JUNIPER NETWORKS

Junos® OS

System Services Administration Guide for Routing Devices

Release
14.1

Published: 2014-05-08

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS System Services Administration Guide for Routing Devices
14.1

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Part 2 Configuration

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- M Series
- MX Series
- T Series
- J Series
- PTX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming

configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xsl; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xv defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xvi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** *metric***>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** *community-ids* **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/

- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

System Services Overview

System Services Overview

For security reasons, remote access to the router is disabled by default. You must configure the router explicitly so that users on remote systems can access it. The router can be accessed from a remote system by means of the DHCP, finger, FTP, rlogin, SSH, and Telnet services. In addition, Junos XML protocol client applications can use Secure Sockets Layer (SSL) or the Junos XML protocol-specific clear-text service, among other services.

NOTE: To protect system resources, you can limit the number of simultaneous connections that a service accepts and the number of processes owned by a single user. If either limit is exceeded, connection attempts fail.

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 26
- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30
- DHCP Access Service Overview on page 6
- Configuring the Router as an Extended DHCP Local Server on page 45
- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools on page 11
- Configuring DTCP-over-SSH Service for the Flow-Tap Application on page 55
- Configuring Finger Service for Remote Access to the Router on page 17
- Configuring FTP Service for Remote Access to the Router or Switch on page 18
- Configuring SSH Service for Remote Access to the Router or Switch on page 18
- Configuring Outbound SSH Service on page 21
- Configuring NETCONF-Over-SSH Connections on a Specified TCP Port on page 25

CHAPTER 2

DHCP Access Service for IP Address Management Overview

DHCP Access Service Overview

DHCP access service consists of two components: a protocol for delivering host-specific configuration information from a server to a client host and a method for allocating network addresses to a client host. The client sends a message to request configuration information. A DHCP server sends the configuration information back to the client.

With DHCP, clients can be assigned a network address for a fixed *lease*, enabling serial reassignment of network addresses to different clients. A DHCP server leases IP addresses for specific times to various clients. If a client does not use its assigned address for some period of time, the DHCP server can assign that IP address to another host. When assignments are made or changed, the DHCP server updates information in the DNS server. The DHCP server provides clients with their previous lease assignments whenever possible.

A DHCP server provides persistent storage of network parameters for clients. Because DHCP is an extension of BOOTP, DHCP servers can handle BOOTP requests.

The DHCP server includes IPv4 address assignment and commonly used DHCP options. The server is compatible with DHCP servers from other vendors on the network. The server does not support IPv6 address assignment, user class-specific configuration, DHCP failover protocol, dynamic DNS updates, or VPN connections. The Junos-FIPS software does not support the DHCP server.

NOTE: **You cannot configure a router as a DHCP server and a BOOTP relay agent at the same time.**

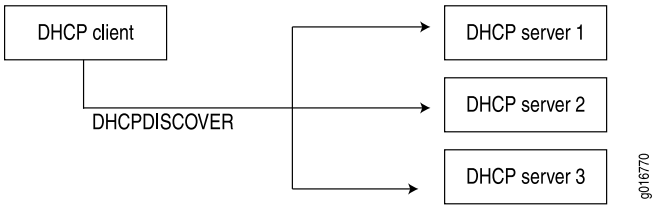
The following topics describe these concepts in detail:

Network Address Assignments (Allocating a New Address)

To receive configuration information and a network address assignment, a DHCP client negotiates with DHCP servers in a series of messages. The following steps show the messages exchanged between a DHCP client and servers to allocate a new network address. When allocating a new network address, the DHCP process can involve more than one server, but only one server is selected by the client.

1. When a client computer is started, it broadcasts a **DHCPDISCOVER** message on the local subnet, requesting a DHCP server. This request includes the hardware address of the requesting client.

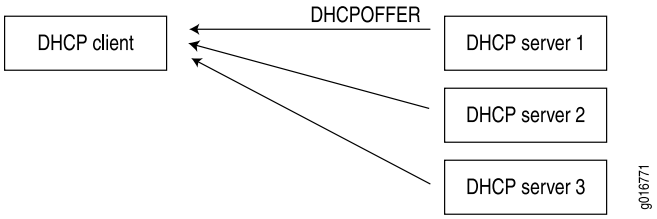
Figure 1: DHCP Discover



NOTE: For improved operation with DHCP clients that do not strictly conform to RFC 2131, the DHCP server accepts and processes **DHCPDISCOVER** messages even if the overload options in the messages are not properly terminated with an end statement.

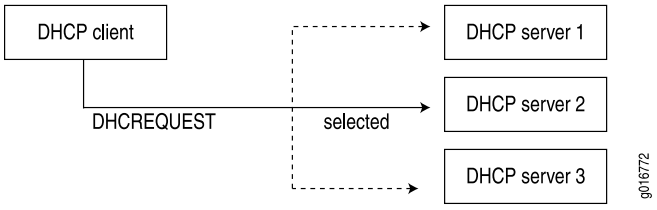
2. Each DHCP server receiving the broadcast sends a **DHCPOFFER** message to the client, offering an IP address for a set period of time, known as the lease period.

Figure 2: DHCP Offer



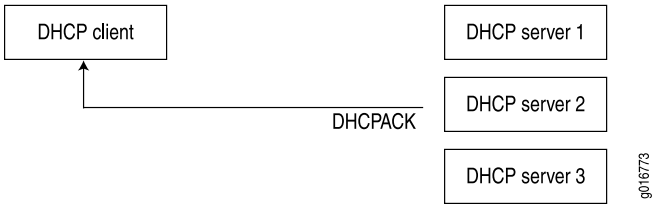
3. The client receives one or more **DHCPOFFER** messages from one or more servers and selects one of the offers received. Normally, a client looks for the longest lease period.
4. The client broadcasts a **DHCPREQUEST** message indicating the client has selected an offered leased IP address and identifies the selected server.

Figure 3: DHCP Request



5. Those servers not selected by the **DHCPREQUEST** message return the unselected IP addresses to the pool of available addresses.
6. The selected DHCP server sends a **DHCPACK** acknowledgment that includes configuration information such as the IP address, subnet mask, default gateway, and the lease period.

Figure 4: DHCP ACK

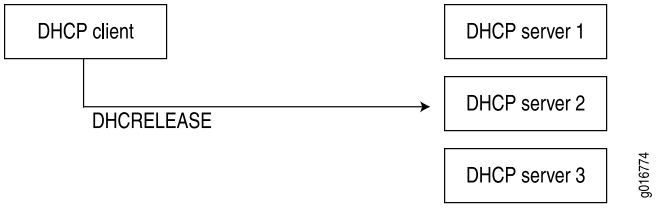


The information offered by the server is configurable.

7. The client receives the **DHCPACK** message with configuration information. The process is complete. The client is configured and has access to the network.

   - If the client receives a **DHCPNAK** message (for example, if the client has moved to a new subnet), the client restarts the negotiation process.
   - The client can relinquish its lease on a network address by sending a **DHCPRELEASE** message to the server (for example, when the client is restarted). When the server receives the **DHCPRELEASE** message, it marks the lease as free and the IP address becomes available again.

Figure 5: DHCP Release



Network Address Assignments (Reusing a Previously Assigned Address)

To enable reuse of a previously allocated network address, the following events occur:

1. A client that previously had a lease broadcasts a **DHCPREQUEST** message on the local subnet.
2. The server with knowledge of the client's configuration responds with a **DHCPACK** message.
3. The client verifies the DHCP configuration information sent by the server and uses this information to reestablish the lease.

Static and Dynamic Bindings

DHCP supports both dynamic and static bindings. For dynamic bindings, IP addresses are assigned to clients from a pool of addresses. Static bindings provide configuration information for a specific client and can include one or more fixed IP addresses for the client. You can configure a DHCP server to include both address pools and static bindings. For any individual client, static bindings take priority over address pools.

Compatibility with Autoinstallation

The DHCP server is compatible with the autoinstallation feature on J Series Services Routers. The server automatically checks autoinstallation settings for conflicts and gives autoinstallation settings priority over corresponding DHCP settings. For example, an IP address set by autoinstallation takes priority over an IP address set by the DHCP server.

NOTE: **The autoinstallation feature includes a fixed address pool and a fixed lease time. With DHCP, you can create address pools and modify lease times.**

Conflict Detection and Resolution

When a client receives an IP address from the DHCP server, the client performs a series of ARP tests to verify that the IP address is available and no conflicts exist. If the client detects an address conflict, the client notifies the DHCP server about the conflict and may request another IP address from the DHCP server.

The DHCP server keeps a log of all conflicts and removes addresses with conflicts from the pool. These addresses remain excluded until you manually clear the conflicts list with the **clear system services dhcp conflict** command.

Related Documentation

- DHCP Statement Hierarchy and Inheritance on page 9

DHCP Statement Hierarchy and Inheritance

DHCP configuration statements are organized hierarchically. Statements at the top of the hierarchy apply to the DHCP server and network, branches contain statements that apply to address pools in a subnetwork, and leaves contain statements that apply to static bindings for individual clients. See Table 3 on page 9.

The **pool** and **static-binding** statements appear at the **[edit system services dhcp]** hierarchy level. You can include the remaining statements at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

Table 3: Pool and Binding Statements

Statement	Description	Hierarchy Level
pool	Configure a pool of IP addresses for DHCP clients on a subnet. When a client joins the network, the DHCP server dynamically allocates an IP address from this pool.	**[edit system services dhcp]**
static-binding	Set static bindings for DHCP clients. A static binding is a mapping between a fixed IP address and the client's MAC address.	

To minimize configuration changes, include common configuration statements shown in Table 4 on page 10 (for example, the **domain-name** statement) at the highest applicable level of the hierarchy (network or subnetwork). Configuration statements at lower levels of the hierarchy override statements inherited from a higher level. For example, if a statement appears at both the **[edit system services dhcp]** and **[edit system services dhcp pool]** hierarchy levels, the value assigned to the statement at the **[edit system services dhcp pool]** level takes priority.

Table 4: Common Configuration Statements

Statement	Description	Hierarchy Level
boot-file	Set the boot filename advertised to clients. The client uses the boot image stored in the boot file to complete configuration.	**[edit system services dhcp]** **[edit system services dhcp pool]** **[edit system services dhcp static-binding]**
boot-server	Set the server that contains the boot file.	
default-lease-time	Set the default lease time assigned to any client that does not request a specific lease time.	
domain-name	Configure the name of the domain in which clients will search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified.	
domain-search	Define a domain search list.	
maximum-lease-time	Set the maximum lease time allowed by the server.	
name-server	Specify the DNS server that maintains the database of client name to IP address mappings.	
option	Configure user-defined DHCP options.	
router	Specify IP address for routers on the client's subnetwork. Routers are listed in order of preference.	
server-identifier	Set the IP address of the DHCP server.	

Related Documentation

- DHCP Access Service Overview on page 6

Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools

In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer, and the DHCP local server is configured on the router. The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, and address-assignment pools:

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber.
2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.
3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server that will grant the address and configuration information.
4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server also installs the host route and ARP entry, and then monitors the lease state.

Extended DHCP Local Server and Address-Assignment Pools

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients. See *Configuring Address-Assignment Pools* for details about creating and using address-assignment pools.

NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

Methods Used by the Extended DHCP Local Server to Determine Which Address-Assignment Pool to Use

You can specify the method that the extended DHCP local server uses to determine which address-assignment pool provides the IP address and configuration for a DHCP client. By default, the server matches the IP address in the client DHCP request to the address of the address-assignment pool.

The following sections describe the methods used by the DHCP local server to determine which address-assignment pool to use:

- Matching the Client IP Address to the Address-Assignment Pool on page 12
- Matching Option 82 Information to Named Address Ranges on page 12

Matching the Client IP Address to the Address-Assignment Pool

In the default configuration, the server selects the address-assignment pool to use by matching the IP address in the client DHCP request with the network address of the address-assignment pool. If the client request contains the gateway IP address (giaddr), the local server matches the giaddr to the address-assignment pool's address. If there is no giaddr in the request, the DHCP local server matches the IP address of the receiving interface to the address of the address-assignment pool.

Matching Option 82 Information to Named Address Ranges

You can also configure the extended DHCP local server to match the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool used for the client. Named ranges are subsets within the overall address-assignment pool address range, and are configured when you create the address-assignment pool. To use the DHCP local server option 82 matching feature, you must ensure that the **option-82** statement is included in the **dhcp-attributes** statement for the address-assignment pool.

NOTE: To enable the option 82 matching method, you must first specify the **ip-address-first** statement in the **pool-match-order** statement, and then specify the **option-82** statement.

Default Options Provided by the Extended DHCP Server for the DHCP Client

The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

- **router**—A router located on the client's subnet. This statement is the equivalent of DHCP option 3.
- **domain name**—The name of the domain in which the client searches for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.
- **domain name server**—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client

When the extended DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The extended DHCP application uses the information from the authentication grant for the response the DHCP application sends to the DHCP client. The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications. For example, if the authentication grant includes an address pool name and a local configuration specifies DHCP attributes for that pool, the extended DHCP application merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional—a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you must configure the local address assignment pool to provide the configuration for the client. When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. The following list shows the information that RADIUS might include in the authentication grant. See *RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework* for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management.

- Client IP address—RADIUS attribute 8, Framed-IP-Address
- Subnet mask for client IP address (DHCP option 1)—RADIUS attribute 9, Framed-IP-Netmask
- Primary domain server (DHCP option 6)—VSA 26-4, Primary-DNS
- Secondary domain server (DHCP option 6)—VSA 26-5 Secondary-DNS
- Primary WINS server (DHCP option 44)—VSA 26-6, Primary-WINS
- Secondary WINS server (DHCP option 44)—VSA 26-7, Secondary-WINS
- Address assignment pool name—RADIUS attribute 88, Framed-Pool
- Lease time—RADIUS attribute 27, Session-Timeout
- DHCP relay server—VSA 26-109, DHCP-Guided-Relay-Server

PART 2

Configuration

CHAPTER 3

Configuring System Services for Remote Router or Switch Access

Configuring Finger Service for Remote Access to the Router

To configure the router to accept finger as an access service, include the **finger** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
finger {
  connection-limit limit;
  rate-limit limit;
}
```

By default, the router supports a limited number of simultaneous finger sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit** *limit*—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 clear-text service sessions and 10 IPv4 clear-text service sessions
- **rate-limit** *limit*—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For

example, a rate limit of 10 allows 10 IPv6 session connection attempts per minute and 10 IPv4 session connection attempts per minute.

You cannot include the **finger** statement on routers that run the Junos-FIPS software. We recommend that you do not use the finger service in a Common Criteria environment.

Configuring FTP Service for Remote Access to the Router or Switch

To configure the router or switch to accept FTP as an access service, include the **ftp** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
ftp {
  connection-limit limit;
  rate-limit limit;
}
```

By default, the router or switch supports a limited number of simultaneous FTP sessions and connection attempts per minute. You can include either or both of the following statements to change the defaults:

- **connection-limit** *limit*—Maximum number of simultaneous connections per protocol (IPV4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 FTP sessions and 10 IPv4 FTP sessions.
- **rate-limit** *limit*—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150.When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 FTP session connection attempts and 10 IPv4 FTP session connection attempts.

You can use passive FTP to access devices that accept only passive FTP services. All commands and statements that use FTP also accept passive FTP. Include the **ftp** statement at the **[edit system services]** hierarchy level to use either active FTP or passive FTP.

To start a passive FTP session, use **pasvftp** (instead of **ftp**) in the standard FTP format (**ftp://*destination***). For example:

```
request system software add pasvftp://name.com/jinstall.tgz
```

You cannot include the **ftp** statement on routers or switches that run the Junos-FIPS software. We recommend that you do not use the finger service in a Common Criteria environment.

