Chapter 17

DHCP Overview

The Dynamic Host Configuration Protocol (DHCP) provides a mechanism through which computers using Transmission Control Protocol/IP (TCP/IP) can obtain protocol configuration parameters automatically from a DHCP server on the network.

The following sections provide overview information for the E-series router DHCP support:

DHCP Overview Information

The most important configuration parameter carried by DHCP is the IP address. A computer must be initially assigned a specific IP address that is appropriate to the network to which the computer is attached and that is not assigned to any other computer on that network. If you move a computer to a new network, it must be assigned a new IP address for that new network. You can use DHCP to manage these assignments automatically.

An IP client contacts a DHCP server for configuration parameters. The DHCP server is typically centrally located and operated by the network administrator. Because the server is run by a network administrator, DHCP clients can be reliably and dynamically configured with parameters appropriate to the current network architecture.

You can configure the E-series router to support the following DHCP features:

- DHCP access model
- DHCP proxy client
- DHCP relay
- DHCP relay proxy
- DHCP local server
- DHCP external server

Session and Resource Control Software

The Session and Resource Control (SRC) software, formerly the Service Deployment System (SDX) software is a component of Juniper Networks management products. The SRC software provides a Web-based interface that allows subscribers to access services, such as the Internet, an intranet, or an extranet.

When a DHCP subscriber logs in, the SRC software can authorize the address request and select the DHCP address pool on the router from which the DHCP address is selected. The SRC software can also control the number of IP addresses that are given to a particular retailer or subscriber and control the lease time of IP addresses assigned to DHCP subscribers.

DHCP Platform Considerations

For information about modules that support DHCP on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, ERX Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support DHCP.

For information about modules that support DHCP on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Module and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support DHCP.

DHCP References

For more information about DHCP, consult the following resources:

- DSL Forum Technical Report (TR)-101—Migration to Ethernet-Based DSL Aggregation (April 2006)
- RFC 2131—Dynamic Host Configuration Protocol (March 1997)
- RFC 2132—DHCP Options and BOOTP Vendor Extensions (March 1997)
- RFC 3046—DHCP Relay Agent Information Option (January 2001)
- RFC 3315—Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (July 2003)
- RFC 3633—IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6 (December 2003)
- RFC 4243—Vendor-Specific Information Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option (December 2005)

NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at http://www.ietf.org for the latest drafts.

For information about supported accounting attributes, see *Chapter 3, Configuring RADIUS Attributes* and *Chapter 6, RADIUS Attribute Descriptions*

Configuring the DHCP Access Model

The E-series router provides a DHCP access model, which enables you to integrate the router into an existing RADIUS-based operation support system (OSS). In the DHCP access model, a DHCP local server or DHCP external service is configured, but the E-series router does not have direct interaction with an OSS or a policy server, such as the SRC software. The router passes the client's DHCP options, client's media access control (MAC) address and, if appropriate, the DHCP relay's IP address in RADIUS requests for authentication.

To configure the DHCP access model to pass the client's information in RADIUS requests, you enable the DHCP options feature, then specify the client information to be passed to RADIUS. You can specify that the client's MAC address be included in the request. You can also specify that the DHCP relay's IP address be sent, if appropriate. For descriptions of the RADIUS attributes used with the DHCP access model, see *Chapter 3, Configuring RADIUS Attributes*.

Configuring DHCP Proxy Clients

DHCP proxy client support enables the router to obtain an IP address from a DHCP server for a remote PPP client. Each virtual router (acting as a DHCP proxy client) can query up to five DHCP servers.

For PPP users, the router acts as a DHCP client to obtain an address for the user. This is referred to as DHCP proxy.

The process for PPP users is as follows:

1. The remote user dials in, and the client requests RADIUS authentication.
2. The AAA server on the router sends a request to the DHCP proxy client on the router for an IP address to be assigned to the remote user's host.
3. The proxy client assumes the role of DHCP client and sends a discovery message to each DHCP server.
4. One or more of the DHCP servers responds with an offer message containing an IP address.
5. The proxy client determines which offer to accept and sends a message to that DHCP server requesting that IP address.
6. The DHCP server responds to the proxy client with an acknowledgment message.
7. The proxy client passes the IP address to the authentication, authorization, and accounting (AAA) server on the router, and the AAA server returns the address to PPP. PPP then assigns the address to the remote host. The new IP address is included when the router next updates its routing table.

