values should exactly match the framed IP address of the session.
- Calling-station-id: The value should match the Mobile Station ID.

To specify the ACL to apply to the subscriber session, use the following attribute:

- Filter-ID: CoA only. This must be the name of an existing Access Control List. If this is present in a CoA request, the specified ACL is immediately applied to the specified subscriber session. The Context Configuration mode command, **radius attribute filter-id direction**, controls in which direction filters are applied.

The following attributes are also supported:

- Event-Timestamp: This attribute is a timestamp of when the event being logged occurred.
- If 3GPP2 service is configured following additional attributes are supported:
  - 3GPP2-Disconnect-Reason: This attribute indicates the reason for disconnecting the user. This attribute may be present in the RADIUS Disconnect-request Message from the Home Radius server to the PDSN.
  - 3GPP2-Session-Termination-Capability: When CoA and DM are enabled by issuing the radius change-authorize-nas-ip command, this attribute is included in a RADIUS Access-request message to the Home RADIUS server and contains the value 3 to indicate that the system supports both Dynamic authorization with RADIUS and Registration Revocation for Mobile IPv4. The attribute is also included in the RADIUS Access-Accept message and contains the preferred resource management mechanism by the home network, which is used for the session and may include values 1 through 3.

CoA and DM Error-Cause Attribute

The Error-Cause attribute is used to convey the results of requests to the system. This attribute is present when a CoA or DM NAK or ACK message is sent back to the RADIUS server.

The value classes of error causes are as follows:

- 0-199, 300-399 reserved
- 200-299 - successful completion
- 400-499 - errors in RADIUS server
- 500-599 - errors in NAS/Proxy

The following error cause is sent in ACK messages upon successful completion of a CoA or DM request:

- 201- Residual Session Context Removed

The following error causes are sent in NAK messages when a CoA or DM request fails:

- 401 - Unsupported Attribute
- 402 - Missing Attribute
- 403 - NAS Identification Mismatch
- 404 - Invalid Request
- 405 - Unsupported Service
- 406 - Unsupported Extension
- 501 - Administratively Prohibited
- 503 - Session Context Not Found
- 504 - Session Context Not Removable
- 506 - Resources Unavailable

Viewing CoA and DM Statistics

View CoA and DM message statistics by entering the following command:

show session subsystem facility aaamgr

The following is a sample output of this command.

```
1 AAA Managers
807 Total aaa requests                                  0 Current aaa requests
379 Total aaa auth requests                             0 Current aaa auth requests
    0 Total aaa auth probes                             0 Current aaa auth probes
    0 Total aaa auth keepalive                          0 Current aaa auth keepalive
426 Total aaa acct requests                             0 Current aaa acct requests
    0 Total aaa acct keepalive                          0 Current aaa acct keepalive
379 Total aaa auth success                              0 Total aaa auth failure
    0 Total aaa auth purged                             0 Total aaa auth cancelled
    0 Total auth keepalive success                      0 Total auth keepalive failure
    0 Total auth keepalive purged
    0 Total aaa auth DMU challenged
367 Total radius auth requests                          0 Current radius auth requests
    2 Total radius auth requests retried
    0 Total radius auth responses dropped
    0 Total local auth requests                         0 Current local auth requests
  12 Total pseudo auth requests                         0 Current pseudo auth requests
    0 Total null-username auth requests (rejected)
    0 Total aaa acct completed                          0 Total aaa acct purged
    0 Total acct keepalive success                      0 Total acct keepalive timeout
    0 Total acct keepalive purged
    0 Total aaa acct cancelled
426 Total radius acct requests                          0 Current radius acct requests
    0 Total radius acct requests retried
    0 Total radius acct responses dropped
    0 Total gtpp acct requests                          0 Current gtpp acct requests
    0 Total gtpp acct cancelled                         0 Total gtpp acct purged
    0 Total null acct requests                          0 Current null acct requests
  54 Total aaa acct sessions                            5 Current aaa acct sessions
    3 Total aaa acct archived                           0 Current aaa acct archived
    0 Current recovery archives                       0 Current valid recovery records

    2 Total aaa sockets opened                          2 Current aaa sockets open
    0 Total aaa requests pend socket open
    0 Current aaa requests pend socket open
    0 Total radius requests pend server max-outstanding
    0 Current radius requests pend server max-outstanding
    0 Total aaa radius coa requests                     0 Total aaa radius dm requests
    0 Total aaa radius coa acks                         0 Total aaa radius dm acks
    0 Total aaa radius coa naks                         0 Total aaa radius dm naks
    2 Total radius charg auth                           0 Current radius charg auth
    0 Total radius charg auth succ                      0 Total radius charg auth fail
    0 Total radius charg auth purg                    0 Total radius charg auth cancel

    0 Total radius charg acct                           0 Current radius charg acct
    0 Total radius charg acct succ                      0 Total radius charg acct purg
    0 Total radius charg acct cancel
357 Total gtpp charg                                    0 Current gtpp charg
357 Total gtpp charg success                            0 Total gtpp charg failure
    0 Total gtpp charg cancel                           0 Total gtpp charg purg
    0 Total prepaid online requests                   0 Current prepaid online requests

    0 Total prepaid online success                    0 Current prepaid online failure

    0 Total prepaid online retried                    0 Total prepaid online cancelled
```

```
0 Current prepaid online purged
0 Total aaamgr purged requests
0 SGSN: Total db records
0 SGSN: Total sub db records
0 SGSN: Total mm records
0 SGSN: Total pdp records
0 SGSN: Total auth records
```

Session Redirection (Hotlining)

Important Functionality described for this feature in this segment is not applicable for HNB-GW sessions.