Configuring SSH Service for Remote Access to the Router or Switch

To configure the router or switch to accept SSH as an access service, include the **ssh** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
```

```
ssh {
  ciphers [ cipher-1 cipher-2 cipher-3 ...]
  client-alive-count-max number;
  client-alive-interval seconds;
  connection-limit limit;
  hostkey-algorithm <algorithm | no-algorithm>;
  key-exchange algorithm;
  macs algorithm;
  max-sessions-per-connection number;
  no-passwords;
  no-tcp-forwarding;
  protocol-version [v1 v2] ;
  rate-limit limit;
  root-login <allow | deny | deny-password>;
}
```

By default, the router or switch supports a limited number of simultaneous SSH sessions and connection attempts per minute. Use the following statements to change the defaults:

- **connection-limit** *limit*—Maximum number of simultaneous connections per protocol (IPV4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of SSH sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 SSH sessions and 10 IPv4 SSH sessions.
- **max-sessions-per-connection** *number*—Include this statement to specify the maximum number of SSH sessions allowed per single SSH connection. This allows you to limit the number of cloned sessions tunneled within a single SSH connection. The default value is 10.
- **rate-limit** *limit*—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 SSH session connection attempts per minute and 10 IPv4 SSH session connection attempts per minute.

By default, a user can create an SSH tunnel over a CLI session to a router running Junos OS via SSH. This type of tunnel could be used to forward TCP traffic, bypassing any firewall filters or ACLs, allowing access to resources beyond the router. Use the **no-tcp-forwarding** option to prevent a user from creating an SSH tunnel to a router via SSH.

For information about other configuration settings, see the following topics:

- Configuring the Root Login Through SSH on page 19
- Configuring the SSH Protocol Version on page 20
- Configuring the Client Alive Mechanism on page 20

Configuring the Root Login Through SSH

By default, users are allowed to log in to the router or switch as **root** through SSH. To control user access through SSH, include the **root-login** statement at the **[edit systems services ssh]** hierarchy level:

```
[edit system services ssh]
root-login (allow | deny | deny-password);
```

allow—Allows users to log in to the router or switch as root through SSH. The default is **allow**.

deny—Disables users from logging in to the router or switch as root through SSH.

deny-password—Allows users to log in to the router or switch as root through SSH when the authentication method (for example, RSA) does not require a password.

Configuring the SSH Protocol Version

By default, both version 1 and version 2 of the SSH protocol are enabled. To configure the router or switch to use only version 1 of the SSH protocol, include the **protocol-version** statement and specify **v1** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
protocol-version [ v1 ];
```

To configure the router or switch to use only version 2 of the SSH protocol, include the **protocol-version** statement and specify **v2** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
protocol-version [ v2 ];
```

To explicitly configure the router or switch to use version 1 and 2 of the SSH protocol, include the **protocol-version** statement and specify **v1** and **v2** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
protocol-version [ v1 v2 ];
```

For J Series Services Routers, the export license software supports SSH version 1 only.

Configuring the Client Alive Mechanism

The client alive mechanism is valuable when the client or server depends on knowing when a connection has become inactive. It differs from the standard keepalive mechanism because the client alive messages are sent through the encrypted channel. The client alive mechanism is not enabled at default. To enable it, configure the **client-alive-count-max** and the **client-alive-interval**. This option applies to SSH protocol version 2 only.

In the following example, unresponsive SSH clients will be disconnected after approximately 100 seconds (20 x 5).

```
[edit system services ssh]
client-alive-count-max 5;
client-alive-interval 20;
```

Configuring Outbound SSH Service

You can configure a router or switch running the Junos OS to initiate a TCP/IP connection with a client management application that would be blocked if the client attempted to initiate the connection (for example, if the router or switch is behind a firewall). A single **outbound-ssh** configuration statement instructs the router or switch to create a TCP/IP connection with the client management application and to forward the identity of the router or switch. Once the connection is established, the management application initiates the SSH sequence as the client and the router or switch as the server that authenticates the client.

NOTE: There is no initiation command with outbound SSH. Once outbound SSH is configured and committed, the router or switch begins to initiate an outbound SSH connection based on the committed configuration. It continues to attempt to create this connection until successful. If the connection between the router or switch and the client management application is broken, the router or switch again attempts to create a new outbound SSH connection until successful. This connection is maintained until the outbound SSH stanza is removed from the configuration.

To configure the router or switch for outbound SSH connections, include the **outbound-ssh** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
outbound-ssh {
  client client-id {
    address address {
      port port-number;
      retry number;
      timeout seconds;
    }
    device-id device-id;
    keep-alive {
      retry number;
      timeout seconds;
    }
    reconnect-strategy (in-order | sticky);
    secret password;
    services netconf;
  }
  traceoptions {
    file filename <files number> <match regex> <size size> <world-readable |
      no-world-readable>;
    flag flag;
    no-remote-trace;
  }
```

}

The following topics describe the tasks for configuring the outbound-SSH service:

1. Configuring the Device Identifier for Outbound SSH Connections on page 22
2. Sending the Public SSH Host Key to the Outbound SSH Client on page 22
3. Configuring Keepalive Messages for Outbound SSH Connections on page 23
4. Configuring a New Outbound SSH Connection on page 24
5. Configuring the Outbound SSH Client to Accept NETCONF as an Available Service on page 24
6. Configuring Outbound SSH Clients on page 24

Configuring the Device Identifier for Outbound SSH Connections

Each time the router or switch establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the router or switch to the management client. Within this transmission is the value of *device-id*.

To configure the device identifier of the router or switch, include the **device-id** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
device-id device-id;
```

The initiation sequence when **secret** is not configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
```

Sending the Public SSH Host Key to the Outbound SSH Client

Each time the router or switch establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the router or switch to the management client. Within this transmission is the value of *device-id*.

To configure the device identifier of the router or switch, include the **device-id** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
device-id device-id;
```

The initiation sequence when **secret** is not configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
```

During the initialization of an SSH connection, the client authenticates the identity of the router or switch using the public SSH host key of the router or switch. Therefore, before the client can initiate the SSH sequence, it needs the public SSH key of the router or switch. When you configure the **secret** statement, the router or switch passes its public SSH key as part of the outbound SSH connection initiation sequence.

When the **secret** statement is set and the router or switch establishes an outbound SSH connection, the router or switch communicates its device ID, its public SSH key, and an SHA1 hash derived in part from the **secret** statement. The value of the **secret** statement is shared between the router or switch and the management client. The client uses the shared secret to authenticate the public SSH host key it is receiving to determine whether the public key is from the router or switch identified by the **device-id** statement.

Using the **secret** statement to transport the public SSH host key is optional. You can manually transport and install the public key onto the client system.

NOTE: Including the secret statement means that the router or switch sends its public SSH host key every time it establishes a connection to the client. It is then up to the client to decide what to do with the SSH host key if it already has one for that router or switch. We recommend that you replace the client's copy with the new key. Host keys can change for various reasons and by replacing the key each time a connection is established, you ensure that the client has the latest key.

To send the router's or switch's public SSH host key when the router or switch connects to the client, include the **secret** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
secret password;
```

The following message is sent by the router or switch when the **secret** attribute is configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
HOST-KEY: <public-hot-key>\r\n
HMAC:<HMAC(pub-SSH-host-key, <secret>>)>\r\n
```

Configuring Keepalive Messages for Outbound SSH Connections

Once the client application has the router's or switch's public SSH host key, it can then initiate the SSH sequence as if it had created the TCP/IP connection and can authenticate the router or switch using its copy of the router's or switch's public host SSH key as part of that sequence. The router or switch authenticates the client user through the mechanisms supported in the Junos OS (RSA/DSA public string or password authentication).

To enable the router or switch to send SSH protocol keepalive messages to the client application, configure the **keep-alive** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
keep-alive {
    retry number;
    timeout seconds;
```

```
}
```

The **timeout** statement specifies how long the router or switch waits to receive data before sending a request for acknowledgment from the application. The default is 15 seconds.

The **retry** statement specifies how many keepalive messages the router sends without receiving a response from the client. When that number is exceeded, the router or switch disconnects from the application, ending the outbound SSH connection. The default is three retries.

Configuring a New Outbound SSH Connection

When disconnected, the router or switch begins to initiate a new outbound SSH connection. To specify how the router or switch reconnects to the server after a connection is dropped, include the **reconnect-strategy** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client-id]
reconnect-strategy (sticky | in-order);
```

The **sticky** option configures the router or switch to reconnect to the server from which it disconnected.

The **in-order** option configures the router or switch to reconnect to the first configured server. If this server is unavailable, the router or switch tries to connect to the next configured server. This process repeats until a connection is completed.

You can also specify the number of retry attempts and set the amount of time before the reconnection attempts stop. See "Configuring Keepalive Messages for Outbound SSH Connections" on page 23.

Configuring the Outbound SSH Client to Accept NETCONF as an Available Service

To configure the application to accept NETCONF as an available service, include the **services netconf** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
services {
  netconf;
}
```

Configuring Outbound SSH Clients

To configure the clients available for this outbound SSH connection, list each client with a separate address statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
  address address {
    retry number;
    timeout seconds;
    port port-number;
  }
```

The **client *client-id*** value is not forwarded to the client management application. This value serves to uniquely identify the **outbound-ssh** configuration stanza. Each **outbound-ssh** stanza represents a single outbound SSH connection. Thus, the administrator is free to assign the **client-id** any meaningful unique value.

The **address *address*** statement is the IP address or host name of the client.

The **timeout** statement specifies how long the application waits between attempts to reconnect to the specified IP address, in seconds. The default is 15 seconds.

The **retry** statement specifies how many connection attempts a router or switch can make to the specified IP address. The default is 3.

The **port** statement specifies the port at which a server listens for outbound SSH connection requests.

Configuring NETCONF-Over-SSH Connections on a Specified TCP Port

The Junos OS enables you to restrict incoming NETCONF connections to a specified TCP port without configuring a firewall. To configure the TCP port used for NETCONF-over-SSH connections, include the **port** statement at the **[edit system services netconf ssh]** hierarchy level. The configured port accepts only NETCONF-over-SSH sessions. Regular SSH session requests for this port are rejected.

You can either configure the default port 830 for NETCONF connections over SSH, as specified in RFC 4742, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)*, or configure any port from 1 through 65535.

NOTE:

- The default SSH port (22) continues to accept NETCONF sessions even with a configured NETCONF server port. To disable the SSH port from accepting NETCONF sessions, specify this in the login event script.
- We do not recommend configuring the default ports for FTP (21) and Telnet (23) services for configuring NETCONF-over-SSH connections.

Related Documentation

- port (NETCONF Server) on page 117

Configuring Telnet Service for Remote Access to a Router or Switch

To configure the router or switch to accept Telnet as an access service, include the **telnet** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
telnet {
   connection-limit limit;
   rate-limit limit;
}
```

By default, the router or switch supports a limited number of simultaneous Telnet sessions and connection attempts per minute.

Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit** *limit*—Maximum number of simultaneous connections per protocol (IPV4 and IPv6). The range is from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of telnet sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 telnet sessions and 10 IPv4 telnet sessions.
- **rate-limit** *limit*—Maximum number of connection attempts accepted per minute (from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 telnet session connection attempts per minute and 10 IPv4 telnet session connection attempts per minute.

You cannot include the **telnet** statement on devices that run the Junos-FIPS software. We recommend that you do not use Telnet in a Common Criteria environment.

Related Documentation

- telnet on page 170

Configuring clear-text or SSL Service for Junos XML Protocol Client Applications

A Junos XML protocol client application can use one of four protocols to connect to the Junos XML protocol server on a router: clear-text (a Junos XML protocol-specific protocol for sending unencrypted text over a TCP connection), SSH, SSL, or Telnet. For clients to use the clear-text or SSL protocol, you must include Junos XML protocol-specific statements in the router configuration.

For more information, see the following topics:

1. Configuring clear-text Service for Junos XML Protocol Client Applications on page 26
2. Configuring SSL Service for Junos XML Protocol Client Applications on page 27

Configuring clear-text Service for Junos XML Protocol Client Applications

To configure the router to accept clear-text connections from Junos XML protocol client applications on port 3221, include the **xnm-clear-text** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
xnm-clear-text {
  connection-limit limit;
  rate-limit limit;
}
```

By default, the Junos XML protocol server supports a limited number of simultaneous clear-text sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit** *limit*—Maximum number of simultaneous connections per protocol (IPv4 and IPv6) (a value from 1 through 250). The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 clear-text service sessions and 10 IPv4 clear-text service sessions.
- **rate-limit** *limit*—Maximum number of connection attempts accepted per minute per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 session connection attempts per minute and 10 IPv4 session connection attempts per minute.

You cannot include the **xnm-clear-text** statement on routers that run the Junos-FIPS software. We recommend that you do not use the clear-text protocol in a Common Criteria environment.

Configuring SSL Service for Junos XML Protocol Client Applications

To configure the router to accept SSL connections from Junos XML protocol client applications on port 3220, include the **xnm-ssl** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
xnm-ssl {
    local-certificate name;
    connection-limit limit;
    rate-limit limit;
}
```

local-certificate is the name of the X.509 authentication certificate used to establish an SSL connection. You must obtain the certificate and copy it to the router before referencing it.

By default, the Junos XML protocol server supports a limited number of simultaneous SSL sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit** *limit*—Maximum number of simultaneous connections per protocol (IPV4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 SSL sessions and 10 IPv4 SSL sessions.
- **rate-limit** *limit*—Maximum number of connection attempts accepted per protocol per minute. The range is a value from 1 through 250. The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 SSL session connection attempts per minute and 10 IPv4 SSL session connection attempts per minute.

Configuring the Junos OS to Work with SRC Software

You can enable Junos OS to work with the Session and Resource Control (SRC) software. The SRC software supports dynamic service activation engine (SAE) functionality on routers and switches running under Junos OS. To do this, include the following statements at the **[edit system services service-deployment]** hierarchy level:

```
[edit system services service-deployment]
servers server-address {
  port port-number;
}
source-address source-address;
```

server-address is the IPv4 address of the SRC server.

By default, *port-number* is set to 3333 and is a TCP port number.

source-address is optional and is the local IP version 4 (IPv4) address to be used as the source address for traffic to the SRC server.

NOTE: By default, when a connection between SRC and a Juniper Networks router or switch is established, the SRC process (sdxd) starts a Junos XML protocol session as **user root**. You have the option of configuring **user sdx** with a different classification at the **[edit system login]** hierarchy level.

For more information about SRC software, see the SRC documentation set.

Related Documentation

- Configuring Finger Service for Remote Access to the Router on page 17
- Configuring FTP Service for Remote Access to the Router or Switch on page 18
- Configuring SSH Service for Remote Access to the Router or Switch on page 18
- Configuring Outbound SSH Service on page 21
- Configuring NETCONF-Over-SSH Connections on a Specified TCP Port on page 25
- Configuring Telnet Service for Remote Access to a Router or Switch on page 25
- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 26

CHAPTER 4

Configuring DHCP Services for IP Address Management

Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers

The Dynamic Host Configuration Protocol (DHCP) server provides a framework for passing configuration information to client hosts (such as PCs) on a TCP/IP network. On J Series Services Routers and EX Series switches, a router, switch, or interface that acts as a DHCP server can allocate network IP addresses and deliver configuration settings to client hosts without user intervention. DHCP access service minimizes the overhead required to add clients to the network by providing a centralized, server-based setup. You do not have to manually create and maintain IP address assignments for clients. DHCP is defined in RFC 2131, *Dynamic Host Configuration Protocol*.

A J Series router or EX Series switch configured as a DHCP server is compatible with the autoinstallation feature.

To configure a J Series router or EX Series switch to accept DHCP as an access service, include the dhcp statement at the **[edit system services]** hierarchy level:

```
[edit system services]
dhcp {
  boot-file filename;
  boot-server (address | hostname);
  domain-name domain-name;
  domain-search [domain-list];
  default-lease-time;
  maximum-lease-time;
  name-server {
    address;
  }
  option {
    [ (id-number option-type option-value) | (id-number array option-type option-value) ];
  }
  pool address/prefix-length) {
    address-range {
      low address;
      high address;
    }
    exclude-address {
      address;
    }
  }
  router {
    address;
  }
  static-binding mac-address {
    fixed-address {
      address;
    }
    host-name hostname;
    client-identifier (ascii client-id | hexadecimal client-id);
  }
  server-identifier address;
```

```
    wins-server {
      address;
    }
  }
```

Related Documentation

- DHCP Access Service Overview on page 6
- DHCP Statement Hierarchy and Inheritance on page 9

Configuring Address Pools for DHCP Dynamic Bindings

For dynamic bindings, set aside a pool of IP addresses that can be assigned to clients. Addresses in a pool must be available to clients on the same subnet.

To configure an address pool, include the following statements at the **[edit system services dhcp]** hierarchy level:

```
[edit system services dhcp]
pool address</prefix-length> {
  address-range {
    low address;
    high address;
  }
  exclude-address {
    address;
  }
}
```

The pool definition must include the client subnet number and prefix length (in bits). Optionally, the definition can include an address range and a list of excluded addresses.

The **address-range** statement defines the lowest and highest IP addresses in the pool that are available for dynamic address assignment. This statement is optional. If no range is specified, the pool will use all available addresses within the subnet specified. (Broadcast addresses, interface addresses, and excluded addresses are not available.)

The **exclude-address** statement specifies addresses within the range that are not used for dynamic address assignment. You can exclude one or more addresses within the range. This statement is optional.

The following is an example of a pool configuration.

```
[edit system services dhcp]
pool 10.3.3.0/24 {
  address-range low 10.3.3.2 high 10.3.3.254;
  exclude-address {
    10.3.3.33;
  }
}
```

For dynamic address assignment, configure an address pool for each client subnet the DHCP server supports. You can configure multiple address pools for a DHCP server, but only one address range per pool is supported.

DHCP maintains the state information for all pools configured. Clients are assigned addresses from pools with subnets that match the interface on which the **DHCPDISCOVER** packet is received. When more than one pool exists on the same interface, addresses are assigned on a rotating basis from all available pools.

