Chapter 19
# Configuring DHCP Local Server

This chapter provides information for configuring the DHCP local server on the E-series router. This chapter contains the following sections:



## Configuring the DHCP Local Server

This section describes how to configure the DHCP local server:

1. Enable the DHCP local server for either equal-access or standalone mode.

   host1(config)#**service dhcp-local equal-access**
   host1(config)#**service dhcp-local standalone**

2. (Optional) Specify the maximum number of IP addresses that the DHCP local server can supply to each VPI/VCI, VLAN, Ethernet subnetwork, or to a particular interface or subinterface. See *Limiting the Number of IP Addresses Supplied by DHCP Local Server* on page 406 for more information about limiting the number of IP addresses.

   host1(config)#**ip dhcp-local limit ethernet 6**

3. (Optional) Specify any addresses that the DHCP local server must not assign. See *Excluding IP Addresses from Address Pools* on page 407 for more information.

   host1(config)#**ip dhcp-local excluded-address 10.10.3.4**

4. (Optional) Enable general DHCP local server traps. See *Using SNMP Traps to Monitor DHCP Local Server Events* on page 409.

   host1(config)#**ip dhcp-local snmpTraps**

5. (Optional) Configure the DHCP local server to support the creation of dynamic subscriber interfaces built over dynamic VLANs that are based on the agent-circuit-id option (suboption 1) of the option 82 field in DHCP messages. See *Configuring DHCP Local Server to Support Creation of Dynamic Subscriber Interfaces* on page 407.

   host1(config)#**ip dhcp-local auto-configure agent-circuit-identifier**

6. (Optional) Specify that DHCP local server use an optional method to differentiate between clients with duplicate client IDs or hardware addresses. Any changes you make have no effect on currently bound clients. See *Differentiating Between Clients with the Same Client ID or Hardware Address* on page 407.

   host1(config)# **ip dhcp-local unique-client-ids**

7. Configure the DHCP local address pool that supplies IP addresses to subscribers who want to access a domain. See *Configuring DHCP Local Address Pools* on page 411 for more information about configuring address pools.

### *Limiting the Number of IP Addresses Supplied by DHCP Local Server*

You can specify the maximum number of IP addresses that the DHCP local server can supply to each VPI/VCI, VLAN, Ethernet subnetwork, or to a particular interface or subinterface.

You can set global limits for a given interface type—all interfaces of that type that are subsequently created, whether dynamically or statically, inherit that limit value.

You can also set an individual interface limit for a specific interface and override the global limit configured for that interface type. For example, suppose the VLAN interface type limit is five. You can specify a limit of 10 for the VLAN interface FastEthernet 1/0.100. All other VLAN interfaces retain the global limit of five.

The global limits for interface types and the individual interface limits set on static interfaces are kept in NVS. These values are restored during a switchover or a reload.

When you assign an individual limit to a dynamic interface, that limit is in force only until either a switchover or reload takes place. After the switchover or reload, if the action that caused the dynamic interface to be created occurs again, a new dynamic interface is created. The new dynamic interface then inherits the limit set by the global values based on the type of interface that is created.

- Setting a global limit for an interface type:

  host1(config)#**ip dhcp-local limit ethernet 6**

- Setting a limit for a specific interface:

  host1(config)#**ip dhcp-local limit interface atm 3/1 15**

**NOTE:** Limits that you specify on dynamic interfaces are not restored after a switchover or reboot.

### Excluding IP Addresses from Address Pools

You can use the **ip dhcp-local excluded-address** command to specify IP addresses that you do not want the DHCP local server to supply from the default address pool. You might exclude addresses if because those addresses are already used by devices on the subnetwork.

You can exclude a single IP address or a range of addresses. To exclude a range, you specify the start-of-range IP address and the end-of-range IP address.

