Chapter 5

Configuring RADIUS Relay Server

This chapter describes the E-series router's RADIUS relay server feature. The RADIUS relay server provides authentication, authorization, accounting, and addressing services to wireless subscribers in public areas, such as airports and coffee shops. This chapter has the following sections:

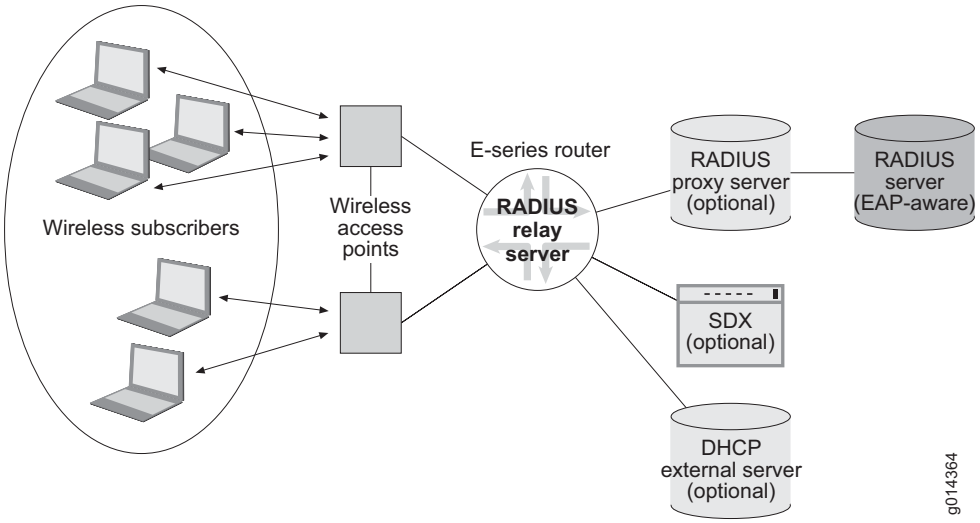
Overview

The JUNOSe RADIUS relay server provides authentication, authorization, accounting, and addressing services in an 802.1x-based wireless environment.

The IEEE 802.1x standard is an authentication standard for wireless LANs; it enables a wireless subscriber to be authenticated by a central authority. The standard uses the Extensible Authentication Protocol (EAP) for message exchange during the authentication process. The E-series router's RADIUS relay server enhances the 802.1x environment by including authorization, accounting, and addressing support for wireless subscribers.

Figure 6 illustrates a typical 802.1x-based wireless environment. In the figure, wireless subscribers connect to wireless access points (WAPs) for authentication. The WAPs in turn connect to the E-series router's RADIUS relay server. The RADIUS relay server passes the request on to the authentication server, which might be a RADIUS or TACACS+ server. The RADIUS server authenticates the subscriber, who is then granted access. After authentication, the RADIUS relay server obtains an IP address for the subscriber from the Dynamic Host Configuration Protocol (DHCP) local or external server. The RADIUS relay server can also use the RADIUS server or the optional Session and Resource Control (SRC) software (formerly the SDX software), to provide the accounting support.

Figure 6: RADIUS Relay Server



Platform Considerations

RADIUS relay 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 RADIUS relay server, see the following resources:

- IEEE 802.1x-2001—Port-Based Network Access Control
- RFC 2869—RADIUS Extensions (June 2000)
- RFC 2284—PPP Extensible Authentication Protocol (EAP) (March 1998)
- RFC 3539—Authentication, Authorization and Accounting (AAA) Transport Profile (June 2003)

How RADIUS Relay Server Works

When a wireless subscriber starts a session, the WAP encapsulates EAP attributes into a RADIUS Access-Request message and sends the request to the E-series router, which the WAP views as the RADIUS server. The encapsulated message uses the RADIUS EAP-Message (79) attribute. The RADIUS relay server does not process any of the EAP attributes in the RADIUS Access-Request message; the encrypted message is simply passed through the router to the actual RADIUS server. The RADIUS server must be EAP aware.

You can also use an optional RADIUS proxy server to provide additional enhancements to the 802.1x-based environment. For example, the RADIUS proxy server enables subscribers to be multiplexed to multiple Internet service providers (ISPs) that are customers of the same carrier. The server performs one of the following actions:

- If the ISP's RADIUS server supports EAP, the RADIUS proxy server extends the EAP session to the RADIUS server.
- If the ISP's RADIUS server does not support EAP, the RADIUS proxy server translates the EAP session into a legacy RADIUS session for the RADIUS server.

Authentication and Addressing

The WAP initiates the authentication and authorization request by sending a standard RADIUS Access-Request to the RADIUS relay server. The Access-Request must include the attributes listed in Table 44. The attributes uniquely identify the wireless subscriber.

Table 44: Required RADIUS Access-Request Attributes

Attribute Name	Description
Called-Station-id [30]	Subscriber's WAP
Calling-Station-id [31]	Subscriber's media access control (MAC) address

When the RADIUS server authenticates the subscriber, the router's RADIUS relay server creates a RADIUS Access-Accept message and sends the message back to the subscriber. The router's DHCP server (either the router's DHCP local server or an external DHCP server) assigns an IP address to the subscriber and creates the subscriber interface.

For information about using the optional SRC software with the RADIUS relay server to assign IP addresses, see *RADIUS Relay Server and the SRC Software* on page 206.

The WAP might periodically reauthenticate a subscriber. For example, reauthentication is necessary to renegotiate a new Wired Equivalent Privacy (WEP) key. The RADIUS relay server ignores any new RADIUS attributes that are sent during a renegotiation operation.