Overview

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address. Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the RADIUS Change of Authorization (CoA) feature.

Note that the session redirection feature is only intended to redirect a very small subset of subscribers at any given time. The data structures allocated for this feature are kept to the minimum to avoid large memory overhead in the session managers.

License Requirements

The Session Redirection (Hotlining) is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Operation

ACL Rule

An ACL rule named **readdress server** supports redirection of subscriber sessions. The ACL containing this rule must be configured in the destination context of the user. Only TCP and UDP protocol packets are supported. The ACL rule allows specifying the redirected address and an optional port. The source and destination address and ports (with respect to the traffic originating from the subscriber) may be wildcarded. If the redirected port is not specified, the traffic will be redirected to the same port as the original destination port in the datagrams. For detailed information on configuring ACLs, refer to the *IP Access Control Lists* chapter in the *System Administration Guide*. For more information on **readdress server**, refer to the *ACL Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Redirecting Subscriber Sessions

An ACL with the **readdress server** rule is applied to an existing subscriber session through CoA messages from the RADIUS server. The CoA message contains the 3GPP2-Correlation-ID, User-Name, Acct-Session-ID, or Framed-IP-Address attributes to identify the subscriber session. The CoA message also contains the Filter-Id attribute which specifies the name of the ACL with the **readdress server** rule. This enables applying the ACL dynamically to existing subscriber sessions. By default, the ACL is applied as both the input and output filter for the matching subscriber unless the Filter-Id in the CoA message bears the prefix **in:** or **out:**.

For information on CoA messages and how they are implemented in the system, refer to RADIUS Change of Authorization and Disconnect Message, on page 1.

Important Changing ACL and rulebase together in a single CoA is not supported. For this, two separate CoA requests can be sent through AAA server requesting for one attribute change per request.

Session Limits On Redirection

To limit the amount of memory consumed by a session manager a limit of 2000 redirected session entries per session manager is allocated. This limit is equally shared by the set of subscribers who are currently being redirected. Whenever a redirected session entry is subject to revocation from a subscriber due to an insufficient number of available session entries, the least recently used entry is revoked.

Stopping Redirection

The redirected session entries for a subscriber remain active until a CoA message issued from the RADIUS server specifies a filter that does not contain the readdress server ACL rule. When this happens, the redirected session entries for the subscriber are deleted.

All redirected session entries are also deleted when the subscriber disconnects.

Handling IP Fragments

Since TCP/UDP port numbers are part of the redirection mechanism, fragmented IP datagrams must be reassembled before being redirected. Reassembly is particularly necessary when fragments are sent out of order. The session manager performs reassembly of datagrams and reassembly is attempted only when a datagram matches the redirect server ACL rule. To limit memory usage, only up to 10 different datagrams may be concurrently reassembled for a subscriber. Any additional requests cause the oldest datagram being reassembled to be discarded. The reassembly timeout is set to 2 seconds. In addition, the limit on the total number of fragments being reassembled by a session manager is set to 1000. If this limit is reached, the oldest datagram being reassembled in the session manager and its fragment list are discarded. These limits are not configurable.

Recovery

When a session manager dies, the ACL rules are recovered. The session redirect entries have to be re-created when the MN initiates new traffic for the session. Therefore when a crash occurs, traffic from the Internet side is not redirected to the MN.

AAA Accounting

Where destination-based accounting is implemented, traffic from the subscriber is accounted for using the original destination address and not the redirected address.

Viewing the Redirected Session Entries for a Subscriber

View the redirected session entries for a subscriber by entering the following command:

show subscribers debug-info { callid *<id>* **| msid** *<id>* **| username** *<name>* **}**