Related Documentation

- DHCP Access Service Overview on page 6
- Configuring Manual (Static) DHCP Bindings Between a Fixed IP Address and a Client MAC Address on page 32

Configuring Manual (Static) DHCP Bindings Between a Fixed IP Address and a Client MAC Address

Static bindings provide configuration information for specific clients. This information can include one or more fixed Internet addresses, the client hostname, and a client identifier.

To configure static bindings, include the following statements at the **[edit system services dhcp]** hierarchy level:

```
[edit system services dhcp]
static-binding mac-address {
    fixed-address {
        address;
    }
    host client-hostname;
    client-identifier (ascii client-id | hexadecimal client-id);
}
```

A static binding defines a mapping between a fixed IP address and the client's MAC address.

The *mac-address* variable specifies the MAC address of the client. This is a hardware address that uniquely identifies each client on the network.

The **fixed-address** statement specifies the fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.

The **host** statement specifies the hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the **domain-name** statement.

The **client-identifier** statement is used by the DHCP server to index the database of address bindings. The client identifier is either an ASCII string or hexadecimal digits. It can include a type-value pair as specified in RFC 1700, *Assigned Numbers*. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.

NOTE: For each unique **client-identifier** *client-id* value, the DHCP server issues a unique lease and IP address from the pool. Previously, when the client provided an incorrect **client-identifier** *client-id* value, the DHCP server did not issue a lease.

The following is an example of a static binding configuration:

```
[edit system services dhcp]
static-binding 00:0d:56:f4:01:ab {
  fixed-address {
    10.5.5.5;
    10.6.6.6;
  }
  host-name "another-host.domain.tld";
  client-identifier hexadecimal 01001122aabbcc;
}
```

Related Documentation

- DHCP Access Service Overview on page 6
- Specifying DHCP Lease Times for IP Address Assignments on page 33

Specifying DHCP Lease Times for IP Address Assignments

For clients that do not request a specific lease time, the default lease time is one day. You can configure a maximum lease time for IP address assignments or change the default lease time.

To configure lease times, include the **maximum-lease-time** and **default-lease-time** statements:

```
maximum-lease-time;
default-lease-time;
```

You can include these statements at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

Lease times defined for static bindings and address pools take priority over lease times defined at the **[edit system services dhcp]** hierarchy level.

The **maximum-lease-time** statement configures the maximum length of time in seconds for which a client can request and hold a lease. If a client requests a lease longer than the maximum specified, the lease is granted only for the maximum time configured on the server. After a lease expires, the client must request a new lease.

NOTE: Maximum lease times do not apply to dynamic BOOTP leases. These leases are not specified by the client and can exceed the maximum lease time configured.

The following example shows a configuration for maximum and default lease times:

```
[edit system services dhcp]
maximum-lease-time 7200;
default-lease-time 3600;
```

Related Documentation

- DHCP Access Service Overview on page 6
- Configuring a DHCP Boot File and DHCP Boot Server on page 34

Configuring a DHCP Boot File and DHCP Boot Server

When a DHCP client starts, it contacts a boot server to download the boot file.

To configure a boot file and boot server, include the **boot-file** and **boot-server** statements:

```
boot-file filename;
boot-server (address | hostname);
```

You can include these statements at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

After a client receives a **DHCPOFFER** response from a DHCP server, the client can communicate directly with the boot server (instead of the DHCP server) to download the boot file. This minimizes network traffic and enables you to specify separate boot server/file pairs for each client pool or subnetwork.

The **boot-file** statement configures the name and location of the initial boot file that the DHCP client loads and executes. This file stores the boot image for the client. In most cases, the boot image is the operating system the client uses to load.

The **boot-server** statement configures the IP address of the TFTP server that contains the client's initial boot file. You must configure an IP address or a hostname for the server.

You must configure at least one boot file and boot server. Optionally, you can configure multiple boot files and boot servers. For example, you might configure two separate boot servers and files: one for static binding and one for address pools. Boot file configurations for pools or static bindings take precedence over boot file configurations at the **[edit system services dhcp]** hierarchy level.

The following example specifies a boot file and server for an address pool:

```
[edit system services dhcp]
pool 10.4.4.0/24 {
   boot-file "boot.client";
   boot-server 10.4.4.1;
}
```

Related Documentation

- DHCP Access Service Overview on page 6
- Configuring a Static IP Address as DHCP Server Identifier on page 35

Configuring the Next DHCP Server to Contact After a Boot Client Establishes Initial Communication

On J Series Services Routers, you can configure the next DHCP server to contact after a DHCP boot client establishes initial communication. You can use this option to specify the IP address of the DHCP server that is used as the "siaddr" in a DHCP protocol packet.

To configure the next server, include the **next-server** ***next-server*** statement at one of the following hierarchy levels:

- **[edit system services dhcp]**
- **[edit system services dhcp pool** ***pool-id*****]**
- **[edit system services dhcp static-binding** ***mac-address*****]**

```
[edit system services dhcp]
next-server next-server;

[edit system services dhcp pool pool-id]
next-server next-server;

[edit system services dhcp static-binging mac-address]
next-server next-server;
```

Related Documentation

- next-server on page 104

Configuring a Static IP Address as DHCP Server Identifier

The host running the DHCP server must itself use a manually assigned, static IP address. It cannot send a request and receive an IP address from itself or another DHCP server.

To configure a DHCP server identifier, include the **server-identifier** statement:

```
server-identifier address;
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The **server-identifier** statement specifies the IP address of the DHCP server. The host must be a TFTP server that is accessible by all clients served within a range of IP addresses (based on either an address pool or static binding).

The following example shows a DHCP server identifier configured for an address pool:

```
[edit system services dhcp]
pool 10.3.3.0/24 {
   address-range low 10.3.3.2 high 10.3.3.254;
   exclude-address {
      10.3.3.33;
   }
```

```
    router {
      10.3.3.1;
    }
    server-identifier 10.3.3.1;
}
```

Related Documentation
- DHCP Access Service Overview on page 6

Configuring a Domain Name and Domain Search List for a DHCP Server Host

To configure the name of the domain in which clients search for a DHCP server host, include the **domain-name** statement:

```
domain-name domain;
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The **domain-name** statement sets the domain name that is appended to hostnames that are not fully qualified. This statement is optional. If you do not configure a domain name, the default is the client's current domain.

To configure a domain search list, include the **domain-search** statement:

```
domain-search [ domain-list ];
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The **domain-search** statement sets the order in which clients append domain names when searching for the IP address of a host. You can include one or more domain names in the list. For more information, see RFC 3397, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*.

The **domain-search** statement is optional, if you do not configure a domain search list, the default is the client's current domain.

Related Documentation
- DHCP Access Service Overview on page 6

Configuring Routers Available to the DHCP Client

After a DHCP client loads the boot image and has booted, the client sends packets to a router.

To configure routers available to the DHCP client, include the **router** statement:

```
router {
```

```
    address;
}
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The **router** statement specifies a list of IP addresses for routers on the client's subnet. List routers in order of preference. You must configure at least one router for each client subnet.

The following example shows routers configured at the **[edit system services dhcp]** hierarchy level:

```
[edit system services dhcp]
router {
    10.6.6.1;
    10.7.7.1;
}
```

Related Documentation

- DHCP Access Service Overview on page 6

Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server

You can configure one or more user-defined options that are not included in the Junos default implementation of the DHCP server. For example, if a client requests a DHCP option that is not included in the DHCP server, you can create a user-defined option that enables the server to respond to the client's request.

To configure a user-defined DHCP option, include the **option** statement:

```
option {
    [ (id-number option-type option-value) | (id-number array option-type option-value) ];
}
```

The **option** statement specifies the following values:

- *id-number*—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.
- *option-type*—Any of the following types: **byte**, **byte-stream**, **flag**, **integer**, **ip-address**, **short**, **string**, **unsigned-integer**, **unsigned-short**.
- *array*—An option can include an array of values.
- *option-value*—Value associated with an option. The option value must be compatible with the option type (for example, an **On** or **Off** value for a **flag** type).

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
```

```
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The following example shows user-defined DHCP options:

```
[edit system services dhcp]
option 19 flag off; # 19: "IP Forwarding" option
option 40 string "domain.tld"; # 40: "NIS Domain" option
option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
```

User-defined options that conflict with DHCP configuration statements are ignored by the server. For example, in the following configuration, the DHCP server ignores the user-defined **option 3 router** statement and uses the **router** statement instead:

```
[edit system services dhcp]
option 3 router 10.7.7.2; # 3: "Default Router" option
router {
  10.7.7.1;
}
```

Related Documentation

- DHCP Access Service Overview on page 6

Configuring Tracing Operations for DHCP Processes

DHCP tracing operations track all DHCP operations and record them to a log file. By default, no DHCP processes are traced. If you include the **traceoptions** statement at the **[edit system services dhcp]** hierarchy level, the default tracing behavior is the following:

- Important events are logged in a file called **dhcpd** located in the **/var/log** directory.
- When the file **dhcpd** reaches 128 kilobytes (KB), it is renamed **dhcpd.0**, then **dhcpd.1**, and so on, until there are three trace files. Then the oldest trace file (**dhcpd.2** is overwritten). For more information about how log files are created, see the *Junos OS System Log Messages Reference*.
- Log files can be accessed only by the user who configures the tracing operation.

You cannot change the directory in which trace files are located. However, you can customize the other trace file settings by including the following statements at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file filename <files number> <match regex> <size size> <world-readable |
  no-world-readable>;
flag {
  all;
}
```

Tasks for configuring DHCP tracing operations are:

1. Configuring the DHCP Processes Log Filename on page 39
2. Configuring the Number and Size of DHCP Processes Log Files on page 39
3. Configuring Access to the DHCP Log File on page 39

4. Configuring a Regular Expression for Refining the Output of DHCP Logged Events on page 39
5. Configuring DHCP Trace Operation Events on page 40

Configuring the DHCP Processes Log Filename

By default, the name of the file that records trace output is **dhcpd**. You can specify a different name by including the file statement at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file filename;
```

Configuring the Number and Size of DHCP Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed ***filename*.0**, then ***filename*.1**, and so on, until there are three trace files. Then the oldest trace file (***filename*.2**) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracking operation (***filename***) reaches 2 MB, ***filename*** is renamed ***filename*.0**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0** is renamed ***filename*.1** and ***filename*** is renamed ***filename*.0**. This process repeats until there are 20 trace files. Then the oldest file (***filename*.19**) is overwritten by the newest file (***filename*.0**).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10KB through 1 gigabyte (GB).

Configuring Access to the DHCP Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file world-readable;
```

To set the default behavior explicitly, include the **file no-world-readable statement** at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file no-world readable;
```

Configuring a Regular Expression for Refining the Output of DHCP Logged Events

By default, the trace operations output includes all lines relevant to the logged events.

You can refine the output by including the match statement at the **[edit system services dhcp traceoptions file *filename*]** hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system services dhcp traceoptions]
file filename match regex;
```

Configuring DHCP Trace Operation Events

By default, only important events are logged. You can configure the trace operations to be logged by including the following options at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit dhcp system services dhcp traceoptions]
flag {
    all;
    binding;
    config;
    conflict;
    event;
    ifdb;
    io;
    lease;
    main;
    misc;
    packet;
    options;
    pool;
    protocol;
    rtsock;
    scope;
    signal;
    trace;
    ui;
}
```

DHCP Processes Tracing Flags

Table 5 on page 40 describes which operation or event is recorded by each DHCP tracing flag. By default, all flags are disabled.

Table 5: DHCP Processes Tracing Flags

Flag	Operation or Event
all	All operations.
binding	Binding operations.
config	Logins to the configuration database.
conflict	Client-detected conflicts for IP addresses.
event	Important events.

Table 5: DHCP Processes Tracing Flags *(continued)*

Flag	Operation or Event
ifdb	Interface database operations.
io	I/O operations.
lease	Lease operations.
main	Main loop operations.
misc	Miscellaneous operations.
packet	DHCP packets.
options	DHCP options.
pool	Address pool operations.
protocol	Protocol operations.
rtsock	Routing socket operations.
scope	Scope operations.
signal	DHCP signal operations.
trace	Tracing operations.
ui	User interface operations.

Example: Complete DHCP Server Configuration

This topic shows a complete DHCP server configuration with address pools, static bindings, and user-defined options.

The following example shows statements at the **[edit interfaces]** hierarchy level. The interface's primary address (**10.3.3.1/24**) has a corresponding address pool (**10.3.3.0/24**) defined at the **[edit system services]** hierarchy level.

```
[edit interfaces]
fe-0/0/1 {
    unit 0 {
        family inet {
            address 10.3.3.1/24;
        }
    }
}
```

NOTE: You can configure a DHCP server only on an interface's primary IP address.

Statements at the **[edit system services]** hierarchy level include the following:

```
[edit system services]
dhcp {
    domain-name "domain.tld";
    maximum-lease-time 7200;
    default-lease-time 3600;
    name-server {
        10.6.6.6;
        10.6.6.7;
    }
    domain-search [ subnet1.domain.tld subnet2.domain.tld ];
    wins-server {
        10.7.7.7;
        10.7.7.9;
    }
    router {
        10.6.6.1;
        10.7.7.1;
    }
    option 19 flag off; # 19: "IP Forwarding" option
    option 40 string "domain.tld"; # 40: "NIS Domain" option
    option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
    pool 10.3.3.0/24 {
        address-range low 10.3.3.2 high 10.3.3.254;
        exclude-address {
            10.3.3.33;
        }
        router {
            10.3.3.1;
        }
        server-identifier 10.3.3.1;
    }
    pool 10.4.4.0/24 {
        boot-file "boot.client";
        boot-server 10.4.4.1;
    }
    static-binding 00:0d:56:f4:20:01 {
        fixed-address 10.4.4.4;
        host-name "host.domain.tld";
    }
    static-binding 00:0d:56:f4:01:ab {
        fixed-address {
            10.5.5.5;
            10.6.6.6;
        }
        host-name "another-host.domain.tld";
        client-identifier "01aa.001a.bc65.3e";
    }
}
```

Example: Viewing DHCP Address Pools

Use the CLI **show system services dhcp pool** command to view information about DHCP address pools.

The following example show address pools configured on a DHCP server:

```
user@ host> show system services dhcp pool
Pool name        Low address     High address     Excluded addresses
10.40.1.0/24     10.40.1.1       10.40.1.254      10.40.1.254
```

Example: Viewing DHCP Bindings

Use the CLI command **show system services dhcp binding** to view information about DHCP address bindings, lease times, and address conflicts.

The following example shows the binding type and lease expiration times for IP addresses configured on a router that supports a DHCP server:

```
user@host> show system services dhcp binding
IP Address       Hardware Address     Type    Lease expires at
192.168.1.2      00:a0:12:00:12:ab       static      never
192.168.1.3      00:a0:12:00:13:02       dynamic     2004-05-03 13:01:42 PDT
```

Enter an IP address to show binding for a specific IP address:

```
user@host> show system services dhcp binding 192.168.1.3
DHCP binding information:
IP address      192.168.1.3
Hardware address      00:a0:12:00:12:ab
Client identifier
61 63 65 64 2d 30 30 3a 61 30 3a 31 32 3a 30 30 aced-00:a0:12:00
3a 31 33 3a 30 32
Lease information:
Type       dynamic
Obtained at       2004-05-02 13:01:42 PDT
Expires at       2004-05-03 13:01:42 PDT
```

Use the **detail** option to show detailed binding information:

```
user@host> show system services dhcp binding detail
DHCP binding information:
IP address                 192.168.1.3
Hardware address           00:a0:12:00:12:ab
Pool                       192.168.1.0/24
Interface                  fe-0/0/0, relayed by 192.168.4.254
Lease information:
Type                       dynamic
Obtained at                2004-05-02 13:01:42 PDT
Expires at                 2004-05-03 13:01:42 PDT
DHCP options:
name-server foo.mydomain.tld
domain-name mydomain.tld
option 19 flag off
```

Example: Viewing and Clearing DHCP Conflicts

When the DHCP server provides an IP address, the client performs an ARP check to make sure the address is not being used by another client and reports any conflicts back to the server. The server keeps track of addresses with conflicts and removes them from the address pool. Use the CLI command **show system services dhcp conflict** to show conflicts.

```
user@host> show system services dhcp conflict
Detection time                  Detection method       Address
2004-08-03 19:04:00 PDT         client      192.168.1.5
2004-08-04 04:23:12 PDT         ping      192.168.1.8
```

Use the **clear system services dhcp conflicts** command to clear the conflicts list and return IP addresses to the pool. The following command shows how to clear an address on the server that has a conflict:

```
user@host> clear system services dhcp conflict 192.168.1.5
```

For more information about CLI commands you can use with the DHCP server, see the CLI Explorer.

Configuring the Router as an Extended DHCP Local Server

You can enable the router to function as an extended DHCP local server and configure the extended DHCP local server options on the router. The extended DHCP local server provides an IP address and other configuration information in response to a client request.

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients. See *Configuring Address-Assignment Pools* for details about creating and using address-assignment pools.

NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

You cannot configure the extended DHCP local server and extended DHCP relay on the same interface.

