Chapter 4

Configuring RADIUS Dynamic-Request Server

This chapter describes the RADIUS dynamic-request server feature on E-series routers. The following topics describe this feature:

Overview

The E-series router's RADIUS dynamic-request server feature provides an efficient way for you to use RADIUS servers to centrally manage user sessions. The RADIUS dynamic-request server enables the router to receive the following types of messages from RADIUS servers:

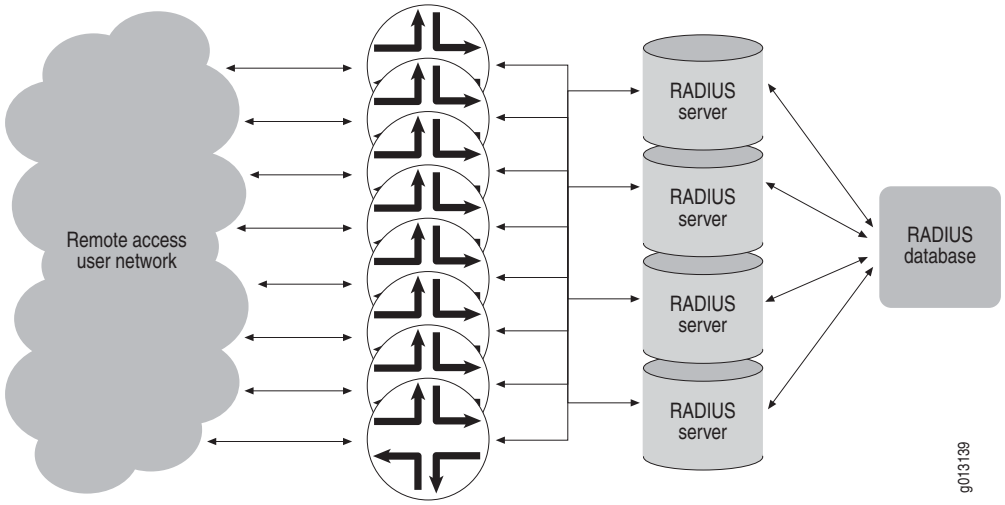
- Disconnect messages—Immediately terminate specific user sessions.
- Change-of-Authorization (CoA) messages—Dynamically modify session authorization attributes, such as data filters.

NOTE: The RADIUS dynamic-request server's support for CoA messages is used by the Service Manager and by the E-series router's packet mirroring feature. For information about using the Service Manager, see *Chapter 27, Configuring Service Manager* in this guide. For specific information about using the dynamic-request server with packet mirroring, see *Configuring RADIUS-Based Mirroring* in *JUNOSe Policy Management Configuration Guide, Chapter 12, Configuring RADIUS-Based Mirroring*

For example, you might use the RADIUS dynamic-request server to terminate specific user sessions. Without the RADIUS dynamic-request server, the only way to disconnect a RADIUS user is from the E-series router. This disconnect method is cumbersome when a network has many systems. The RADIUS dynamic-request server allows RADIUS servers to initiate user-related operations, such as a termination operation, by sending unsolicited request messages to an E-series router.

Figure 5 shows a network that would benefit from the RADIUS dynamic-request server functionality. In Figure 5, instead of disconnecting users on each E-series router, the RADIUS servers can initiate the disconnection. Although the network has multiple RADIUS servers, the servers share a common database that contains authorization and accounting information. Having a common database allows any server to view who is currently valid and connected, and allows service providers to manage the disconnection of users.

Figure 5: Sample Remote Access Network Using RADIUS



Platform Considerations

RADIUS dynamic-request server is supported on all E-series routers. For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

References

For more information about the RADIUS dynamic-request server feature, see the following references:

- RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)
- RFC 2866—RADIUS Accounting (June 2000)
- RFC 3576—Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS) (July 2003)

How RADIUS Dynamic-Request Server Works

In a typical client-server RADIUS environment, the E-series router functions as the client and the RADIUS server functions as the server. However, when using the RADIUS dynamic-request server feature, the roles are reversed. For example, during a RADIUS-initiated disconnect operation, the E-series router's RADIUS dynamic-request server functions as the server, and the RADIUS server functions as the disconnect client.

RADIUS-Initiated Disconnect

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

Disconnect Messages

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

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

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

Message Exchange

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

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

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

Supported Error-Cause Codes (RADIUS Attribute 101)

When a disconnect request fails, the RADIUS dynamic-request server includes an error-cause attribute (RADIUS attribute 101) in the Disconnect-NAK message that it sends back to the RADIUS server. If the detected error does not map to one of the supported error-cause attributes, the router sends the Disconnect-NAK without an error-cause attribute. Table 19 lists the supported error-cause codes.