The following command displays debug information for a subscriber with the MSID 0000012345:

show subscribers debug-info msid 0000012345

The following is a sample output of this command:

```
username: user1 callid: 01ca11b1    msid: 0000100003
  Card/Cpu: 4/2
  Sessmgr Instance: 7
  Primary callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:            27         26         15700ms        15700ms
     Micro:           76         76          4200ms         4200ms
    Current state: SMGR_STATE_CONNECTED
    FSM Event trace:
            State                           Event
            SMGR_STATE_OPEN                 SMGR_EVT_NEWCALL
            SMGR_STATE_NEWCALL_ARRIVED      SMGR_EVT_ANSWER_CALL
            SMGR_STATE_NEWCALL_ANSWERED     SMGR_EVT_LINE_CONNECTED
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_LINK_CONTROL_UP
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_AUTH_REQ
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_IPADDR_ALLOC_SUCCESS
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_UPDATE_SESS_CONFIG
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_LOWER_LAYER_UP
Data Reorder statistics
         Total timer expiry:       0         Total flush (tmr expiry):  0
         Total no buffers:         0         Total flush (no buffers):  0
         Total flush (queue full): 0         Total flush (out of range):0
         Total flush (svc change): 0         Total out-of-seq pkt drop: 0
                  Total out-of-seq arrived: 0
IPv4 Reassembly Statistics:
         Success:                  0         In Progress:               0
         Failure (timeout):        0         Failure (no buffers):      0
         Failure (other reasons):  0
Redirected Session Entries:
         Allowed:                  2000      Current:                   0
         Added:                    0         Deleted:                   0
         Revoked for use by different subscriber: 0
  Peer callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:             0          0             0ms            0ms
     Micro:            0          0             0ms            0ms
    Current state: SMGR_STATE_CONNECTED
    FSM Event trace:
            State                           Event
            SMGR_STATE_OPEN                 SMGR_EVT_MAKECALL
            SMGR_STATE_MAKECALL_PENDING     SMGR_EVT_LINE_CONNECTED
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_LOWER_LAYER_UP
            SMGR_STATE_CONNECTED            SMGR_EVT_AUTH_REQ
```

CoA, RADIUS DM, and Session Redirection (Hotlining)

```
            SMGR_STATE_CONNECTED             SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_CONNECTED             SMGR_EVT_REQ_SUB_SESSION
            SMGR_STATE_CONNECTED             SMGR_EVT_RSP_SUB_SESSION
username: user1 callid: 01ca11b1    msid: 0000100003
  Card/Cpu: 4/2
  Sessmgr Instance: 7
  Primary callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:            27         26         15700ms        15700ms
     Micro:           76         76          4200ms         4200ms
    Current state: SMGR_STATE_CONNECTED
    FSM Event trace:
            State                            Event
            SMGR_STATE_OPEN                  SMGR_EVT_NEWCALL
            SMGR_STATE_NEWCALL_ARRIVED       SMGR_EVT_ANSWER_CALL
            SMGR_STATE_NEWCALL_ANSWERED      SMGR_EVT_LINE_CONNECTED
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_LINK_CONTROL_UP
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_AUTH_REQ
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_IPADDR_ALLOC_SUCCESS
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_UPDATE_SESS_CONFIG
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_LOWER_LAYER_UP
Data Reorder statistics
         Total timer expiry:       0         Total flush (tmr expiry):  0
         Total no buffers:         0         Total flush (no buffers):  0
         Total flush (queue full): 0         Total flush (out of range):0
         Total flush (svc change): 0         Total out-of-seq pkt drop: 0
                  Total out-of-seq arrived: 0
IPv4 Reassembly Statistics:
         Success:                  0         In Progress:               0
         Failure (timeout):        0         Failure (no buffers):      0
         Failure (other reasons):  0
Redirected Session Entries:
         Allowed:                  2000      Current:                   0
         Added:                    0         Deleted:                   0
         Revoked for use by different subscriber: 0
Peer callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:             0          0             0ms            0ms
     Micro:            0          0             0ms            0ms
    Current state: SMGR_STATE_CONNECTED
    FSM Event trace:
            State                            Event
            SMGR_STATE_OPEN                  SMGR_EVT_MAKECALL
            SMGR_STATE_MAKECALL_PENDING      SMGR_EVT_LINE_CONNECTED
            SMGR_STATE_LINE_CONNECTED        SMGR_EVT_LOWER_LAYER_UP
            SMGR_STATE_CONNECTED             SMGR_EVT_AUTH_REQ
            SMGR_STATE_CONNECTED             SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_CONNECTED             SMGR_EVT_REQ_SUB_SESSION
            SMGR_STATE_CONNECTED             SMGR_EVT_RSP_SUB_SESSION
            SMGR_STATE_CONNECTED             SMGR_EVT_ADD_SUB_SESSION
            SMGR_STATE_CONNECTED             SMGR_EVT_AUTH_REQ
            SMGR_STATE_CONNECTED             SMGR_EVT_AUTH_SUCCESS
  Data Reorder statistics
         Total timer expiry:       0         Total flush (tmr expiry):  0
         Total no buffers:         0         Total flush (no buffers):  0
         Total flush (queue full): 0         Total flush (out of range):0
         Total flush (svc change): 0         Total out-of-seq pkt drop: 0
         Total out-of-seq arrived: 0
  IPv4 Reassembly Statistics:
         Success:                  0         In Progress:               0
         Failure (timeout):        0         Failure (no buffers):      0
```

CoA, RADIUS DM, and Session Redirection (Hotlining)

```
       Failure (other reasons):  0
Redirected Session Entries:
       Allowed:                  2000      Current:                  0
       Added:                    0         Deleted:                  0
       Revoked for use by different subscriber: 0
```