- Excluding a specific IP address:

  host1(config)#**ip dhcp-local excluded-address 10.10.3.4**

- Excluding a range of IP addresses:

  host1(config)#**ip dhcp-local excluded-address 10.10.3.4 10.10.3.100**

### Configuring DHCP Local Server to Support Creation of Dynamic Subscriber Interfaces

You can use the **ip dhcp-local auto-configure agent-circuit-identifier** command to configure the DHCP local server to support the creation of dynamic subscriber interfaces built over dynamic VLANs that are based on the agent-circuit-id option (suboption 1) of the option 82 field in DHCP messages.

- Use this command within a specific virtual router context.
- This command requires that the user's DHCP control traffic and data traffic traverse the same client-facing ingress port on the E-series router.

The use of the option 82 field enables you to stack an IP interface that is associated with a particular subscriber over a dynamically created VLAN; the VLAN is dynamically created based on the agent-circuit-id option (suboption 1) that is contained in the DHCP option 82 field.

For information about configuring agent-circuit-id–based dynamic VLAN subinterfaces, see *JUNOSe Link Layer Configuration Guide, Chapter 16, Configuring Dynamic Interfaces Using Bulk Configuration*.

### Differentiating Between Clients with the Same Client ID or Hardware Address

A JUNOSe software feature enables the DHCP local server to create unique client IDs to support roaming clients and to manage situations in which two clients in the network have the same hardware address.

**NOTE:** This feature replaces the previous router behavior for DHCP local server client roaming and duplicate address support. The **ip dhcp-local unique-client-ids** command replaces the **ip dhcp-local inhibit-roaming** command, which has been removed from the CLI and has no effect on the DHCP local server.

You can configure the method DHCP local server uses when the router receives a DISCOVER or REQUEST packet that contains a client ID or hardware address that matches the ID or address of a currently bound client on another subnet or subinterface.

In the default configuration, the DHCP local server uses the DHCP client's subnet or subinterface to differentiate duplicate clients and support client roaming. When a new client, with a duplicate ID or hardware address, requests an address lease, DHCP assigns that client a new address and lease—the existing client's lease is unchanged.

The following table describes how the DHCP local server differentiates between a new DHCP client with the same ID or hardware address as a currently bound DHCP client. The determination is based on whether the DHCP clients exist on the same or on different subnets and subinterfaces.

| Location of DHCP Clients with Identical IDs or Addresses | How DHCP Local Server Differentiates Clients |
|---|---|
| On different subinterfaces in the same subnet | By unique subinterface |
| On the same subinterface in different subnets | By unique subnet |
| On different subinterfaces in different subnets | By unique subinterface and unique subnet |
| On the same subinterface in the same subnet | DHCP local server *cannot distinguish clients* with identical IDs or identical hardware addresses in this configuration |

In the optional configuration, you use the **ip dhcp-local unique-client-ids** command to disable the use of the DHCP client's subnet or subinterface to differentiate between clients with duplicate client IDs or hardware addresses. When DHCP receives the request from a duplicate ID or address, DHCP terminates the address lease for the existing client and returns the address to its original address pool. DHCP then assigns a new address and lease to the new client.

We recommend that you enable the **ip dhcp-local unique-client-ids** command only when duplicate client IDs and hardware addresses do not exist in your network.

## *Logging Out DHCP Local Server Subscribers*

You can use the **logout subscribers** command from Privileged Exec mode to log out DHCP local server subscribers. For example, you might use this feature if you want to force a user to request a new lease or if you want to recover functional resources. The **logout subscribers** command, unlike the **clear ip address binding** command (described in *Clearing an IP DHCP Local Server Binding* on page 409), does not terminate the subscriber's user session or management representation.

This command applies to DHCP local server local-access and standalone clients, as well as to PPP users. You can log out **all** subscribers, or log out subscribers by **username**, **domain**, **virtual-router**, or **port**.

### *Clearing an IP DHCP Local Server Binding*

**NOTE:** This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **dhcp delete-binding** command.

You can use the **clear ip dhcp-local binding** command to force the removal of a connected user's IP address lease and associated route configuration. Using this command enables you 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.