To configure the extended DHCP local server on the router, include the **dhcp-local-server** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
dhcp-local-server {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      mac-address;
      option-60;
```

```
        option-82 <circuit-id> <remote-id>;
        routing-instance-name;
        user-prefix user-prefix-string;
      }
    }
    group group-name {
      authentication {
        password password-string;
        username-include {
          circuit-type;
          delimiter delimiter-character;
          domain-name domain-name-string;
          logical-system-name;
          mac-address;
          option-60;
          option-82 <circuit-id> <remote-id>;
          routing-instance-name;
          user-prefix user-prefix-string;
        }
      }
      interface interface-name <upto upto-interface-name> <exclude>;
    }
    pool-match-order {
      ip-address-first;
      option-82;
    }
  }
```

You can also include these statements at the following hierarchy levels:

- **[edit logical-systems *logical-system-name* system services]**
- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services]**
- **[edit routing-instances *routing-instance-name* system services]**

In addition, you can configure tracing for DHCP local server operations by including the **traceoptions** statement at the **[edit system processes dhcp-service]** hierarchy level:

```
[edit system processes]
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  level  (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

NOTE: The extended DHCP local server is incompatible with the J Series router DHCP server. As a result, the DHCP local server and the DHCP or BOOTP relay agent cannot both be enabled on the router at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

Related Documentation

- Example: Configuring the Minimum Extended DHCP Local Server Configuration on page 47
- Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 47

Example: Configuring the Minimum Extended DHCP Local Server Configuration

The following example shows the minimum configuration you need to use the extended DHCP local server on the router:

This example creates the server group named **group_one**, and specifies that the DHCP local server is enabled on interface **fe-0/0/2.0** within the group. The DHCP local server uses the default pool match configuration of **ip-address-first.**

```
[edit system services]
dhcp-local-server {
   group group_one {
      interface fe-0/0/2.0;
   }
}
```

Example: Extended DHCP Local Server Configuration with Optional Pool Matching

The following example shows an extended DHCP local server configuration that includes optional pool matching and interface groups. This configuration specifies that the DHCP local server uses option 82 information to match the named address range for client IP address assignment. The option 82 matching must also be included in the address-assignment pool configuration.

```
[edit system services]
dhcp-local-server {
   group group_one {
      interface fe-0/0/2.0;
      interface fe-0/0/2.1;
   }
   group group_two {
      interface fe-0/0/3.0;
      interface fe-0/0/3.1;
   }
   pool-match-order {
      ip-address-first:
      option-82:
   }
}
```

Verifying and Managing the DHCP Server Configuration

To display the client address bindings for the extended DHCP local server, use the following operational commands:

- **show dhcp server binding**
- **show dhcp server statistics**

To clear client address bindings and DHCP local server statistics, use the following operational commands:

- **clear dhcp server binding**
- **clear dhcp server statistics**

For information about using these operations commands, see the *Junos System Basics and Services Reference*.

Using External AAA Authentication Services to Authenticate DHCP Clients

Both the extended DHCP local server and the extended DHCP relay agent support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.

NOTE: This topic uses the term extended DHCP application to refer to both the extended DHCP local server and the extended DHCP relay agent.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors the logout and views it as if it was requested by a CLI management command. All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the **authentication-server** statement at the **[edit access profile *profile-name*]** hierarchy level.

Tasks for configuring External AAA authentication services are:

1. Configuring Authentication Support for an Extended DHCP Application on page 48
2. Grouping Interfaces with Common DHCP Configurations on page 50
3. Configuring Passwords for Usernames the DHCP Application Presents to the External AAA Authentication Service on page 51
4. Creating Unique Usernames the Extended DHCP Application Passes to the External AAA Authentication Service on page 51

Configuring Authentication Support for an Extended DHCP Application

To configure authentication support for an extended DHCP application, include the **authentication** statement at these hierarchy levels. You can configure either global authentication support or group-specific support.

You must configure the **username-include** statement to enable the use of authentication. The **password** statement is not required and does not cause DHCP to use authentication if the **username-include** statement is not included.

Extended DHCP local server hierarchies:

- [edit system services dhcp-local-server]
- [edit system services dhcp-local-server group *group-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*]
- [edit logical-systems *logical-system-name* system services dhcp-local-server]
- [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*]
- [edit routing-instances *routing-instance-name* system services dhcp-local-server]
- [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*]

Extended DHCP relay agent hierarchies:

- [edit forwarding-options dhcp-relay]
- [edit forwarding-options dhcp-relay group *group-name*]
- [edit logical-systems *logical-system-name* forwarding-options dhcp-relay]
- [edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name*]
- [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay]
- [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name*]

```
authentication {
  password password-string;
  username-include {
    circuit-type;
    delimiter delimiter-character;
    domain-name domain-name-string;
    logical-system-name;
    mac-address;
    option-60;
```

```
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
```

Grouping Interfaces with Common DHCP Configurations

The extended DHCP applications enable you to group together a set of interfaces and apply a common DHCP configuration to the named interface group.

To configure an interface group, use the **group** statement.

```
group group-name {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  interface interface-name <upto upto-interface-name> <exclude>;
}
```

You can specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the **interface *interface-name*** statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. For example:

```
group boston {
  interface 192.168.10.1;
  interface 192.168.15.5;
}
```

You can use the *upto* option to specify a range of interfaces on which the extended DHCP application is enabled. For example:

```
group quebec {
  interface 192.168.10.1 upto 192.168.10.255;
}
```

You can use the **exclude** option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
group paris {
  interface 192.168.100.1 exclude;
  interface 192.168.100.100 upto 192.168.100.125 exclude;
}
```

Configuring Passwords for Usernames the DHCP Application Presents to the External AAA Authentication Service

You can configure an optional password that the extended DHCP application presents to the external AAA authentication service to authenticate the specified username.

To configure a password that authenticates the username, use the **password** statement. See *Special Requirements for Junos OS Plain-Text Passwords* for information about supported characters in passwords. For example:

```
authentication {
  password myPassworD1234;
}
```

Creating Unique Usernames the Extended DHCP Application Passes to the External AAA Authentication Service

You can configure the extended DHCP application to include additional fields in the username passed to the external AAA authentication service when the DHCP client logs in. This additional information enables you to construct usernames that uniquely identify subscribers.

NOTE: No authentication is performed if you do not include a username in the authentication configuration; however, the IP address is provided by the local pool if it is configured.

To configure unique usernames, use the **username-include** statement. You can include any or all of the additional statements.

```
authentication {
  username-include {
    circuit-type;
    delimiter delimiter-character;
    domain-name domain-name-string;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    routing-instance-name;
    user-prefix user-prefix-string;
  }
}
```

The following list describes the attributes that can be included as part of the username:

- **circuit-type**—The circuit type used by the DHCP client, for example **enet**.
- **delimiter**—The delimiter character that separates components that make up the concatenated username. The semicolon (;) is not supported as a delimiter character.
- **domain-name**—The client domain name as string. The router adds the @ delimiter to the username.

- **logical-system-name**—The name of the logical system, if the receiving interface is in a logical system.
- **mac-address**—The client MAC address, in a string of format ***xxxx.xxxx.xxxx***.
- **option-60**—The portion of the option 60 payload that follows the length field.
- **option-82 <circuit-id> <remote-id>**—The specified contents of the option 82 payload.
  - **circuit-id**—The payload of the agent circuit ID suboption.
  - **remote-id**—The payload of the Agent Remote ID suboption.
  - Both **circuit-id** and **remote-id**—The payloads of both suboptions, in the format: **circuit-id[delimiter]remote-id**.
  - Neither **circuit-id** or **remote-id**—The raw payload of the option 82 from the PDU is concatenated to the username.
- **routing-instance-name**—The name of the routing instance, if the receiving interface is in a routing instance.
- **user-prefix**—A string indicating the user prefix.

The router creates the unique username by including the specified additional information in the following order, with the fields separated by a delimiter. The default delimiter is a period (.). You can specify a different delimiter; however, the semicolon character (;) is not allowed.

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]
routing-instance-name[delimiter]circuit-type[delimiter]option-82[delimiter]
option-60@domain-name
```

The following example shows a sample configuration that creates a unique username. The username is shown after the configuration.

```
authentication {
  username-include {
    circuit-type;
    domain-name isp55.com;
    mac-address;
    user-prefix wallybrown;
  }
}
```

The resulting unique username is:

```
wallybrown.0090.1a01.1234.enet@isp55.com
```

Tracing Extended DHCP Local Server Operations

The extended DHCP tracing operations track the extended DHCP local server operations and record them in a log file. By default, no extended DHCP local server processes are traced. If you include the **traceoptions** statement at the **[edit system processes dhcp-service]** hierarchy level, the default tracing behavior is the following:

- Important extended DHCP local server events are logged in a file called **jdhcpd** located in the **/var/log** directory.
- When the file **jdhcpd** reaches 128 kilobytes (KB), it is renamed **jdhcpd.0**, then **jdhcpd.1**, and so on, until there are three trace files. Then the oldest trace file (**jdhcpd.2**) is overwritten. For more information about how log files are created, see the *Junos System Log Messages Reference*.
- Log files can be accessed only by the user who configures the tracing operation.

NOTE: In software releases earlier than Junos OS 11.4, you configured tracing statements at the **[edit system services dhcp-local-server]** and **[edit forwarding-options dhcp-relay]** hierarchy levels. Starting in Junos OS Release 11.4, these statements have been deprecated and hidden in favor of a new statement at the **[edit system processes dhcp-service]** hierarchy level. The deprecated statements may be removed from a future release; we recommend that you transition to the new statement.

To trace DHCP local server operations, include the **traceoptions** statement at the **[edit system processes dhcp-service]** hierarchy level:

```
traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
        <world-readable | no-world-readable>;
    flag flag;
    level  (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
```

The following topics describe the tracing operation configuration statements:

1. Configuring the Filename of the Extended DHCP Local Server Processes Log on page 53
2. Configuring the Number and Size of Extended DHCP Local Server Processes Log Files on page 54
3. Configuring Access to the Log File on page 54
4. Configuring a Regular Expression for Lines to Be Logged on page 54
5. Configuring Trace Option Flags on page 54

Configuring the Filename of the Extended DHCP Local Server Processes Log

By default, the name of the file that records trace output is **jdhcpd**. You can specify a different name by including the **file** statement at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-servicetraceoptions]
file filename;
```

Configuring the Number and Size of Extended DHCP Local Server Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed **jdhcpd.0**, then **jdhcpd.1**, and so on, until there are three trace files. Then the oldest trace file (**jdhcpd.2**) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracking operation (**jdhcpd**) reaches 2 MB, **jdhcpd** is renamed **jdhcpd.0**, and a new file called **jdhcpd** is created. When the new **jdhcpd** reaches 2 MB, **jdhcpd.0** is renamed **jdhcpd.1** and ***filename*** is renamed **jdhcpd.0**. This process repeats until there are 20 trace files. Then the oldest file (**jdhcpd.19**) is overwritten by the newest file (**jdhcpd.0**).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename world-readable;
```

To set the default behavior explicitly, include the **file no-world-readable** statement at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename no-world readable;
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operations output includes all lines relevant to the logged events.

You can refine the output by including the **match** statement at the **[edit system processes dhcp-service traceoptions]** hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system processes dhcp-service traceoptions]
file filename match regex;
```

Configuring Trace Option Flags

By default, only important events are logged. You can configure the trace operations to be logged by including extended DHCP local server tracing flags at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]
flag flag;
```

You can configure the following tracing flags:

- **all**—Trace all operations.
- **auth**—Trace authentication operations.
- **database**—Trace database events.
- **fwd**—Trace firewall process events.
- **general**—Trace miscellaneous events.
- **ha**—Trace high availability-related events.
- **interface**—Trace interface operations.
- **io**—Trace I/O operations.
- **packet**—Trace packet decoding operations.
- **performance**—Trace performance measurement operations.
- **profile**—Trace profile operations.
- **rpd**—Trace routing protocol process events.
- **rtsock**—Trace routing socket operations.
- **session-db**—Trace session database operations.
- **state**—Trace changes in state.
- **statistics**—Trace baseline statistics.
- **ui**—Trace user interface operations.

Configuring DTCP-over-SSH Service for the Flow-Tap Application

The active monitoring flow-tap application requires Dynamic Tasking Control Protocol, by configuring the flow-tap DTCP-over-SSH service. Flow-tap enables you to intercept IPv4 packets transiting an active monitoring router and send a copy of matching packets to one or more content destinations, for use in flexible trend analysis of security threats and in lawful intercept of data.

NOTE: **The flow-tap feature is not supported on outbound, or egress, traffic. Only inbound, or ingress, traffic is supported.**

To enable the flow-tap DTCP-over-SSH service, include the following statements at the **[edit system services]** hierarchy level:

```
flow-tap-dtcp {
  ssh {
    connection-limit limit;
    rate-limit limit;
```

```
    }
}
```

By default, the router supports a limited number of simultaneous flow-tap DTCP-over-SSH sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit *limit***—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 clear-text service sessions and 10 IPv4 clear-text service sessions.
- **rate-limit *limit***—Maximum number of connection attempts accepted per minute per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 session connection attempts per minute and 10 IPv4 session connection attempts per minute.

You must also define user permissions that enable flow-tap users to configure flow-tap services. Specify a login class and access privileges for flow-tap users at the **[edit system login class *class-name* permissions]** hierarchy level:

```
[edit system login class class-name permissions]
(flow-tap | flow-tap-control | flow-tap-operation);
```

The permission bit for a flow-tap login class can be one of the following:

- **flow-tap**—Can view the flow-tap configuration in configuration mode.
- **flow-tap-control**—Can view the flow-tap configuration in configuration mode and configure flow-tap configuration information at the **[edit services flow-tap]** hierarchy level.
- **flow-tap-operation**—Can make flow-tap requests to the router from a remote location using a DTCP client.

NOTE: Only users with a configured access privilege of **flow-tap-operation** can initiate flow-tap requests.

You can also specify user permissions through the Juniper-User-Permissions RADIUS attribute.

To enable the flow-tap DTCP-over-SSH service, you must also include statements at the **[edit interfaces]** hierarchy level to specify an Adaptive Services PIC that runs the flow-tap service and conveys flow-tap filters from the mediation device to the router. In addition, you must include the **flow-tap** statement at the **[edit services]** hierarchy level.