Table 19: Error-Cause Codes (RADIUS Attribute 101)

Code	Value	Description
401	Unsupported attribute	The request contains an attribute that is not supported (for example, a third-party attribute).
402	Missing attribute	A critical attribute (for example, the session identification attribute) is missing from a request.
404	Invalid request	Some other aspect of the request is invalid, such as if one or more attributes (for example, the packet mirroring Mirror Identifier value) are not formatted properly.
503	Session context not found	The session context identified in the request does not exist on the NAS.
504	Session context not removable	The subscriber identified by attributes in the disconnect request is owned by a component that does not support RADIUS-initiated disconnect (for example, IP LAC subscribers cannot be disconnected).
506	Resources unavailable	A request could not be honored due to lack of available NAS resources (such as memory).

Qualifications for Disconnect

For the server to disconnect a user, the Disconnect-Request message must contain an attribute with a session ID. The Disconnect-Request message can contain an Acct-Session-Id (44) attribute or a Acct-Multi-Session-Id (50) attribute for the session ID or both. If both the Acct-Session-Id and Acct-Multi-Session-Id attributes are present in the request, the router uses both attributes. If the User-Name (1) attribute is also present in the request, the username and session ID are used to perform the disconnection. Authentication, authorization, and accounting (AAA) services handle the actual request.

NOTE: To enable the disconnection of L2TP LAC user sessions, the RADIUS Disconnect-Request message must not include the Acct-Multi-Session-Id (50) attribute. The Acct-Multi-Session-Id attribute does not apply to LAC L2TP user sessions and including this attribute causes the disconnect operation to fail.

Security/Authentication

The RADIUS server (the disconnect client) must calculate the authenticator as specified for an Accounting-Request message in RFC 2866. The router's RADIUS dynamic-request server verifies the request using authenticator calculation as specified for an Accounting-Request message in RFC 2866. A key (secret), as specified in RFC 2865, must be configured and used in the calculation of the authenticator. The response authenticator is calculated as specified for an Accounting-Response message in RFC 2866.

Configuring RADIUS-Initiated Disconnect

To configure RADIUS-initiated disconnect feature, perform the following steps to set up the RADIUS dynamic-request server that will perform the disconnect operation:

1. Configure the RADIUS dynamic-request server, and enter RADIUS Configuration mode.

   host1(config)#**radius dynamic-request server 10.10.5.10**
   host1(config-radius)#

2. Enable the RADIUS-initiated disconnect capability on the RADIUS dynamic-request server.

   host1(config-radius)#**subscriber disconnect**

3. Define the secret used in the RADIUS Authenticator field during exchanges between the RADIUS dynamic-request server and the RADIUS server.

   host1(config-radius)#**key Secret3Clientkey**

4. (Optional) Specify the UDP port on which the RADIUS dynamic-request server listens for messages from the RADIUS server. The default is 1700.

   host1(config-radius)#**udp-port 1770**

RADIUS-Initiated Change of Authorization

This section describes the RADIUS dynamic-request server's support for CoA messages. CoA messages are used by the E-series router's RADIUS-initiated packet mirroring feature, which is described in *JUNOSe Policy Management Configuration Guide, Chapter 12, Configuring RADIUS-Based Mirroring*, and by Service Manager, which is described in *Chapter 27, Configuring Service Manager* of this guide.

Change-of-Authorization Messages

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

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

Message Exchange

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

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

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

Supported Error-Cause Codes (RADIUS Attribute 101)

When AAA is unsuccessful, the RADIUS dynamic-request server includes an error-cause attribute (RADIUS attribute 101) in the CoA-NAK message that it sends back to the RADIUS server. If the detected error does not map to one of the supported error-cause attributes, the router sends the CoA-NAK without an error-cause attribute. Table 20 lists the supported error-cause codes.

Table 20: Error-Cause Codes (RADIUS Attribute 101)

Code	Value	Description
401	Unsupported attribute	The request contains an attribute that is not supported (for example, a third-party attribute).
402	Missing attribute	A critical attribute (for example, the session identification attribute) is missing from a request.

Table 20: Error-Cause Codes (RADIUS Attribute 101) (continued)

Code	Value	Description
404	Invalid request	Some other aspect of the request is invalid, such as if one or more attributes (for example, the packet mirroring Mirror Identifier value) are not formatted properly.
503	Session context not found	The session context identified in the request does not exist on the NAS.
504	Session context not removable	The subscriber identified by attributes in the disconnect request is owned by a component that does not support RADIUS-initiated disconnect (for example, IP LAC subscribers cannot be disconnected).
506	Resources unavailable	A request could not be honored due to lack of available NAS resources (such as memory).