Accounting

The RADIUS relay server's clients (the WAPs) send standard accounting request messages to the RADIUS relay server. The accounting server processes the request and sends the results back to the RADIUS relay server, which then creates a RADIUS accounting response message and forwards the information to the client WAP.

For tracking purposes, the forwarding RADIUS relay server adds the Radius-Client-Address vendor-specific attribute (VSA 26-52) to the forwarded accounting request messages. The VSA indicates the RADIUS relay server's IP address.

For information about using the SRC software with the RADIUS relay server to provide accounting, see *RADIUS Relay Server and the SRC Software* on page 206.

Table 45 shows the RADIUS attributes that must be included in accounting requests. The attributes uniquely identify subscribers.

Table 45: Required RADIUS Accounting Attributes

For RADIUS Acct-Start and Acct-Stop Messages	Description
Called-Station-id [30]	Subscriber's WAP
Calling-Station-id [31]	Subscriber's MAC address
For RADIUS Acct-On and Acct-Off Messages	
Called-Station-id [30]	Subscriber's WAP

Terminating the Wireless Subscriber's Connection

The RADIUS relay server terminates the wireless subscriber's session when one of the following events occurs. When a subscriber session is terminated, the subscriber's IP address is released back into the available address pool.

- The RADIUS relay server receives a RADIUS accounting stop request.
- No RADIUS accounting messages are received for this subscriber for more than 24 hours.

RADIUS Relay Server and the SRC Software

The SRC software is an advanced subscriber configuration and management service. The RADIUS relay server can optionally use the SRC software to perform addressing and accounting services for the subscriber and WAP.

The RADIUS relay server uses the E-series router's DHCP local server or DHCP external server and SRC client process to communicate with the SRC software.

Using the SRC Software for Addressing

If you integrate the SAE software into the RADIUS relay server configuration, the application can contribute to the address pool selection used to lease an address to the subscriber. The SRC software only contributes to address pool selection when the DHCP local server is used; it is not supported when a DHCP external server is used.

Using the SRC Application for Accounting

If you use the SRC software with the RADIUS relay server feature, two accounting domains might actually be created. The first domain is established by the WAP, when the subscriber is authenticated. The second domain is created for the connection between the E-series router and the SRC software.

If you want to continue to use the SRC software's user session and problem-tracking features, you should *not* configure the SRC software to generate RADIUS accounting records. Also, the following attributes must be configured on the RADIUS server used by the WAP:

- Service-Bundle [26-31]
- Class [25]
- User-Name [1]

Configuring RADIUS Relay Server Support

To configure the RADIUS relay server feature, you enable support for the feature on the E-series router and identify the key (secret) used for the connection between the WAP and the RADIUS relay server. The following example configures a RADIUS relay authentication server. Use similar steps to configure a RADIUS relay accounting server.

NOTE: The E-series router supports one instance of the RADIUS relay server per virtual router. The instance can provide authentication, authorization, and accounting support.

1. Enable RADIUS relay server support on the E-series router, and enter RADIUS Relay Configuration mode.

   host1(config)#**radius relay authentication server**
   host1(config-radius-relay)#

2. Specify the IP address and mask of the network that will use the relay authentication server, and the secret used during exchanges between the relay authentication server and clients (the WAPs).

   host1(config-radius-relay)#**key 192.168.25.9 255.255.255.255 mysecret**

3. Specify the router's User Datagram Protocol (UDP) port on which the RADIUS relay server listens.

   host1(config-radius-relay)#**udp-port 1812**

4. (Optional) Verify the configuration.

```
host1(config-radius-relay)#exit
host1(config)#exit
host1#show radius relay servers

RADIUS Relay Authentication Server Configuration
------------------------------------------------
 IP Address         IP Mask        Secret
-------------   ---------------   ---------
10.10.15.0      255.255.255.0     secret
10.10.8.15      255.255.255.255   newsecret
192.168.25.9    255.255.255.255   mysecret
192.168.102.5   255.255.255.255   999Y2K
Udp Port: 1812

RADIUS Relay Accounting Server Configuration
--------------------------------------------
 IP Address         IP Mask       Secret
-------------   ---------------   -------
10.10.1.0       255.255.255.0     NO8pxq
192.168.102.5   255.255.255.255   12BE$56
Udp Port: 1813
```

key

- Use to enter the IP address and mask of the network that will use the RADIUS relay server, and to specify the key (secret) used during exchanges between the RADIUS relay server and client.
- Example

  host1(config-radius-relay)#**key 10.10.15.25 255.255.255.0 Secret3Clientkey**

- Use the **no** version to delete the secret.

radius relay server

- Use to configure a RADIUS relay authentication or accounting server and enter RADIUS Relay Configuration mode.
- Example

  host1(config)#**radius relay authentication server**
  host1(config-radius-relay)#

- Use the **no** version to unconfigure the RADIUS relay server.

radius relay udp-checksum

- Use to enable or disable UDP checksum for RADIUS relay packets.
- Example

  host1(config)#**radius relay udp-checksum enable**

- Use the **no** version to restore the default, enable.

udp-port

- Use to specify the router's UDP port on which the RADIUS relay server resides.
- Example

  host1(config-radius-relay)#**udp-port 1850**

- Use the **no** version to return to the default, port 1812 for authentication servers or port 1813 for accounting servers.

Monitoring RADIUS Relay Server

To monitor RADIUS relay server, see:

- Setting the Baseline for RADIUS Dynamic-Request Server Statistics on page 252
- Monitoring RADIUS Dynamic-Request Server Statistics on page 253
- Monitoring the Configuration of the RADIUS Dynamic-Request Server on page 254