### *Using SNMP Traps to Monitor DHCP Local Server Events*

The DHCP local server supports configurable global SNMP traps that monitor events related to the DHCP local server and local SNMP traps that are related to address pool utilization.You use the **ip dhcp-local snmpTraps** command to enable the global SNMP traps for DHCP local server.

The DHCP local server's global SNMP trap generates severity level 1 (alert), 2 (critical), and 3 (error) events. This trap helps administrators monitor DHCP local server general health, error statistics, address lease status, and protocol events. The global SNMP trap generates a severity level 4 (warning) event when a duplicate MAC address is detected. The global SNMP trap information is captured in the dhcpLocalGeneral logging category.

SNMP also traps events related to address pool utilization. You use the **warning** command to define the maximum and minimum threshold values and the **snmpTrap** command to generate traps when utilization occurs above or below the defined values.

For linked or shared pools, SNMP treats the members of the pool as a group, and uses the values configured for the first pool in the chain as the group's threshold.

The address pool utilization SNMP trap information is captured in the dhcpLocalPool logging category.

**NOTE:** You must configure your SNMP management client to read the MIB objects, and your SNMP trap collector must be capable of decoding the new traps. For information about setting up SNMP, see *JUNOSe System Basics Configuration Guide, Chapter 4, Configuring SNMP*.

### *Using DHCP Local Server Event Logs*

To troubleshoot and monitor your DHCP local server, use the following system event logs:

- dhcpLocalClients—DHCP local server client events and duplicate MAC address detection
- dhcpLocalGeneral—DHCP local server infrastructure-related events and number of client threshold events

**NOTE:** The dhcpLocalGeneral category replaces the dhcpLocalServerGeneral category.

- dhcpLocalHighAvailability—DHCP high availability events
- dhcpLocalPool—DHCP local address pool events, including normal, linked, and shared pools
- dhcpLocalProtocol—DHCP local server protocol events

See the *JUNOSe System Event Logging Reference Guide* for additional information about the DHCP local server logs.

### *Related Topics*

- Clearing an IP DHCP Local Server Binding on page 409
- Configuring DHCP Local Address Pools on page 411
- Configuring AAA Authentication for DHCP Local Server Standalone Mode on page 415
- Configuring DHCP Local Server to Support Creation of Dynamic Subscriber Interfaces on page 407
- Differentiating Between Clients with the Same Client ID or Hardware Address on page 407
- Excluding IP Addresses from Address Pools on page 407
- Limiting the Number of IP Addresses Supplied by DHCP Local Server on page 406
- Logging Out DHCP Local Server Subscribers on page 408
- Using DHCP Local Server Event Logs on page 410
- Using SNMP Traps to Monitor DHCP Local Server Events on page 409
- **clear ip dhcp-local binding** command
- **dhcp delete-binding** command
- **ip dhcp-local auto-configure agent-circuit-identifier** command

- **ip dhcp-local excluded-address** command
- **ip dhcp-local limit** command
- **ip dhcp-local unique-client-ids** command
- **logout subscribers** command
- **service dhcp-local** command

## Configuring DHCP Local Address Pools

This section describes how to configure DHCP local address pool. DHCP local server uses the address pool to supply IP addresses to subscribers who want to access a domain.

1. Specify the pool name and access DHCP Local Pool Configuration mode.

   host1(config)#**ip dhcp-local pool ispBoston**
   host1(config-dhcp-local)#

2. Specify the IP address of the router for the subscriber's computer to use for traffic destined for locations beyond the local subnetwork.

   host1(config-dhcp-local)#**default-router 10.10.1.1**

   The default router must be on the same subnetwork as the local server pool IP addresses that you configure with the **network** command.

   You specify the IP address of a primary server, and optionally, the IP address of a secondary server.