CHAPTER 5

Configuration Statements

System Management Configuration Statements

This topic lists all the configuration statements that you can include at the **[edit system]** hierarchy level to configure system management features:

```
system {
  accounting {
    destination {
      radius {
        server {
          server-address {
            accounting-port port-number;
            retry number;
            secret password;
            source-address address;
            timeout seconds;
          }
        }
      }
      tacplus {
        server {
          server-address {
            port port-number;
            secret password;
            single-connection;
            timeout seconds;
          }
        }
      }
    }
    enhanced-avs-max;
    events [ login change-log interactive-commands ];
  }
  archival {
    configuration {
      archive-sites {
        ftp://<username>:<password>@<host>:<port>/<url-path>;
        ftp://<username>:<password>@<host>:<port>/<url-path>;
      }
      transfer-interval interval;
      transfer-on-commit;
    }
  }
```

```
allow-v4mapped-packets;
arp {
   aging-timer minutes;
   gratuitous-arp-delay;
   gratuitous-arp-on-ifup;
   interfaces;
   passive-learning;
   purging;
}
authentication-order [ authentication-methods ];
backup-router address <destination destination-address>;
commit {
   fast-synchronize;
   persist-groups-inheritance ;
   server;
   synchronize
}
synchronize;
(compress-configuration-files | no-compress-configuration-files);
default-address-selection;
dump-device (compact-flash | remove-compact | usb);
diag-port-authentication (encrypted-password "password" | plain-text-password);
dynamic-profile-options {
   versioning;
}
domain-name domain-name;
domain-search [ domain-list ];
host-name hostname;
inet6-backup-router address <destination destination-address>;
internet-options {
   tcp-mss mss-value;
   (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
   icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate;
   icmpv6-rate-limit bucket-size bucket-size packet-rate packet-rate;
   (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
   (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
   ipv6-path-mtu-discovery-timeout;
   no-tcp-rfc1323-paws;
   no-tcp-rfc1323;
   (path-mtu-discovery | no-path-mtu-discovery);
   source-port upper-limit <upper-limit>;
   (source-quench | no-source-quench);
   tcp-drop-synfin-set;
}
location {
   altitude feet;
   building name;
   country-code code;
   floor number;
   hcoord horizontal-coordinate;
   lata service-area;
   latitude degrees;
   longitude degrees;
   npa-nxx number;
   postal-code postal-code;
   rack number;
```



```
    vcoord vertical-coordinate;
}
login {
    announcement text;
    class class-name {
        access-end;
        access-start;
        allow-commands "regular-expression";
        ( allow-configuration | allow-configuration-regexps) "regular expression 1" "regular
            expression 2";
        allowed-days;
        deny-commands "regular-expression";
        ( deny-configuration | deny-configuration-regexps )  "regular expression 1" "regular
            expression 2 ";
        idle-timeout minutes;
        login-script
        login-tip;
        permissions [ permissions ];
    }
    message text;
    password {
        change-type (set-transitions | character-set);
        format (md5 | sha1 | des);
        maximum-length length;
        minimum-changes number;
        minimum-length length;
    }
    retry-options {
        backoff-threshold number;
        backoff-factor seconds;
        minimum-time seconds;
        tries-before-disconnect number;
    }
    user username {
        full-name complete-name;
        uid uid-value;
        class class-name;
        authentication {
            (encrypted-password "password" | plain-text-password);
            ssh-rsa "public-key";
            ssh-dsa "public-key";
        }
    }
}
login-tip number;
mirror-flash-on-disk;
name-server {
    address;
}
no-multicast-echo;
no-redirects;
no-ping-record-route;
no-ping-time-stamp;
ntp {
    authentication-key key-number type type value password;
    boot-server address;
```

```
    broadcast <address> <key key-number> <version value> <ttl value>;
    broadcast-client;
    multicast-client <address>;
    peer address <key key-number> <version value> <prefer>;
    source-address source-address;
    server address <key key-number> <version value> <prefer>;
    trusted-key [ key-numbers ];
}
ports {
    auxiliary {
        type terminal-type;
    }
    pic-console-authentication {
        encrypted-password encrypted-password;
        plain-text-password;
        console {
            insecure;
            log-out-on-disconnect;
            type terminal-type;
            disable;
        }
    }
    processes {
        process--name (enable | disable) failover (alternate-media | other-routing-engine);
        timeout seconds;
    }
}
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry number;
    secret password;
    source-address source-address;
    timeout seconds;
}
radius-options {
    attributes {
        nas-ip-address ip-address;
    }
    enhanced-accounting;
    password-protocol mschap-v2;
}
root-authentication {
    (encrypted-password “password” | plain-text-password);
    ssh-rsa “public-key”;
    ssh-dsa “public-key”;
}
(saved-core-context | no-saved-core-context);
saved-core-files saved-core-files;
scripts {
    commit {
        allow-transients;
        file filename {
            optional;
            refresh;
            refresh-from url;
```

```
            source url;
        }
        traceoptions {
            file <filename> <files number> <size size> <world-readable | no-world-readable>;
            flag flag;
            no-remote-trace;
        }
        op {
            file filename {
                arguments {
                    argument-name {
                        description descriptive-text;
                    }
                }
                command filename-alias;
                description descriptive-text;
                refresh;
                refresh-from url;
                source url;
            }
            refresh;
            refresh-from url;
            traceoptions {
                file <filename> <files number> <size size> <world-readable | no-world-readable>;
                flag flag;
                no-remote-trace;
            }
        }
    }
    services {
        finger {
            connection-limit limit;
            rate-limit limit;
        }
        flow-tap-dtcp {
            ssh {
                connection-limit limit;
                rate-limit limit;
            }
        }
        ftp {
            connection-limit limit;
            rate-limit limit;
        }
        service-deployment {
            servers server-address {
                port port-number;
            }
            source-address source-address;
        }
        ssh {
            root-login (allow | deny | deny-password);
            protocol-version [v1 v2];
            connection-limit limit;
            rate-limit limit;
        }
```

```
    telnet {
      connection-limit limit;
      rate-limit limit;
    }
    web-management {
      http {
        interfaces [ interface-names ];
        port port;
      }
      https {
        interfaces [ interface-names ];
        local-certificate name;
        port port;
      }
      session {
        idle-timeout [ minutes ];
        session-limit [ session-limit ];
      }
    }
    xnm-clear-text {
      connection-limit limit;
      rate-limit limit;
    }
    xnm-ssl {
      connection-limit limit;
      local-certificate name;
      rate-limit limit;
    }
  }
  static-host-mapping {
    hostname {
      alias [ alias ];
      inet [ address ];
      sysid system-identifier;
    }
  }
  syslog {
    archive <files number> <size size> <world-readable | no-world-readable>;
    console {
      facility severity;
    }
    file filename {
      facility severity;
      archive <archive-sites {ftp-url <password password>}> <files number> <size size>
        <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
        no-world-readable>;
      explicit-priority;
      match "regular-expression";
      structured-data {
        brief;
      }
    }
    host (hostname | other-routing-engine | scc-master) {
      facility severity;
      explicit-priority;
      facility-override facility;
```

```
            log-prefix string;
            match "regular-expression";
            source-address source-address;
            structured-data {
              brief;
            }
          }
          source-address source-address;
          time-format (year | millisecond | year millisecond);
          user (username | *) {
            facility severity;
            match "regular-expression";
          }
        }
        tacplus-options {
          enhanced-accounting;
          service-name service-name;
          (no-cmd-attribute-value | exclude-cmd-attribute);
        }
        tacplus-server server-address {
          secret password;
          single-connection;
          source-address source-address;
          timeout seconds;
        }
        time-zone (GMThour-offset | time-zone);
        }
        tracing {
          destination-override {
          syslog host;
          }
        }
        use-imported-time-zones;
      }
```

authentication (DHCP Local Server)

Syntax

```
authentication {
  password password-string;
  username-include {
    circuit-type;
    client-id;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-name ;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    relay-agent-interface-id;
    relay-agent-remote-id;
    relay-agent-subscriber-id;
    routing-instance-name;
    user-prefix user-prefix-string;
  }
}
```

Hierarchy Level

[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group *group-name*],
[edit system services dhcp-local-server group *group-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server ...],
[edit logical-systems *logical-system-name* system services dhcp-local-server ...],
[edit routing-instances *routing-instance-name* system services dhcp-local-server ...]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay or DHCP local server configuration.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Using External AAA Authentication Services with DHCP*

boot-file

Syntax boot-file *filename*;

Hierarchy Level [edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches only. Set the boot file advertised to DHCP clients. After the client receives an IP address and the boot file location from the DHCP server, the client uses the boot image stored in the boot file to complete DHCP setup.

Options ***filename***—The location of the boot file on the boot server. The filename can include a pathname.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30
- boot-server on page 68

boot-server (DHCP)

Syntax boot-server (*address* | *hostname*);

Hierarchy Level [edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches only. Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup.

Options

- ***address***—IP address of a DHCP boot server.
- ***hostname***—Hostname of a DHCP boot server.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30
- boot-file on page 67

ciphers

Syntax ciphers [*cipher-1 cipher-2 cipher-3* ...]

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 11.2.

Description Specify the set of ciphers the SSH server can use to perform encryption and decryption functions.

Options

- **3des-cbc**—Triple Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode.
- **aes128-cbc**—128-bit Advanced Encryption Standard (AES) in CBC mode.
- **aes256-cbc**—256-bit AES in CBC mode.
- **aes128-ctr**—128-bit AES in CBC mode.
- **aes192-ctr**—192-bit AES in counter mode.
- **aes256-ctr**—256-bit AES in counter mode.
- **aes128-gcm@openssh.com**—128-bit AES in Galois/Counter Mode.
- **aes256-gcm@openssh.com**—256-bit AES in Galois/Counter Mode.
- **arcfour128**—128-bit RC4-stream cipher in CBC mode.
- **arcfour256**—256-bit RC4-stream cipher in CBC mode.
- **blowfish128-cbc**—128-bit blowfish-symmetric block cipher in CBC mode.
- **cast128-cbc**—128-bit cast in CBC mode.

NOTE: Ciphers represent a set. To configure SSH ciphers:

user@host**#set system services ssh ciphers [aes256-cbc aes192-cbc]**

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 18
- *Junos OS Security Configuration Guide*

circuit-type

Syntax circuit-type;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authenticationusername-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify that the circuit type is concatenated with the username during the subscriber authentication process.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Using External AAA Authentication Services to Authenticate DHCP Clients on page 48

client-alive-count-max

Syntax client-alive-count-max*number*;

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 11.2.

Description Configure the number of client alive messages that can be sent without sshd receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. Client alive messages are sent through the encrypted channel. Use in conjunction with client-alive-interval to disconnect unresponsive SSH clients.

Default 3 messages

Options **Range:** 1 through 255

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring SSH Service for Remote Access to the Router or Switch on page 18

client-alive-interval

Syntax client-alive-interval *seconds*;

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 12.1.

Description Configure a timeout interval in seconds, after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. This option applies to SSH protocol version 2 only. Use in conjunction with client-alive-count-max to disconnect unresponsive SSH clients.

Default 0 seconds

Options **Range:** 1 through 65535

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring SSH Service for Remote Access to the Router or Switch on page 18

client-identifier

Syntax client-identifier (ascii *client-id* | hexadecimal *client-id*);

Hierarchy Level [edit system services dhcp],
[edit system services dhcp]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches only. Configure the client's unique identifier. This identifier is used by the DHCP server to index its database of address bindings. Either a client identifier or the client's MAC address is required to uniquely identify the client on the network.

Options ***client-id***—A name or number that uniquely identifies the client on the network. The client identifier can be an ASCII string or hexadecimal digits.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30
- *Configuring a DHCP Server on Switches (CLI Procedure)*

connection-limit

Syntax connection-limit *limit*;

Hierarchy Level [edit system services finger],
[edit system services ftp],
[edit system services netconf ssh],
[edit system services ssh],
[edit system services telnet],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the maximum number of connections sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).

Options ***limit***—(Optional) Maximum number of established connections per protocol (either IPv6 or IPv4).

Range: 1 through 250

Default: 75

NOTE: The actual number of maximum connections depends on the availability of system resources, and might be fewer than the configured connection-limit value if the system resources are limited.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 26
- Configuring DTCP-over-SSH Service for the Flow-Tap Application on page 55
- Configuring Finger Service for Remote Access to the Router on page 17
- Configuring FTP Service for Remote Access to the Router or Switch on page 18
- Configuring SSH Service for Remote Access to the Router or Switch on page 18
- Configuring Telnet Service for Remote Access to a Router or Switch on page 25

default-lease-time

Syntax default-lease-time *seconds*;

Hierarchy Level [edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches only. Specify the length of time in seconds that a client holds the lease for an IP address assigned by a DHCP server. This setting is used if a lease time is not requested by the client.

Options ***seconds***—Number of seconds the lease can be held.

Default: 86400 (1day)

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30
- maximum-lease-time on page 103

delimiter (DHCP Local Server)

Syntax delimiter *delimiter-character*;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Specify the character used as the delimiter between the concatenated components of the username.

Options *delimiter-character*—Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Using External AAA Authentication Services with DHCP*

dhcp

Syntax

```
dhcp {
  boot-file filename;
  boot-server (address | hostname);
  default-lease-time seconds;
  domain-name domain-name;
  domain-search [domain-list];
  maximum-lease-time seconds;
  name-server {
    address;
  }
  next-servernext-server
  option option-identifier-code ;
  pool address/prefix-length {
    address-range {
      low address;
      high address;
    }
    exclude-address {
      address;
    }
  }
  router {
    address;
  }
  static-binding mac-address {
    fixed-address {
      address;
    }
    host-name hostname;
    client-identifier (ascii client-id | hexadecimal client-id);
  }
  wins-server {
    address;
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.

Description For J Series Services Routers only. Configure a router, switch, or interface as a DHCP server. A DHCP server can allocate network addresses and deliver configuration information to client hosts on a TCP/IP network.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30

- System Management Configuration Statements on page 59

dhcpv6 (DHCP Local Server)

Syntax

```
dhcpv6 {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  group group-name {
    authentication {
    ...
    interface interface-name {
      exclude;
      liveness-detection {
        failure-action (clear-binding | clear-binding-if-interface-up | log-only);
        method {
          bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
              minimum-interval milliseconds;
              threshold milliseconds;
            }
            detection-time {
              threshold milliseconds;
            }
            session-mode(automatic | multihop | singlehop);
            holddown-interval milliseconds;
          }
        }
      }
      overrides {
        interface-client-limit number;
        multi-address-embedded-option-response;
        process-inform {
          pool pool-name;
        }
        rapid-commit;
      }
      service-profile dynamic-profile-name;
      trace;
```

```
        upto upto-interface-name;
    }
    overrides {
        delegated-pool;
        interface-client-limit number;
        multi-address-embedded-option-response;
        process-inform {
            pool pool-name;
        }
        rapid-commit;
    }
    route-suppression;
    service-profile dynamic-profile-name;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode(automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
    }
}
overrides {
    delegated-pool;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
    reconfigure {
        attempts attempt-count;
        clear-on-abort;
        strict;
        timeout timeout-value;
        token token-value;
        trigger {
            radius-disconnect;
        }
    }
}
reconfigure {
    attempts attempt-count;
```

```
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
      radius-disconnect;
    }
  }
  requested-ip-network-match subnet-mask;
  route-suppression;
  service-profile dynamic-profile-name;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
[edit logical-systems *logical-system-name* system services dhcp-local-server],
[edit routing-instances *routing-instance-name* system services dhcp-local-server],
[edit system services dhcp-local-server]

Release Information

Statement introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Configure DHCPv6 local server options on the router or switch and enable the router or switch to function as a server for the DHCP protocol for IP version 6 (IPv6). The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. The local server works together with the AAA service framework to control subscriber access (or DHCP client access) and accounting.

The DHCPv6 local server is fully compatible with the extended DHCP local server and DHCP relay agent.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *DHCPv6 Local Server Overview*

dhcp-local-server

Syntax

```
dhcp-local-server {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-name ;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  dhcpv6 {
    authentication {
      ...
    }
    group group-name {
      authentication {
        ...
      }
      interface interface-name {
        exclude;
        liveness-detection {
          failure-action (clear-binding | clear-binding-if-interface-up | log-only);
          method {
            bfd {
              version (0 | 1 | automatic);
              minimum-interval milliseconds;
              minimum-receive-interval milliseconds;
              multiplier number;
              no-adaptation;
              transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
              }
              detection-time {
                threshold milliseconds;
              }
              session-mode(automatic | multihop | singlehop);
              holddown-interval milliseconds;
            }
          }
        }
        overrides {
          interface-client-limit number;
          multi-address-embedded-option-response;
          process-inform {
            pool pool-name;
```

```
        }
        rapid-commit;
      }
      service-profile dynamic-profile-name;
      trace;
      upto upto-interface-name;
    }
    overrides {
      delegated-pool;
      interface-client-limit number;
      multi-address-embedded-option-response;
      process-inform {
        pool pool-name;
      }
      rapid-commit;
    }
    route-suppression;
    service-profile dynamic-profile-name;
  }
  liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        detection-time {
          threshold milliseconds;
        }
        session-mode(automatic | multihop | singlehop);
        holddown-interval milliseconds;
      }
    }
  }
  overrides {
    delegated-pool;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
      pool pool-name;
    }
    rapid-commit;
  }
  reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
```

```
        radius-disconnect;
      }
    }
    route-suppression;
    service-profile dynamic-profile-name;
}
duplicate-clients-in-subnet (incoming-interface | option-82);
dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
  primary-profile-name>;
forward-snooped-clients (all-interfaces | configured-interfaces |
  non-configured-interfaces);
group group-name {
  authentication {
    ...
  }
  dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
  interface interface-name {
    exclude;
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
        bfd {
          version (0 | 1 | automatic);
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          detection-time {
            threshold milliseconds;
          }
          session-mode (automatic | multihop | singlehop);
          holddown-interval milliseconds;
        }
      }
    }
    overrides {
      client-discover-match (option60-and-option82 | incoming-interface);
      interface-client-limit number;
      process-inform {
        pool pool-name;
      }
    }
    service-profile dynamic-profile-name;
    trace;
    upto upto-interface-name;
  }
  overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    interface-client-limit number;
    process-inform {
      pool pool-name;
```

```
        }
      }
      requested-ip-network-match subnet-mask
      route-suppression;
      service-profile dynamic-profile-name;
    }
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
        bfd {
          version (0 | 1 | automatic);
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          detection-time {
            threshold milliseconds;
          }
          session-mode(automatic | multihop | singlehop);
          holddown-interval milliseconds;
        }
      }
    }
    overrides {
      client-discover-match (option60-and-option82 | incoming-interface);
      interface-client-limit number;
      process-inform {
        pool pool-name;
      }
    }
    pool-match-order {
      external-authority;
      ip-address-first;
      option-82;
    }
    reconfigure {
      attempts attempt-count;
      clear-on-abort;
      strict;
      timeout timeout-value;
      token token-value;
      trigger {
        radius-disconnect;
      }
    }
    requested-ip-network-match subnet-mask;
    route-suppression;
    service-profile dynamic-profile-name;
  }
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services],
[edit logical-systems *logical-system-name* system services],
[edit routing-instances *routing-instance-name* system services],
[edit system services]

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Configure Dynamic Host Configuration Protocol (DHCP) local server options on the router or switch and enable the router or switch to function as an extended DHCP local server. The DHCP local server receives DHCP request and reply packets from DHCP clients and then responds with an IP address and other optional configuration information to the client.

The extended DHCP local server is incompatible with the DHCP server on J Series routers and so is not supported on J Series routers. Also, the DHCP local server and the DHCP/BOOTP relay server, which are configured under the **[edit forwarding-options helpers]** hierarchy level, cannot both be enabled on the router or switch at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

The **dhcpv6** stanza configures the router or switch to support Dynamic Host Configuration Protocol for IPv6 (DHCPv6). The DHCPv6 local server is fully compatible with the extended DHCP local server and the extended DHCP relay feature.

NOTE: When you configure the dhcp-local-server statement at the routing instance hierarchy level, you must use a routing instance type of virtual-router.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Extended DHCP Local Server Overview*
- *DHCPv6 Local Server Overview*
- *Configuring a DHCP Server on Switches (CLI Procedure)*

domain-name (DHCP)

Syntax domain-name *domain-name*;

Hierarchy Level
[edit system services dhcp
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches only. Configure the name of the domain in which clients search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified.

Options ***domain-name***—Name of the domain.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30
- *Configuring a DHCP Server on Switches (CLI Procedure)*

domain-name (DHCP Local Server)

Syntax domain-name *domain-name-string*;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Specify the domain name that is concatenated with the username during the subscriber authentication or DHCP client authentication process.

Options ***domain-name-string***—Domain name formatted string.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Using External AAA Authentication Services with DHCP*

finger

Syntax

```
finger {
  connection-limit limit;
  rate-limit limit;
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.