Dynamic IP addresses are *leased* to the remote host for a specific period of time, which can range from minutes to days. At the halfway point in the lease period, the proxy client requests an extension from the DHCP server on behalf of the remote host. The lease is extended for a period specified in the acknowledgment (ACK) message returned by the DHCP server—typically equal to the original lease. If the DHCP server returns a negative acknowledgment (NAK) message to the proxy client, the proxy client notifies the server on the router that the extension has been denied. The AAA server logs out the remote host and frees the IP address for reuse.

When a remote host disconnects, the AAA server notifies the proxy client that the IP address is available for reuse. The proxy client informs the DHCP server, which can now reassign that IP address.

For additional information on managing client bindings, see *Viewing and Deleting DHCP Client Bindings* on page 398.

To configure a proxy client from Global Configuration mode:

1. Specify the address of the DHCP server that will provide IP addresses for remote hosts. You can specify a maximum of five DHCP servers.

   host1(config)#**ip dhcp-server 10.6.128.10**

2. Direct the router to request IP addresses for remote users from the DHCP server(s).

   host1(config)#**ip address-pool dhcp**

Related Topics

- **ip address-pool** command
- **ip dhcp-server** command

Logging DHCP Packet Information

The JUNOSe software enables you to collect and log DHCP packet information for all JUNOSe DHCP access models on a per-interface basis. To log packets for a specific DHCP application, you enable DHCP packet logging on the interface that serves the application. JUNOSe software supports per-interface DHCP packet logging on a maximum of 16 interfaces. Per-interface DHCP packet logging is disabled by default.

You can specify which packets are logged—receive, transmit, or all. You can optionally assign low or high priority to the logged packets. Packets are assigned a low priority by default, which does not interfere with router DHCP packet processing. The logged packets are output to the dhcpCapture event logging category.

You can configure per-interface DHCP packet logging on statically configured and dynamically created IP interfaces. However, configuration information for dynamic interface configurations is lost after a cold restart. Both static and dynamic interface configuration information is maintained after a warm restart.

You use the **ip dhcp-capture** command with the following keywords to enable DHCP packet logging for all DHCP applications on the interface.

- Use the **receive**, **transmit**, and **all** keywords to specify the type of DHCP packets that is logged.
- Use the optional **priority** keyword to assign a **low** or **high** priority to logged packets. By default, logged packets have a low priority and do not interfere with the router's DHCP packet processing.

You can specify DHCP packet logging on a maximum of 16 interfaces.

- To enable DHCP packet logging:

  host1(config-if)#**ip dhcp-capture all**

Related Topics

- **ip dhcp-capture** command

Viewing and Deleting DHCP Client Bindings

The JUNOSe software provides commands that enable you to manage your router's DHCP external server, DHCP local server, and DHCP relay proxy client bindings. A client binding associates an IP address with a DHCP client, and describes both the client (for example hardware address and state) and the IP address (for example subnet and lease time).

The commands enable you to view information about current DHCP bindings, and to remove current bindings that are no longer needed. Use the **show dhcp binding** command to display information for current client bindings and track lease times and status. Use the **dhcp delete-binding** command to delete a connected user's IP address lease and the associated route configuration. When you delete a client binding, the lease is removed on the router. You might delete client bindings to:

- Recover functional resources from a user who has not explicitly terminated connectivity and whose lease is unexpired.
- Discontinue connectivity to a user, prompting or forcing the user to request a new lease in order to reestablish network connectivity.

NOTE: This command replaces the **clear ip dhcp-local binding** and **dhcp-external delete-binding** commands, which are deprecated and might be removed in a future release.

You can use the following keywords with the **dhcp delete-binding** command:

  - **all**—Specifies all DHCP local server, DHCP external server, and DHCP relay proxy client bindings
  - **all-local**—Specifies all DHCP local server client bindings
  - **all-external**—Specifies all DHCP external server client bindings
  - **all-relay-proxy**—Specifies all DHCP relay proxy client bindings
  - **binding-id**—Specifies a particular binding ID

- To delete all external bindings:

  host1#**dhcp delete-binding all-external**

- To delete a specific binding:

  host1#**dhcp delete-binding binding-id 3972819365**

Related Topics

- **dhcp delete-binding** command