3. (Optional) Assign a DNS server to an address pool. Some DHCP clients request the DHCP local server to assign a DNS server.

   host1(config-dhcp-local)#**dns-server 10.10.1.1**

4. (Optional) Specify a domain name that can be returned to the subscriber if requested.

   host1(config-dhcp-local)#**domain-name ispBoston**

   The name of the domain must match the name you specified for the RADIUS vendor-specific attribute (VSA) and for authentication, authorization, accounting, and address assignment.

5. Specify the time period for which the supplied IP address is valid.

   host1(config-dhcp-local)#**lease 0 0 24**

   Specify the number of days, and optionally, the number of hours, minutes, and seconds. Use the keyword **infinite** to specify a lease that does not expire. The default lease time is 30 minutes.

6. (Optional) Link the DHCP local address pool being configured to another local address pool. See *Linking Local Address Pools* on page 413 for more information about linking local address pools.

   host1(config-dhcp-local)#**link ispChicago**

7. (Optional) Assign a NetBIOS server for subscribers. Some DHCP clients request the DHCP local server to assign a NetBIOS server.

   host1(config-dhcp-local)#**netbios-name-server 10.10.1.1 10.10.1.2**

   Specify the IP address of a primary server and, optionally, the address of a secondary server.

8. (Optional) Specify NetBIOS node type.

   host1(config-dhcp-local)#**netbios-node-type b-node**

   Specify one of the following types of NetBIOS nodes. By default, the node type is unspecified.

   - **b-node**—Broadcast
   - **p-node**—Peer-to-peer
   - **m-node**—Mixed
   - **h-node**—Hybrid

9. Specify the IP addresses that the DHCP local server can provide from an address pool.

   host1(config-dhcp-local)#**network 10.10.1.0 255.255.0.0**

   Use the **force** keyword with the **no** version of the command to delete the address pool even if the pool is in use.

10. For standalone mode, you can reserve an IP address for a specific MAC address.

    host1(config-dhcp-local)#**reserve 10.10.13.8 0090.1a10.0552**

11. For standalone mode, you can specify the DHCP server address that is sent to DHCP clients.

    host1(config-dhcp-local)#**server-address 10.10.20.0**

12. (Optional) Enable Simple Network Management Protocol (SNMP) traps for local address pool utilization, including normal, linked, and shared address pools. Traps are generated based on threshold values for utilization. You can define threshold values by using the **warning** command. See *Using SNMP Traps to Monitor DHCP Local Server Events* on page 409 for more information about SNMP and local address pools.

    host1(config-dhcp-local)#**snmpTrap**
    host1(config-dhcp-local)#**warning 50 40**

13. (Optional) Configure a grace period for address leases allocated from the current DHCP local address pool. Specify the number of days and, optionally, the number of hours, minutes, and seconds in the grace period.

    host1(config-dhcp-local)#**grace-period 0 12**

    This command applies only to address leases that expire. Use the **use-release-grace-period** command to also apply the configured grace period to the local pool addresses that are explicitly released by clients. See *Setting Grace Periods for Address Leases* on page 413 for more information about grace periods.

14. (Optional) Specify that the grace period is applied to addresses that have been explicitly released by clients. By default, the grace period is applied only to address leases that expire, not to addresses that have been released. See *Setting Grace Periods for Address Leases* on page 413 for more information about grace periods.

    host1(config-dhcp-local)#**use-release-grace-period**

### *Linking Local Address Pools*

In both equal-access mode and standalone mode, you can link a DHCP local pool to another local pool. The linked pool serves as a backup pool. If no addresses are available in a pool, the DHCP local server attempts to allocate an address from the linked pool. The address pools that are linked are viewed as a group.

### *Setting Grace Periods for Address Leases*

The JUNOSe software enables you to configure a grace period for a particular local address pool—the grace period is applied to all address leases associated with the address pool. The grace period is the amount of time that a client continues to retain its address lease after the lease expires or is released. An address cannot be assigned to any other client during the grace period. When the grace period expires, the address is released back to the address pool.