Description Allow finger requests from remote systems to the local router.

The remaining statements are explained separately.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring Finger Service for Remote Access to the Router on page 17

flow-tap-dtcp

Syntax

```
flow-tap-dtcp {
  ssh {
    connection-limit limit;
    rate-limit limit;
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 8.1.

Description Configure Dynamic Tasking Control Protocol (DTCP) sessions to run over SSH in support of the flow-tap application. Note that the flow-tap feature is not supported on outbound, or egress, traffic. Only inbound, or ingress, traffic is supported.

Options

connection-limit *limit*—(Optional) Maximum number of connections allowed.

Range: 1 through 250

Default: 75

rate-limit *limit*—(Optional) Maximum number of connection attempts allowed per minute.

Range: 1 through 250

Default: 150

Required Privilege Level

flow-tap—To view this statement in the configuration.
flow-tap-control—To add this statement to the configuration.

Related Documentation

- Configuring DTCP-over-SSH Service for the Flow-Tap Application on page 55

ftp

Syntax

```
ftp {
  connection-limit limit;
  rate-limit limit;
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Allow FTP requests from remote systems to the local router or switch.

Options The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring FTP Service for Remote Access to the Router or Switch on page 18

group (DHCP Local Server)

Syntax

```
group group-name {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      relay-agent-interface-id
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
  interface interface-name {
    exclude;
    overrides {
      client-discover-match (option60-and-option82 | incoming-interface);
      interface-client-limit number;
      process-inform {
        pool pool-name;
      }
      rapid-commit;
    }
    service-profile dynamic-profile-name;
    trace;
    upto upto-interface-name;
  }
  liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        detection-time {
          threshold milliseconds;
        }
        session-mode(automatic | multihop | singlehop);
```

```
            holddown-interval milliseconds;
          }
        }
      }
      overrides {
        client-discover-match (option60-and-option82 | incoming-interface);
        delegated-pool;
        interface-client-limit number;
        process-inform {
          pool pool-name;
        }
        rapid-commit;
      }
      reconfigure {
        attempts attempt-count;
        clear-on-abort;
        strict;
        timeout timeout-value;
        token token-value;
        trigger {
          radius-disconnect;
        }
      }
      route-suppression;
      service-profile dynamic-profile-name;
    }
```

Hierarchy Level

[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server ...],
[edit logical-systems *logical-system-name* system services dhcp-local-server ...],
[edit routing-instances *routing-instance-name* system services dhcp-local-server ...]

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Configure a group of interfaces that have a common configuration, such as authentication parameters. A group must contain at least one interface.

Options

group-name—Name of the group.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Extended DHCP Local Server Overview*
- *Grouping Interfaces with Common DHCP Configurations*
- *Using External AAA Authentication Services with DHCP*
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- *Configuring a DHCP Server on Switches (CLI Procedure)*

http

Syntax

```
http {
  interfaces [ interface-names ];
  port port;
}
```

Hierarchy Level [edit system services web-management]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the port and interfaces for HTTP service, which is unencrypted.

Options

interfaces [*interface-names*]—Name of one or more interfaces on which to allow the HTTP service. By default, HTTP access is allowed through built-in Fast Ethernet or Gigabit Ethernet interfaces only.

The remaining statement is explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Configuring Management Access for the EX Series Switch (J-Web Procedure)*
- *J-Web Interface User Guide*
- https on page 95
- port on page 116
- web-management on page 144

https

Syntax

```
https {
  interfaces [ interface-names ];
  local-certificate name;
  port port;
}
```

Hierarchy Level [edit system services web-management]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the secure version of HTTP (HTTPS) service, which is encrypted.

Options

interfaces [*interface-names*]—Name of one or more interfaces on which to allow the HTTPS service. By default, HTTPS access is allowed through any ingress interface, but HTTP access is allowed through built-in Fast Ethernet or Gigabit Ethernet interfaces only.

local-certificate *name*—Name of the X.509 certificate for a Secure Sockets Layer (SSL) connection. An SSL connection is configured at the **[edit security certificates local]** hierarchy.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Configuring Management Access for the EX Series Switch (J-Web Procedure)*
- *J-Web Interface User Guide*
- http on page 94
- port on page 116
- web-management on page 144

hostkey-algorithm

Syntax hostkey-algorithm <*algorithm* | *no-algorithm*>

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 11.2.
<*algorithm* | *no algorithm*> statements introduced in Junos OS Release 12.2.

Description Allow or disallow a host-key signature algorithm for the SSH host to use to authenticate another host.

Options

- **no-ssh-dss**—Do not allow generation of a 1024-bit Digital Signature Algorithm (DSA) host key.
- **no-ssh-ecdsa**—Do not allow generation of an Elliptic Curve Digital Signature Algorithm (ECDSA) host key.
- **no-ssh-rsa**—Do not allow generation of a 2048-bit RSA host key.
- **ssh-ecdsa**—Allow generation of an ECDSA host key.
- **ssh-rsa**—Allow generation of a 2048-bit RSA host key.
- **ssh-dss**—Allow generation of a 1024-bit DSA host key.

NOTE: On systems operating in FIPS mode, host keys are regenerated to be of compliant size. However, DSA keys are not supported in FIPS, so the ssh-dss option is not available on systems operating in FIPS mode. RSA keys are also not supported in FIPS, so the ssh-rsa option is also not available. In FIPS mode, by default, ECDSA host keys of 256 bit length are generated.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 18
- *Junos OS Security Configuration Guide*

interface (DHCP Local Server)

Syntax

```
interface interface-name {
  exclude;
  overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    interface-client-limit number;
    rapid-commit;
  }
  service-profile dynamic-profile-name;
  trace;
  upto upto-interface-name;
}
```

Hierarchy Level

[edit system services dhcp-local-server group *group-name*],
[edit system services dhcp-local-server dhcpv6 group *group-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server ...],
[edit logical-systems *logical-system-name* system services dhcp-local-server ...],
[edit routing-instances *routing-instance-name* system services dhcp-local-server ...]

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Options **upto** and **exclude** introduced in Junos OS Release 9.1.

Description

Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the **interface** *interface-name* statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP relay agent.

NOTE: DHCP values are supported in Integrated Routing and Bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently only supports static DHCP configurations. For additional information about how to configure IRB, see *Configuring Integrated Routing and Bridging for Bridge Domains*.

Options

exclude—Exclude an interface or a range of interfaces from the group. This option and the **overrides** option are mutually exclusive.

interface-name—Name of the interface. You can repeat this option multiple times.

upto-interface-name—Upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the ***upto-interface-name*** must be the same as the device name of the ***interface-name***.

The remaining statements are explained separately.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Extended DHCP Local Server Overview*
- *Grouping Interfaces with Common DHCP Configurations*
- *Using External AAA Authentication Services with DHCP*

ip-address-first

Syntax
ip-address-first;

Hierarchy Level
[edit logical-systems *logical-system-name* system services dhcp-local-server pool-match-order],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server pool-match-order],
[edit routing-instances *routing-instance-name* system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]

Release Information
Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Configure the extended DHCP local server to use the IP address method to determine which address-assignment pool to use. The local server uses the IP address in the gateway IP address if one is present in the DHCP client PDU. If no gateway IP address is present, the local server uses the IP address of the receiving interface to find the address-assignment pool. The DHCP local server uses this method by default when no method is explicitly specified.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use*
- *Extended DHCP Local Server Overview*
- *Address-Assignment Pools Overview*
- *Configuring a DHCP Server on Switches (CLI Procedure)*

key-exchange

Syntax key-exchange <*algorithm*>

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Release 11.2 of Junos OS.

Description Specify the set of Diffie-Hellman key exchange methods that the SSH server can use.

Options

- **ecdh-sha2-nistp256**—The ECDH key exchange method with ephemeral keys generated on the nistp256 curve.
- **ecdh-sha2-nistp384**—The ECDH key exchange method with ephemeral keys generated on the nistp384 curve.
- **ecdh-sha2-nistp521**—The ECDH key exchange method with ephemeral keys generated on the nistp521 curve.
- **group-exchange-sha2**—The group exchange algorithm using SHA-2.
- **group-exchange-sha1**—The group exchange algorithm using SHA-1.
- **dh-group14-sha1**—The Diffie-Hellman group14 algorithm using SHA-1.
- **dh-group1-sha1**—The Diffie-Hellman group1 algorithm using SHA-1.

NOTE: The key-exchange represents a set. To configure key-exchange:

user@host#set system services ssh key-exchange

NOTE: The following options are not available on systems operating in FIPS mode: group-exchange-sha1, dh-group14-sha1, and dh-group1-sha1.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 18

local-certificate

Syntax local-certificate;

Hierarchy Level [edit system services service-deployment],
[edit system services web-management https],
[edit system services xnm-ssl]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Import or reference an SSL certificate.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 26
- *Generating SSL Certificates to Be Used for Secure Web Access*
- *Importing SSL Certificates for Junos XML Protocol Support*

logical-system-name (DHCP Local Server)

Syntax logical-system-name;

Hierarchy Level [edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server ...]
[edit logical-systems *logical-system-name* system services dhcp-local-server ...],
[edit routing-instances *routing-instance-name* system services dhcp-local-server ...]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Specify that the logical system name be concatenated with the username during the subscriber authentication or DHCP client process. No logical system name is concatenated if the configuration is in the default logical system.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Using External AAA Authentication Services with DHCP*

mac-address (DHCP Local Server)

Syntax mac-address;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Using External AAA Authentication Services with DHCP*

macs

Syntax macs [*algorithm-1 algorithm-2* ...]

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Junos OS Release 11.2.
SHA-2 options introduced in Junos OS Release 12.1.

Description Specify the set of message authentication code (MAC) algorithms that the SSH server can use to authenticate messages.

Options

- **hmac-md5**—Hash-based MAC using Message-Digest 5 (MD5).
- **hmac-md5-96**—96-bits of Hash-based MAC using MD5.
- **hmac-md5-96-etm@openssh.com**—96-bits of Hash-based Encrypt-then-MAC using MD5.
- **hmac-md5-etm@openssh.com**—Hash-based Encrypt-then-MAC using MD5.
- **hmac-ripemd160**—Hash-based MAC using RIPEMD.
- **hmac-ripemd160-etm@openssh.com**—Hash-based Encrypt-then-MAC using RIPEMD.
- **hmac-sha1**—Hash-based MAC using Secure Hash Algorithm (SHA-1).
- **hmac-sha1-96**—96-bits of Hash-based MAC using SHA-1.
- **hmac-sha1-96-etm@openssh.com**—96-bits of Hash-based Encrypt-then-MAC using SHA-1.
- **hmac-sha1-etm@openssh.com**—Hash-based Encrypt-then-MAC using SHA-1.
- **hmac-sha2-256**—256-bits of Hash-based MAC using Secure Hash Algorithm (SHA-2).
- **hmac-sha2-256-etm@openssh.com**—256-bits of Hash-based Encrypt-then-Mac using SHA-2.
- **hmac-sha2-512**—512-bits of Hash-based MAC using SHA-2.
- **hmac-sha2-512-etm@openssh.com**—512-bits of Hash-based Encrypt-then-Mac using SHA-2.
- **umac-64@openssh.com**—Message Authentication Code using Universal Hashing specified in RFC4418.
- **umac-64-etm@openssh.com**—Encrypt-then-MAC using UMAC-64 algorithm specified in RFC4418.
- **umac-128@openssh.com**—UMAC-128 algorithm specified in RFC4418.
- **umac-128-etm@openssh.com**—Encrypt-then-MAC using UMAC-128 algorithm specified in RFC4418.

NOTE: The macs configuration statement represents a set. To configure SSH MAC algorithms:

```
user@host#set system services ssh macs [hmac-md5 hmac-sha1]
```

NOTE: The following options are not available on systems operating in FIPS mode: hmac-md5, hmac-md5-96, hmac-md5-96-etm@openssh.com, hmac-md5-etm@openssh.com, hmac-ripemd160, hmac-ripemd160-etm@openssh.com, umac-64@openssh.com, umac-64-etm@openssh.com, umac-128@openssh.com, and umac-128-etm@openssh.com.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring SSH Service for Remote Access to the Router or Switch on page 18
- *Junos OS Security Configuration Guide*

maximum-lease-time (DHCP)

Syntax
maximum-lease-time *seconds*;

Hierarchy Level
[edit system services dhcp],

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
For J Series Services Routers and EX Series switches only. Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.

An exception is that the dynamic BOOTP lease length can exceed the maximum lease length specified.

Options
seconds—The maximum number of seconds the lease can be held.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration

Related Documentation
- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30
- default-lease-time on page 74

max-sessions-per-connection

Syntax max-sessions-per-connection *number*

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Release 11.4 of Junos OS.

Description Specify the maximum number of ssh sessions allowed per single SSH connection.

Options **Default:** 10

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring SSH Service for Remote Access to the Router or Switch on page 18
- ssh on page 129
- *Junos OS Security Configuration Guide*

next-server

Syntax next-server *next-server*;

Hierarchy Level [edit system services dhcp],
[edit system services dhcp pool *pool-id*],
[edit system services dhcp static-binding *mac-address*]

Release Information Statement introduced in Junos OS Release 8.4.

Description (J Series Services Routers only) Specify the IP address for the next DHCP server used for communication after a DHCP boot client establishes initial contact.

Options ***next-server***—The IP address of the DHCP server that is used as the “siaddr” in a DHCP protocol packet.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring the Next DHCP Server to Contact After a Boot Client Establishes Initial Communication on page 35
- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30

no-passwords

Syntax no-passwords;

Hierarchy Level [edit system services ssh]

Description Disable ssh password based authentication.

NOTE: Enabling this option under **[edit system services ssh]** applies to **SSH** login service and **NETCONF** running over ssh services.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring SSH Service for Remote Access to the Router or Switch on page 18

no-tcp-forwarding

Syntax no-tcp-forwarding

Hierarchy Level [edit system services ssh]

Release Information Statement introduced in Release 11.4 of Junos OS.

Description Use this configuration option to prevent a user from creating an SSH tunnel over a CLI session to a Junos router via SSH. This type of tunnel could be used to forward TCP traffic, bypassing any firewall filters or ACLs, allowing access to resources beyond the router.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring SSH Service for Remote Access to the Router or Switch on page 18
- ssh on page 129
- *Junos OS Security Configuration Guide*

option (DHCP server)

Syntax

```
option {
   [ (id-number option-type option-value) | (id-number array option-type option-value) ];
}
```

Hierarchy Level

[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information

Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure one or more user-defined options that are not included in the Junos default implementation of the DHCP server. For example, if a client requests a DHCP option that is not included in the DHCP server, you can create a user-defined option that enables the server to respond to the client's request.

Options

- ***id-number***—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.
- ***option-type***—Any of the following types: **byte**, **byte-stream**, **flag**, **integer**, **ip-address**, **short**, **string**, **unsigned-integer**, **unsigned-short**.
- **array**—An option can include an array of values.
- ***option-value***—Value associated with an option. The option value must be compatible with the option type (for example, an **On** or **Off** value for a **flag** type).

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server on page 37
- *Configuring a DHCP Server on Switches (CLI Procedure)*

option-60 (DHCP Local Server)

Syntax option-60;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Specify that the payload of Option 60 (Vendor Class Identifier) from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Using External AAA Authentication Services with DHCP*

option-82 (DHCP Local Server Authentication)

Syntax option-82 <circuit-id> <remote-id>;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Specify the type of Option 82 information from the client PDU that is concatenated with the username during the subscriber authentication or DHCP client authentication process. You can specify either, both, or neither of the Agent Circuit ID and Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If you specify that neither suboption is supplied, the raw payload of Option 82 from the PDU is concatenated to the username.