Qualifications for Change of Authorization

To complete the change of authorization for a user, the CoA-Request must contain one of the following RADIUS attributes. AAA services handle the actual request.

- User-Name [attribute 1] (per virtual router context)
- Framed-IP-Address [attribute 8] (per virtual router context)
- Calling-Station-ID [attribute 31]
- Acct-Session-ID [attribute 44]

Security/Authentication

For change-of-authorization operations, the RADIUS server calculates the authenticator as specified for an Accounting-Request message in RFC 2866. The RADIUS dynamic-request server verifies the request using authenticator calculation as specified for an Accounting-Request in RFC 2866. A key (secret), as specified in RFC 2865, must be configured and used in the calculation of the authenticator. The response authenticator is calculated as specified for an Accounting-Response message in RFC 2866.

Configuring RADIUS-Initiated Change of Authorization

To configure the RADIUS dynamic-request change of authorization feature, perform the following steps to set up the RADIUS dynamic-request server that will perform the CoA operation:

1. Configure the RADIUS dynamic-request server, and enter RADIUS Configuration mode.

   host1(config)#**radius dynamic-request server 10.10.5.10**

2. Enable the CoA capability on the RADIUS dynamic-request server.

   host1(config-radius)#**authorization change**

3. Define the key (secret) used in the RADIUS Authenticator field during exchanges between the RADIUS dynamic-request server and the RADIUS server.

   host1(config-radius)#**key Secret21Clientkey**

4. (Optional) Specify the UDP port on which the router listens for messages from the RADIUS server. The default is 1700.

   host1(config-radius)#**udp-port 1770**

RADIUS Dynamic-Request Server Commands

This section describes commands used to configure RADIUS dynamic-request servers.

authorization change

- Use to enable the RADIUS dynamic-request server to receive CoA messages, such as packet mirroring attributes and Service Manager attributes, from the RADIUS server.
- Example

  host1(config)#**radius dynamic-request server 192.168.5.3**
  host1(config-radius)#**authorization change**

- Use the **no** version to disable receipt of the messages; any currently configured operations will continue.

key

- Use to define the key (secret) that is used to calculate the RADIUS Authenticator field during exchanges between the RADIUS dynamic-request server and the RADIUS server.
- If no key is specified, the router drops all requests from the RADIUS server.
- Example

  host1(config-radius)#**key Secret3Clientkey**

- Use the **no** version to set the default, no Authenticator.

radius disconnect client

- Use to configure a RADIUS disconnect client and enter RADIUS Configuration mode. Include the IP address of the RADIUS server that is acting as the disconnect client.
- Example

  host1(config)#**radius disconnect client 10.10.5.10**
  host1(config-radius)#

- Use the **no** version to remove the RADIUS disconnect client.

NOTE: The function of this command has been replaced by a combination of the RADIUS dynamic-request server feature and the **subscriber disconnect** command. This command might be removed completely in a future release.

radius dynamic-request server

- Use to configure a RADIUS dynamic-request server and enter RADIUS Configuration mode. Specify the IP address of the RADIUS server that exchanges messages with the RADIUS dynamic-request server.
- Example

  host1(config)#**radius dynamic-request server 10.10.5.10**
  host1(config-radius)#

- Use the **no** version to unconfigure the RADIUS dynamic-request server.

subscriber disconnect

- Use to enable the RADIUS dynamic-request server to receive RADIUS disconnect messages from a RADIUS server.
- Example

  host1(config-radius)#**subscriber disconnect**

- Use the **no** version to disable processing of disconnect packets.

NOTE: This command and the RADIUS dynamic-request server feature replace the **radius disconnect client** command, which may be removed completely in a future release. The RADIUS Disconnect Configuration mode is also deprecated.

udp-port

- Use to specify the UDP port on which the RADIUS dynamic-request server listens to receive messages from the RADIUS server.
- Example

  host1(config-radius)#**udp-port 1770**

- Use the **no** version to return to the default, port 1700.

Monitoring RADIUS Dynamic-Request Servers

To monitor RADIUS dynamic-request servers, see:

- Setting the Baseline for RADIUS Dynamic-Request Server Statistics on page 238
- Monitoring RADIUS Dynamic-Request Server Statistics on page 239
- Monitoring the Configuration of the RADIUS Dynamic-Request Server on page 240