Grace periods help to ensure that a DHCP client retains its previously assigned IP address in situations that might normally cause a lease termination followed by a new address assignment. For example, if a client loses its lease due to a network disruption, the grace period enables the client to be reassigned the same address when the client requests an address after the network stabilizes. Grace periods are also useful during client reboots and in cases where a non-compliant or unreliable DHCP implementation triggers a lease renewal.

You configure a grace period for a local address pool. The grace period is immediately applied to all addresses that are allocated from the pool, including previously allocated addresses that are currently active—the new grace period takes precedence over a previously configured grace period for the address pool.

**NOTE:** Configuring a new grace period that is shorter than the address pool current grace period immediately terminates any existing address leases that are in the grace period state and that have already exceeded the length of the new grace period.

**NOTE:** An address continues to be counted against the address pool resources while in a grace period. For example, if the address pool is exhausted, a new address cannot be assigned to other clients.

Client address leases enter the grace period in two ways—the lease might expire or the address can be explicitly released by the client. In both cases the address remains unavailable to other clients and can only be reapplied to the original client during the grace period. The address is released back to the address pool if the grace period expires before the address is reapplied to the original client.

When you configure a grace period, by default it is applied to address leases that *expire*, but not to addresses that are *released* by clients. However, you can optionally apply the grace period to released addresses.

### *Related Topics*

- Linking Local Address Pools on page 413
- Setting Grace Periods for Address Leases on page 413
- Using SNMP Traps to Monitor DHCP Local Server Events on page 409
- **default-router** command
- **dns-server** command
- **domain-name** command
- **grace-period** command
- **ip dhcp-local pool** command
- **lease** command
- **link** command
- **netbios-name-server**command
- **netbios-node-type** command
- **network** command
- **reserve** command

- **server-address** command
- **snmpTrap** command
- **use-release-grace-period** command
- **warning** command

## Configuring AAA Authentication for DHCP Local Server Standalone Mode

The DHCP local server enables you to optionally configure AAA-based authentication of standalone mode DHCP clients. In addition to providing increased security, AAA authentication also provides RADIUS-based input to IP address pool selection for standalone mode clients. By default, clients are not authenticated in standalone mode.

Typically, an incoming DHCP client does not provide a username—therefore, the DHCP local server constructs a username based on the user's attachment parameters and optional DHCP parameters. AAA uses the constructed username to authenticate the incoming client and create the AAA subscriber record for the client. The information in the AAA subscriber record is then used to determine the IP address pool from which to assign the address for the DHCP client. You can include the following elements in the username:

| Attachment Parameters | DHCP Parameters |
|---|---|
| domain | circuit ID |
| user prefix | circuit type |
| – | MAC address |
| – | option 82 |
| – | virtual router name |

**NOTE:** The nondomain portion of a constructed username must contain at least one character. Otherwise, the DHCP local server rejects the DHCP client without performing the AAA authentication request.

When using authentication, AAA accepts the DHCP client as a subscriber—this enables you to use **show** commands to monitor configuration information and statistics about the client. You can also use the **logout subscriber** command to manage subscribers.

To configure AAA-based authentication for DHCP local server standalone mode clients:

**CAUTION:** Configuring authentication on the DHCP local server requires that you first disable the DHCP local server for standalone mode. Doing so removes your entire DHCP local server configuration. Therefore, if you want to configure authentication, do so before you have otherwise configured the DHCP local server.

1. Disable the DHCP local server for standalone mode.

   host1(config)#**no service dhcp-local standalone**

2. Enable AAA-based authentication for DHCP local server standalone mode clients.

   host1(config)#**service dhcp-local standalone authenticate**

3. Specify the password. that authenticates a locally configured DHCP standalone mode client. In DHCP standalone mode, the password is presented to AAA in an authentication request.

   host1(config)#**ip dhcp-local auth password to4tooL8**

4. Specify the domain for a username that is locally configured for a DHCP standalone mode client. The locally configured username is presented to AAA in an authentication request.

   host1(config)#**ip dhcp-local auth domain ISP1.com**

5. Specify the user-prefix for a username that is locally configured for a DHCP standalone mode client. The locally configured username is presented to AAA in an authentication request.

   host1(config)#**ip dhcp-local auth user-prefix ERX4-Boston**

6. Include optional information as part of the locally configured username for a DHCP standalone mode client. The optional information becomes part of the AAA subscriber record, and is then used to determine the IP address pool from which to assign the address for the DHCP client.