Options **circuit-id**—(Optional) Agent Circuit ID suboption (suboption 1).

remote-id—(Optional) Agent Remote ID suboption (suboption 2).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Using External AAA Authentication Services with DHCP*

option-82 (DHCP Local Server Pool Matching)

Syntax option-82;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server pool-match-order],
[edit logical-systems *logical-system-name* system services dhcp-local-server pool-match-order],
[edit routing-instances *routing-instance-name* system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]

Release Information Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Configure the extended DHCP local server to use the option 82 value in the DHCP client DHCP PDU together with the ip-address-first method to determine which address-assignment pool to use. You must configure the **ip-address-first** statement before configuring the **option-82** statement. The DHCP local server first determines which address-assignment pool to use based on the ip-address-first method. Then, the local server matches the option 82 value in the client PDU with the option 82 configuration in the address-assignment pool. This statement is supported for IPv4 address-assignment pools only.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use*
- *Extended DHCP Local Server Overview*
- *Address-Assignment Pools Overview*

outbound-ssh

Syntax

```
[edit system services]
outbound-ssh {
  client client-id {
    address {
      port port-number;
      retry number;
      timeout seconds;
    }
    device-id device-id;
    keep-alive {
      retry number;
      timeout seconds;
    }
    reconnect-strategy (in-order | sticky);
    secret password;
    services netconf;
  }
  traceoptions {
    file filename <files number> <match regex> <size size> <world-readable |
      no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure a router or switch running the Junos OS behind a firewall to communicate with client management applications on the other side of the firewall.

Default To configure transmission of the router's or switch's device ID to the application, include the **device-id** statement at the **[edit system services]** hierarchy level.

Options

client-id—Identifies the **outbound-ssh** configuration stanza on the router or switch. Each **outbound-ssh** stanza represents a single outbound SSH connection. This attribute is not sent to the client.

device-id—Identifies the router or switch to the client during the initiation sequence.

keep-alive—(Optional) When configured, specifies that the router or switch send keepalive messages to the management server. To configure the keepalive message, you must set both the **timeout** and **retry** attributes.

reconnect-strategy—(Optional) Specify the method the router or switch uses to reestablish a disconnected outbound SSH connection. Two methods are available:

- **in-order**—Specify that the router or switch first attempt to establish an outbound SSH session based on the management server address list. The router or switch attempts to establish a session with the first server on the list. If this connection is not available, the router or switch attempts to establish a session with the next server, and so on down the list until a connection is established.
- **sticky**—Specify that the router or switch first attempt to reconnect to the management server that it was last connected to. If the connection is unavailable, it attempts to establish a connection with the next client on the list and so forth until a connection is made.

retry—Number of keepalive messages the router or switch sends without receiving a response from the client before the current SSH connection is disconnected. The default is three messages.

secret—(Optional) Router's or switch's public SSH host key. If added to the **outbound-ssh** statement, during the initialization of the outbound SSH service, the router or switch passes its public key to the management server. This is the recommended method of maintaining a current copy of the router's or switch's public key.

timeout—Length of time that the Junos server waits for data before sending a keep alive signal. The default is 15 seconds.

When reconnecting to a client, the router or switch attempts to reconnect to the client based on the **retry** and **timeout** values for each client listed.

address—Hostname or the IPv4 address of the NSM application server. You can list multiple clients by adding each client's IP address or hostname along with the following connection parameters:

- **port**—Outbound SSH port for the client. The default is port 22.
- **retry**—Number of times the router or switch attempts to establish an outbound SSH connection before giving up. The default is three tries.
- **timeout**—Length of time that the router or switch attempts to establish an outbound SSH connection before giving up. The default is fifteen seconds.

filename—(Optional) By default, the filename of the log file used to record the trace options is the name of the traced process (for example, **mib2d** or **snmpd**). Use this option to override the default value.

files—(Optional) Maximum number of trace files generated. By default, the maximum number of trace files is 10. Use this option to override the default value.

When a trace file reaches its maximum size, the system archives the file and starts a new file. The system archives trace files by appending a number to the filename in sequential order from 1 to the maximum value (specified by the default value or the options value set here). Once the maximum value is reached, the numbering sequence is restarted at 1, overwriting the older file.

size—(Optional) Maximum size of the trace file in kilobytes (KB). Once the maximum file size is reached, the system archives the file. The default value is 1000 KB. Use this option to override the default value.

match—(Optional) When used, the system only adds lines to the trace file that match the regular expression specified. For example, if the match value is set to **=error**, the system only records lines to the trace file that include the string **error**.

services—Services available for the session. Currently, NETCONF is the only service available.

world-readable | no-world-readable—(Optional) Whether the files are accessible by the originator of the trace operation only or by any user. By default, log files are only accessible by the user that started the trace operation (**no-world-readable**).

all | configuration | connectivity—(Optional) Type of tracing operation to perform.

all—Log all events.

configuration—Log all events pertaining to the configuration of the router or switch.

connectivity—Log all events pertaining to the establishment of a connection between the client server and the router or switch.

no-remote-trace—(Optional) Disable remote tracing.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Outbound SSH Service on page 21
- System Management Configuration Statements on page 59

password (DHCP Local Server)

Syntax password *password-string*;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 authentication],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* authentication],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication],
[edit system services dhcp-local-server authentication],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group *group-name* authentication],
[edit system services dhcp-local-server group *group-name* authentication]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Configure the password that is sent to the external AAA authentication server for subscriber authentication or DHCP client authentication.

Options ***password-string***—Authentication password.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Using External AAA Authentication Services with DHCP*

pool (System)

Syntax

```
pool address/prefix-length {
  address-range {
    low address;
    high address;
  }
  exclude-address {
    address;
  }
}
```

Hierarchy Level [edit system services dhcp],

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches only. Configure a pool of IP addresses for DHCP clients on a subnet. When a client joins the network, the DHCP server dynamically allocates an IP address from this pool.

Options

address-range—Lowest and highest IP addresses in the pool that are available for dynamic address assignment. If no range is specified, the pool will use all available addresses within the subnet specified. (Broadcast addresses, interface addresses, and excluded addresses are not available.)

exclude-address—Addresses within the range that are not used for dynamic address assignment. You can exclude one or more addresses within the range.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30

pool-match-order

Syntax

```
pool-match-order {
    external-authority;
    ip-address-first;
    option-82;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
[edit logical-systems *logical-system-name* system services dhcp-local-server],
[edit routing-instances *routing-instance-name* system services dhcp-local-server],
[edit system services dhcp-local-server]

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1.

Description

Configure the order in which the DHCP local server uses information in the DHCP client PDU to determine how to obtain an address for the client.

The remaining statements are explained separately.

Default

DHCP local server uses the **ip-address-first** method to determine which address pool to use.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use*
- *Extended DHCP Local Server Overview*
- *Configuring a DHCP Server on Switches (CLI Procedure)*

port (HTTP/HTTPS)

Syntax port *port-number*;

Hierarchy Level [edit system services web-management]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the port on which the HTTP or HTTPS service is connected.

Options ***port-number***—The TCP port number on which the specified service listens.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Configuring Management Access for the EX Series Switch (J-Web Procedure)*
- *J-Web Interface User Guide*
- http on page 94
- https on page 95
- web-management on page 144

port (NETCONF Server)

Syntax port *port-number*;

Hierarchy Level [edit system services netconf]

Release Information Statement introduced in Junos OS Release 10.0.

Description Configure the TCP port used for NETCONF-over-SSH connections.

NOTE:

- The configured port accepts only NETCONF-over-SSH connections. Regular SSH session requests for this port are rejected.
- The default SSH port (22) continues to accept NETCONF sessions even with a configured NETCONF server port. To disable the SSH port from accepting NETCONF sessions, you can specify this in the login event script.
- We do not recommend configuring the default ports for FTP (21) and Telnet (23) services for configuring NETCONF-over-SSH connections.

Options **port *port-number***—Port number on which to enable incoming NETCONF connections over SSH.

Default: 830 (as specified in RFC 4742, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)*)

Range: 1 through 65535

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *NETCONF XML Management Protocol Guide*
- Configuring NETCONF-Over-SSH Connections on a Specified TCP Port on page 25

port (SRC Server)

Syntax port *port-number*;

Hierarchy Level [edit system services service-deployment servers *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the port number on which to contact the SRC server.

Options ***port-number***—(Optional) The TCP port number for the SRC server.
Default: 3333

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS to Work with SRC Software on page 28

protocol-version

Syntax protocol-version *version*;

Hierarchy Level [edit system services ssh]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify the secure shell (SSH) protocol version.

Default **v2**—SSH protocol version 2 is the default, introduced in Junos OS Release 11.4.

Options ***version***—SSH protocol version: **v1**, **v2**, or both.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring the SSH Protocol Version on page 20

rate-limit

Syntax rate-limit *limit*;

Hierarchy Level [edit system services finger],
[edit system services ftp],
[edit system services netconf ssh],
[edit system services ssh],
[edit system services telnet],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the maximum number of connections attempts per protocol (either IPv6 or IPv4) on an access service.

Default 150 connections

Options **rate-limit *limit***—(Optional) Maximum number of connection attempts allowed per minute, per IP protocol (either IPv4 or IPv6).

Range: 1 through 250

Default: 150

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 26

root-login

Syntax root-login (allow | deny | deny-password);

Hierarchy Level [edit system services ssh]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Control user access through SSH.

Default Allow user access through SSH.

Options

allow—Allow users to log in to the router or switch as root through SSH.

deny—Disable users from logging in to the router or switch as root through SSH.

deny-password—Allow users to log in to the router or switch as root through SSH when the authentication method (for example, RSA authentication) does not require a password.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Root Login Through SSH on page 19

router

Syntax

```
router {
  address;
}
```

Hierarchy Level

[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp-service],
[edit system services dhcp-service pool],
[edit system services dhcp-service static-binding]

Release Information

Statement introduced before Junos OS Release 7.4. Statement for EX Series switches introduced in Junos OS Release 9.0.

Description

For J Series Services Routers and EX Series switches only, specify IPv4 addresses for one or more devices available to a DHCP client. List devices (switches or routers) in order of preference.

Options

address—IPv4 address of the router or switch. To configure multiple devices, include multiple **address** options.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30
- *Configuring a DHCP Server on Switches (CLI Procedure)*

routing-instance-name (DHCP Local Server)

Syntax routing-instance-name;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Specify that the routing instance name be concatenated with the username during the subscriber authentication or DHCP client authentication process. No routing instance name is concatenated if the configuration is in the default routing instance.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Using External AAA Authentication Services with DHCP*

server-identifier

Syntax server-identifier *address*;

Hierarchy Level [edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches only. Configure a server identifier. The identifier can be used to identify a DHCP server in a DHCP message. It can also be used as a destination address from clients to servers (for example, when the boot file is set, but not the boot server).

Servers include the server identifier in **DHCPOFFER** messages so that clients can distinguish between multiple lease offers. Clients include the server identifier in **DHCPREQUEST** messages to select a lease and indicate which offer is accepted from multiple lease offers. Also, clients can use the server identifier to send unicast request messages to specific DHCP servers to renew a current lease.

This address must be a manually assigned, static IP address. The server cannot send a request and receive an IP address from itself or another DHCP server.

Default If no server identifier is set, the DHCP server sets the server identifier based on the primary interface address used by the server to receive a client request. For example, if the client sends a DHCP request and the server receives it on **fe-0/0/0** and the primary interface address is **1.1.1.1**, then the server identifier is set to **1.1.1.1**.

Options ***address***—IPv4 address of the server. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30

servers

Syntax

```
servers server-address {
  port port-number;
}
```

Hierarchy Level [edit system services service-deployment]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure an IPv4 address for the Session and Resource Control (SRC) server.

Options *server-address*—The TCP port number.

Default: 3333

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Work with SRC Software on page 28

service-deployment

Syntax

```
service-deployment {
  servers server-address {
    port port-number;
  }
  source-address source-address;
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Enable Junos OS to work with the Session and Resource Control (SRC) software.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Work with SRC Software on page 28

services (System Services)

Syntax

```
services {
  dhcp { \* DHCP not supported on a DCF
    dhcp_services;
  }
  finger {
    connection-limit limit;
    rate-limit limit;
  }
  ftp {
    connection-limit limit;
    rate-limit limit;
  }
  service-deployment {
    servers address {
      port-number port-number;
    }
    source-address address;
  }
  ssh {
    connection-limit limit;
    protocol-version [v1 v2];
    rate-limit limit;
    root-login (allow | deny | deny-password);
  }
  telnet {
    connection-limit limit;
    rate-limit limit;
  }
  web-management {
    http {
      interfaces [ names ];
      port port;
    }
    https {
      interfaces [ names ];
      local-certificate name;
      port port;
    }
    session {
      idle-timeout [ minutes ];
      session-limit [ limit ];
    }
  }
  xnm-clear-text {
    connection-limit limit;
    rate-limit limit;
  }
  xnm-ssl {
    connection-limit limit;
    local-certificate name;
    rate-limit limit;
    ssl-renegotiation;
```

```
  }
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the router or switch so that users on remote systems can access the local router or switch through the DHCP server, finger, rlogin, SSH, telnet, Web management, Junos XML protocol clear-text, Junos XML protocol SSL, and network utilities or enable Junos OS to work with the Session and Resource Control (SRC) software.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 26
- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30
- Configuring the Junos OS to Work with SRC Software on page 28

session (Time-out)

Syntax

```
session {
  idle-timeout minutes;
  session-limit session-limit;
}
```

Hierarchy Level [edit system services web-management]

Release Information Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure limits for the number of minutes a session can be idle before it times out, and configure the number of simultaneous J-Web user login sessions.

Options

idle-timeout *minutes*—Configure the number of minutes a session can be idle before it times out.

Range: 1 through 1440

Default: 1440

session-limit *session-limit*—Configure the maximum number of simultaneous J-Web user login sessions.

Range: 1 through 1024

Default: Unlimited

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *J-Web Interface User Guide*

source-address (SRC Software)

Syntax source-address *source-address*;

Hierarchy Level [edit system services service-deployment]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Enable Junos OS to work with the Session and Resource Control (SRC) software.

Options ***source-address***— Local IPv4 address to be used as source address for traffic to the SRC server. The source address restricts traffic within the out-of-band network.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Work with SRC Software on page 28

ssh

Syntax

```
ssh {
  ciphers [ cipher-1 cipher-2 cipher-3 ...];
  client-alive-count-max seconds;
  client-alive-interval seconds;
  connection-limit limit;
  hostkey-algorithm <algorithm|no-algorithm>;
  key-exchange <algorithm>;
  macs <algorithm>;
  max-sessions-per-connection <number>;
  no-passwords;
  no-tcp-forwarding;
  protocol-version [v1 v2];
  rate-limit limit;
  root-login (allow | deny | deny-password);
}
```

Hierarchy Level [edit system services]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
client-alive-interval and **client-alive-max-count** statements introduced in Junos OS Release 12.2.
no-passwords statement introduced in Junos OS Release 13.3.

Description Allow SSH requests from remote systems to the local router or switch.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 18

ssl-renegotiation

Syntax ssl-renegotiation;

Hierarchy Level [edit system services xnm-ssl]

Release Information Statement introduced in Junos Os Release 13.3.

Description Enable or disable SSL re-negotiation for xnm-ssl service.

Default SSL re-negotiation for xnm-ssl service is disabled by default.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 26

static-binding

Syntax

```
static-binding mac-address {
  client-identifier (ascii client-id | hexadecimal client-id);
  fixed-address {
    address;
  }
  host-name client-hostname;
}
```

Hierarchy Level

[edit system services dhcp],
[edit system services dhcp]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

For J Series Services routers and EX Series switches only. Set static bindings for DHCP clients. A static binding is a mapping between a fixed IP address and the client's MAC address or client identifier.