   Use the following keywords to include specific information:

   - **circuit-identifier**—Specifies the circuit identifier of the interface on which the DHCP client's request was received.
   - **circuit-type**—Specifies the circuit type of the interface on which the DHCP client's request was received.
   - **mac-address**—Specifies the DHCP client's MAC address.
   - **option82**—Specifies the DHCP client's option 82 value.
   - **virtual-router-name**—Specifies the DHCP local server's virtual router name.

   host1(config)#**ip dhcp-local auth include virtual-router-name**
   host1(config)#**ip dhcp-local auth include circuit-type**
   host1(config)#**ip dhcp-local auth include circuit-identifier**

7. (Optional) Verify your authentication configuration.

```
host1(config)#show ip dhcp-local auth config

DHCP Local Server Authentication Configuration

User-Prefix          : ERX4-Boston
Domain               : ISP1.com
Password             : to4TooL8
Virtual Router       : included
Circuit Type         : included
Circuit ID           : included
MAC Address          : excluded
Option 82            : excluded
```

### *Related Topics*

- **ip dhcp-local auth domain** command
- **ip dhcp-local auth include** command
- **ip dhcp-local auth password** command
- **ip dhcp-local auth user-prefix** command
- **service dhcp-local authenticate** command

## Configuring the DHCPv6 Local Server

In addition to the embedded DHCP local server that is used for IP version 4 (IPv4) address support, E-series routers include an embedded DHCPv6 local server. This server enables the router to function as a server for the DHCP protocol for IP version 6 (IPv6). The DHCPv6 local server sends and receives packets via IPv6 and informs IPv6 of the routing requirements of the router clients.

The DHCPv6 local server provides the following IPv6 address support:

- Delegates IPv6 prefixes to client routers; each client can have one prefix; prefixes and DNS information can be locally configured or derived from RADIUS via AAA.
- Provides DNS server information to directly connected router clients.

**NOTE:** You must add a vendor-specific attribute to RADIUS to enable E-series routers to retrieve IPv6 Domain Name System (DNS) addresses.

Use the following steps to configure the DHCPv6 local server:

1. Enable the DHCPv6 local server.

   host1(config)#**service dhcpv6-local**

2. Specify the IPv6 prefix and lifetime that are to be delegated to the DHCPv6 client. The specified prefix is delegated by the DHCPv6 local server when requested by the client.

   host1(config-if)#**ipv6 dhcpv6-local delegated-prefix 2001:db8:17::/48 lifetime infinite**

   Use the **lifetime** keyword to specify the time period for which the prefix is valid. This lifetime overrides the default lifetime that is set in Global Configuration mode. If no lifetime is specified, the default lifetime is assigned.

   - Specify the number of days and, optionally, the number of hours, minutes, and seconds. You cannot specify a lifetime of zero (that is, you cannot set the days, hours, minutes, and seconds fields all to zero).
   - Use the keyword **infinite** to specify a lifetime that does not expire.

3. Specify the name of a DNS domain for DHCPv6 clients in the current virtual router to search. You can specify a maximum of four DNS domains for a DHCPv6 local server's search list.

   host1(config-if)#**ipv6 dhcpv6-local dns-domain-search xyzcorporation.com**
   host1(config-if)#**ipv6 dhcpv6-local dns-domain-search xyzcorp.com**

4. Specify the IPv6 address of the DNS server and to assign the server to the DHCPv6 clients in the current virtual router. Your can specify a maximum of four DNS servers.

   host1(config-if)#**ipv6 dhcpv6-local dns-server 2001:db8:18::**

5. Set the default lifetime for which a prefix delegated by this DHCPv6 local server is valid. This default is overridden by an interface-specific lifetime.

   host1(config-if)#**ipv6 dhcpv6-local prefix-lifetime infinite**

   - Specify the number of days and, optionally, the number of hours, minutes, and seconds. You cannot specify a lifetime of zero (that is, you cannot set the days, hours, minutes, and seconds fields all to zero).
   - Use the keyword **infinite** to specify a lifetime that does not expire.

### *Related Topics*

- **ip dhcp-local auth domain** command
- **service dhcpv6-local** command
- **ipv6 dhcpv6-local delegated-prefix** command

- **ipv6 dhcpv6-local dns-domain-search** command
- **ipv6 dhcpv6-local dns-server** command
- **ipv6 dhcpv6-local prefix-lifetime** command

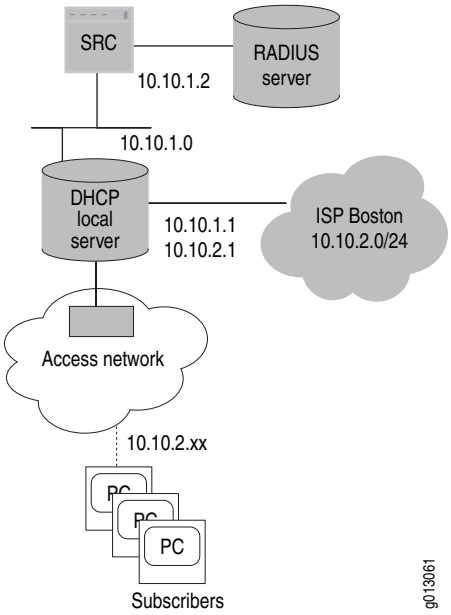
## Configuring the Router to Work with the SRC Software

E-series routers have an embedded SRC client that interacts with the SRC software. For information about configuring the SRC client, see *Configuring the SRC Client* in *Chapter 1, Configuring Remote Access*.

**Configuration Example**

Figure 12 shows the scenario for this example. Subscribers obtain access to ISP Boston via a router. Subscribers log in through the SRC software, and a RADIUS server provides authentication.

**Figure 12: Non-PPP Equal-Access Configuration Example**




The following steps describe how to configure this scenario.

1. Configure interfaces on the router.

```
host1(config)#interface loopback 0
host1(config-if)#ip address 10.10.1.1 255.255.255.0
host1(config-if)#ip address 10.10.2.1 255.255.255.0 secondary
host1(config-if)#exit
host1(config)#interface fastEthernet 2/0
host1(config-if)#ip unnumbered loopback 0
```

2. Configure the parameters to enable the router to forward authentication requests to the RADIUS server.

   host1(config)#**radius authentication server 10.10.1.2**
   host1(config)#**udp-port 1645**
   host1(config)#**key radius**

3. Specify the authentication method.

   host1(config)#**aaa authentication ppp default radius**

   Or

   host1(config)#**aaa authentication ppp default none**

4. Enable the DHCP local server.

   host1(config)#**service dhcp-local**

5. Specify the IP addresses that are in use, so that the DHCP local server cannot assign these addresses.

   host1(config)#**ip dhcp-local excluded-address 10.10.1.1**
   host1(config)#**ip dhcp-local excluded-address 10.10.1.2**

6. Configure the DHCP local server to provide IP addresses to subscribers of ISP Boston.

   host1(config)**ip dhcp-local pool ispBoston**
   host1(config-dhcp-local)#**network 10.10.2.0 255.255.255.0**
   host1(config-dhcp-local)#**domain-name ispBoston**
   host1(config-dhcp-local)#**default-router 10.10.2.1**
   host1(config-dhcp-local)#**lease 0 0 10**
   host1(config-dhcp-local)#**ip dhcp-local limit atm 5**

7. Configure the SRC client.

   host1(config)#**sscc primary address 10.10.1.2 port 3310**
   host1(config)#**sscc enable**
   host1(config)#**sscc retryTimer 200**