Options

mac-address—The MAC address of the client. This is a hardware address that uniquely identifies a client on the network.

fixed-address *address*—Fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.

host-name *client-hostname*—Hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the **domain-name** statement.

client-identifier (ascii *client-id* | hexadecimal *client-id*)—Used by the DHCP server to index the database of address bindings. The client identifier is an ASCII string or hexadecimal number and can include a type-value pair as specified in RFC 1700, *Assigned Numbers*. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30
- *Configuring a DHCP Server on Switches (CLI Procedure)*

system

Syntax system { ... }

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure system management properties. Set values in the **edit system** hierarchy of the configuration.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- System Management Configuration Statements on page 59

telnet

Syntax
```
telnet {
  connection-limit limit;
  rate-limit limit;
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Provide Telnet connections from remote systems to the local router or switch.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring Telnet Service for Remote Access to a Router or Switch on page 25

traceoptions (Address-Assignment Pool)

Syntax

```
traceoptions {
  file filename {
    files number;
    size maximum-file-size;
    match regex;
    (world-readable | no-world-readable);
  }
  flag address-assignment;
  flag all;
  flag configuration;
  flag framework;
  flag ldap;
  flag local-authentication;
  flag radius;
}
```

Hierarchy Level [edit system processes general-authentication-service]

Release Information Flag for tracing address-assignment pool operations introduced in Junos OS Release 9.0.
option-name option introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure tracing options.

Options

file *filename*—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **address-assignment**—All address-assignment events
- **all**—All tracing operations
- **configuration**—Configuration events
- **framework**—Authentication framework events
- **ldap**—LDAP authentication events
- **local-authentication**—Local authentication events

- **radius**—RADIUS authentication events

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

no-world-readable—(Optional) Restrict access to the originator of the trace operation only.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- *Configuring Address-Assignment Pools*

traceoptions (DHCP)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  level  (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

Hierarchy Level [edit system processes dhcp-service]

Release Information Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Define global tracing operations for extended DHCP local server and extended DHCP relay agent processes.

Replaces deprecated **traceoptions** statements at the **[edit forwarding-options dhcp-relay]** and **[edit system services dhcp-local-server]** hierarchy levels.

Options **file *filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements

- **all**—Trace all events.
- **auth**—Trace authentication events.
- **database**—Trace database events.
- **fwd**—Trace firewall process events.
- **general**—Trace miscellaneous events.
- **ha**—Trace high availability-related events.
- **interface**—Trace interface operations.
- **io**—Trace I/O operations.
- **packet**—Trace packet and option decoding operations.
- **performance**—Trace performance measurement operations.
- **profile**—Trace profile operations.
- **rpd**—Trace routing protocol process events.

- **rtsock**—Trace routing socket operations.
- **session-db**—Trace session database events.
- **state**—Trace changes in state.
- **statistics**—Trace baseline statistics.
- **ui**—Trace user interface operations.

level—Level of tracing to perform; also known as severity level. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

- **all**—Match messages of all levels.
- **error**—Match error messages.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

Default: error

match ***regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access, allowing only the user **root** and users who have the Junos OS **maintenance** permission to access the trace files.

size ***maximum-file-size***—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***size*****k** to specify KB, ***size*****m** to specify MB, or ***size*****g** to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *Tracing Extended DHCP Operations*

traceoptions (DHCP Server)

Syntax

```
traceoptions {
  file filename <files number> <match regex> <size size> <world-readable |
    no-world-readable>;
  flag flag;
}
```

Hierarchy Level [edit system services dhcp]

Release Information Statement for tracing J Series Services Router DHCP processes introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Define tracing operations for DHCP processes for J Series Services Routers and EX Series switches.

Options

file *filename*—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—All tracing operations
- **binding**—Trace binding operations
- **config**—Log reading of configuration
- **conflict**—Trace user-detected conflicts for IP addresses
- **event**—Trace important events
- **ifdb**—Trace interface database operations
- **io**— Trace I/O operations
- **lease**—Trace lease operations
- **main**—Trace main loop operations
- **misc**— Trace miscellaneous operations
- **packet**—Trace DHCP packets

- **options**—Trace DHCP options
- **pool**—Trace address pool operations
- **protocol**—Trace protocol operations
- **rtsock**—Trace routing socket operations
- **scope**—Trace scope operations
- **signal**—Trace DHCP signal operations
- **trace**—All tracing operations
- **ui**—Trace user interface operations

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

- **all**—All tracing operations
- **binding**—Trace binding operations
- **config**— Log reading of configuration
- **conflict**—Trace user-detected conflicts for IP addresses
- **event**—Trace important events
- **ifdb**— Trace interface database operations
- **io**—Trace I/O operations
- **lease**—Trace lease operations
- **main**—Trace main loop operations
- **match *regex***— Refine the output to include lines that contain the regular expression.
- **misc**—Trace miscellaneous operations
- **packet**—Trace DHCP packets
- **options**—Trace DHCP options
- **pool**—Trace address pool operations
- **protocol**—Trace protocol operations
- **rtsock**—Trace routing socket operations
- **scope**—Trace scope operations
- **signal**—Trace DHCP signal operations
- **trace**—All tracing operations
- **ui**—Trace user interface operations

no-world-readable—(Optional) Disable unrestricted file access.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the ***trace-file*** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Tracing Operations for DHCP Processes on page 38
- System Management Configuration Statements on page 59

traceoptions (SBC Configuration Process)

Syntax

```
traceoptions {
  file filename <files number> <match regex> <size size>
    <world-readable | no-world-readable>;
  flag flag;
}
```

Hierarchy Level [edit system processes sbc-configuration-process]

Release Information Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 9.5 for EX Series switches.

Description Configure trace options for the session border controller (SBC) process of the border signaling gateway (BSG).

Options

file *filename*—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory **/var/log**. You can include the following file options:

- **files** *number*—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

  If you specify a maximum number of files, you must also specify a maximum file size with the **size** option and a filename.

  Range: 2 through 1000

  Default: 3 files

- **match** *regex*—(Optional) Refine the output to include lines that contain the regular expression.
- **no-world-readable**—(Optional) Disable unrestricted file access.
- **size** *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the trace-file again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

  Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB.

  Range: 10 KB through 1 GB

  Default: 128 KB

- **world-readable**—(Optional) Enable unrestricted file access.

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all *trace-level***—Trace all SBC process operations.
- **common *trace-level***—Trace common events.
- **configuration *trace-level***—Trace configuration events.
- **device-monitor *trace-level***—Trace device monitor events.
- **ipc *trace-level***—Trace IPC events.
- **memory—pool *trace-level***—Trace memory pool events.
- ***trace-level***—Trace level options are related to the severity of the event being traced. When you choose a trace level, messages at that level and higher levels are captured. Enter one of the following trace levels as the ***trace-level***:
  - **debug**—Log all code flow of control.
  - **error**—Log failures with a short-term effect.
  - **info**—Log summary for normal operations, such as the policy decisions made for a call.
  - **trace**—Log program trace START and EXIT macros.
  - **warning**—Log failure recovery events or failure of an external entity.
- **ui *trace-level***—Trace user interface operations.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- See “Troubleshooting the IMSG” in the *Junos Multiplay Solutions Guide*
- System Management Configuration Statements on page 59

username-include (DHCP Local Server)

Syntax

```
username-include {
  circuit-type;
  client-id;
  delimiter delimiter-character;
  domain-name domain-name-string;
  interface-name ;
  logical-system-name;
  mac-address;
  option-60;
  option-82 <circuit-id> <remote-id>;
  relay-agent-interface-id;
  relay-agent-remote-id;
  relay-agent-subscriber-id;
  routing-instance-name;
  user-prefix user-prefix-string;
}
```

Hierarchy Level

[edit system services dhcp-local-server authentication],
[edit system services dhcp-local-server dhcpv6 authentication],
[edit system services dhcp-local-server dhcpv6 group *group-name* authentication],
[edit system services dhcp-local-server group *group-name* authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server ...],
[edit logical-systems *logical-system-name* system services dhcp-local-server ...],
[edit routing-instances *routing-instance-name* system services dhcp-local-server ...]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the username that the router or switch passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router (or switch) accesses the local authentication service only and does not use external authentication services, such as RADIUS.

The statements are explained separately. The option-60 and option-82 statements are not supported in the DHCPv6 hierarchy levels. The *client-id*, *relay-agent-interface-id*, *relay-agent-remote-id* and *relay-agent-subscriber-id* statements are supported in the DHCPv6 hierarchy levels only.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Using External AAA Authentication Services with DHCP*
- *Creating Unique Usernames for DHCP Clients*

user-prefix (DHCP Local Server)

Syntax user-prefix *user-prefix-string*;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group *group-name* authentication username-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Specify the user prefix that is concatenated with the username during the subscriber authentication or DHCP client authentication process.

Options ***user-prefix-string***—User prefix string.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Using External AAA Authentication Services with DHCP*

web-management

Syntax

```
web-management {
  http {
    interfaces [ interface-names ];
    port port;
  }
  https {
    interfaces [ interface-names ];
    local-certificate name;
    port port;
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure settings for HTTP or HTTPS access. HTTP access allows management of the router or switch using the browser-based J-Web graphical user interface. HTTPS access allows secure management of the router or switch using the J-Web interface. With HTTPS access, communication between the router or switch Web server and your browser is encrypted.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Configuring Management Access for the EX Series Switch (J-Web Procedure)*
- *J-Web Interface User Guide*
- http on page 94
- https on page 95
- port on page 116

wins-server (System)

Syntax

```
wins-server {
  address;
}
```

Hierarchy Level

[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

For J Series Services Routers and EX Series switches only. Specify one or more NetBIOS Name Servers. When a DHCP client is added to the network and assigned an IP address, the NetBIOS Name Server manages the Windows Internet Name Service (WINS) database that matches IP addresses (such as **192.168.1.3**) to Windows NetBIOS names (such as **\\Marketing**). List servers in order of preference.

Options

address—IPv4 address of the NetBIOS Name Server running WINS. To configure multiple servers, include multiple ***address*** options.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 30
- *Configuring a DHCP Server on Switches (CLI Procedure)*

xnm-clear-text

Syntax

```
xnm-clear-text {
  connection-limit limit;
  rate-limit limit;
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.

Description Allow Junos XML protocol clear-text requests from remote systems to the local router.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 26

xnm-ssl

Syntax

```
xnm-ssl {
  connection-limit limit;
  rate-limit limit;
  ssl-renegotiation ;
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.
Support for the **ssl-renegotiation** statement added in Junos OS Release 13.3.

Description Allow Junos XML protocol SSL requests from remote systems to the local router.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 26

PART 3

Administration

CHAPTER 6

Administrative Commands

clear system services dhcp binding

Syntax clear system services dhcp binding
<*address*>

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (J Series routers and EX Series switches only) Remove obsolete IP address bindings on a Dynamic Host Configuration Protocol (DHCP) server and return them to the IP address pool.

Options ***address***—(Optional) Remove a specific IP address binding and return it to the address pool.

Required Privilege Level view and system

Related Documentation
- show system services dhcp binding on page 154

List of Sample Output clear system services dhcp binding on page 150

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear system services dhcp binding

```
user@host> clear system services dhcp binding
```

clear system services dhcp conflict

Syntax clear system services dhcp conflict
<*address*>

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (J Series routers and EX Series switches only) Remove IP addresses from the Dynamic Host Configuration Protocol (DHCP) server conflict list and return them to the IP address pool.

Options ***address***—(Optional) Remove a specific IP address from the conflict list and return it to the address pool.

Required Privilege Level view and system

Related Documentation
- show system services dhcp conflict on page 157

List of Sample Output clear system services dhcp conflict on page 151

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear system services dhcp conflict

```
user@host> clear system services dhcp conflict
```

clear system services dhcp statistics

Syntax clear system services dhcp statistics

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (J Series routers and EX Series switches only) Clear Dynamic Host Configuration Protocol (DHCP) server statistics.

Options This command has no options.

Required Privilege Level view and system

Related Documentation
- show system services dhcp statistics on page 162

List of Sample Output clear system services dhcp statistics on page 152

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear system services dhcp statistics

```
user@host> clear system services dhcp statistics
```

CHAPTER 7

Monitoring Commands

- show system services dhcp binding
- show system services dhcp conflict
- show system services dhcp global
- show system services dhcp pool
- show system services dhcp statistics
- show system services service-deployment

show system services dhcp binding

Syntax
show system services dhcp binding
<detail>
<*address*>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
(J Series routers only) Display Dynamic Host Configuration Protocol (DHCP) server client binding information.

Options
none—Display brief information about all active client bindings.

detail—(Optional) Display detailed information about all active client bindings.

address—(Optional) Display detailed client binding information for the specified IP address only.

Required Privilege Level
view and system

Related Documentation
- clear system services dhcp binding on page 150

List of Sample Output
show system services dhcp binding on page 155
show system services dhcp binding address on page 155
show system services dhcp binding address detail on page 155

Output Fields
Table 6 on page 154 describes the output fields for the **show system services dhcp binding** command. Output fields are listed in the approximate order in which they appear.

Table 6: show system services dhcp binding Output Fields

Field Name	Field Description	Level of Output
Allocated address	List of IP addresses the DHCP server has assigned to clients.	All levels
MAC address	Corresponding media access control (MAC) hardware address of the client.	All levels
Client identifier	(***address*** option only) Client's unique identifier (represented by an ASCII string or hexadecimal digits). This identifier is used by the DHCP server to index its database of address bindings.	All levels
Binding Type	Type of binding assigned to the client. DHCP servers can assign a dynamic binding from a pool of IP addresses or a static binding to one or more specific IP addresses.	All levels
Lease Expires at	Time the lease expires or **never** for leases that do not expire.	All levels
Lease Obtained at	(***address*** option only) Time the client obtained the lease from the DHCP server.	**detail**

Table 6: show system services dhcp binding Output Fields *(continued)*

Field Name	Field Description	Level of Output
State	Status of the binding. Bindings can be active or expired.	**detail**
Pool	Address pool that contains the IP address assigned to the client.	**detail**
Request received on	Interface on which the DHCP message exchange occurs. The IP address pool is configured based on the interface's IP address. If a relay agent is used, its IP address is also displayed.	**detail**
DHCP options	User-defined options created for the DHCP server. If no options have been defined, this field is blank.	**detail**

Sample Output

show system services dhcp binding

```
user@host> show system services dhcp binding

Allocated address   MAC address        Binding Type   Lease expires at
192.168.1.2         00:a0:12:00:12:ab  static         never
192.168.1.3         00:a0:12:00:13:02  dynamic        2004-05-03 13:01:42 PDT
```

show system services dhcp binding address

```
user@host> show system services dhcp binding 192.168.1.3

DHCP binding information:
Allocated address: 192.168.1.3
Mac address: 00:a0:12:00:12:ab
Client identifier
61 63 65 64 2d 30 30 3a 61 30 3a 31 32 3a 30 30aced-00:a0:12:00
3a 31 33 3a 30 32:13:02

Lease information:
    Binding Type dynamic
    Obtained at 2004-05-02 13:01:42 PDT
    Expires at 2004-05-03 13:01:42 PDT
```

show system services dhcp binding address detail

```
user@host> show system services dhcp binding 192.168.1.3 detail
DHCP binding information:
Allocated address        192.168.1.3
MAC address  00:a0:12:00:12:ab
    Pool             192.168.1.0/24
Request received on fe-0/0/0, relayed by 192.168.4.254

Lease information:
    Type             DHCP
    Obtained at      2004-05-02 13:01:42 PDT
    Expires at       2004-05-03 13:01:42 PDT
State active

DHCP options:
    Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
```

```
Name: domain-name, Value: mydomain.tld
Code: 19, Type: flag, Value: off
Code: 40, Type: string, Value: domain.tld
Code: 32, Type: ip-address, Value: 3.3.3.33
```

show system services dhcp conflict

Syntax show system services dhcp conflict

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (J Series routers only and EX Series switches) Display Dynamic Host Configuration Protocol (DHCP) client-detected conflicts for IP addresses. When a conflict is detected, the DHCP server removes the address from the address pool.

Options This command has no options.

Required Privilege Level view and system

Related Documentation
- clear system services dhcp conflict on page 151

List of Sample Output show system services dhcp conflict on page 157

Output Fields Table 7 on page 157 describes the output fields for the **show system services dhcp conflict** command. Output fields are listed in the approximate order in which they appear.

Table 7: show system services dhcp conflict Output Fields

Field Name	Field Description
Detection time	Date and time the client detected the conflict.
Detection method	How the conflict was detected.
Address	IP address where the conflict occurs. The addresses in the conflicts list remain excluded from the pool until you use a **clear system services dhcp conflict** command to manually clear the list.

Sample Output

show system services dhcp conflict

```
user@host> show system services dhcp conflict

Detection time           Detection method  Address
2004-08-03 19:04:00 PDT  ARP               3.3.3.5
2004-08-04 04:23:12 PDT  Ping              4.4.4.8
2004-08-05 21:06:44 PDT  Client            3.3.3.10
```

show system services dhcp global

Syntax show system services dhcp global

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) global configuration options. Global options apply to all scopes and clients served by the DHCP server. Global options are overridden if specified otherwise in scope or client options. Scope options apply to specific subnets or ranges of addresses. Client options apply to specific clients.

Options This command has no options.

Required Privilege Level view and system

List of Sample Output show system services dhcp global on page 159

Output Fields Table 8 on page 158 describes the output fields for the **show system services dhcp global** command. Output fields are listed in the approximate order in which they appear.

Table 8: show system services dhcp global Output Fields

Field Name	Field Description
BOOTP lease length	Length of lease time assigned to BOOTP clients.
Default lease time	Lease time assigned to clients that do not request a specific lease time.
Minimum lease time	Minimum time a client retains an IP address lease on the server.
Maximum lease time	Maximum time a client can retain an IP address lease on the server.
DHCP options	User-defined options created for the DHCP server. If no options have been defined, this field is blank.

Sample Output

show system services dhcp global

```
user@host> show system services dhcp global

Global settings:
    BOOTP lease length         infinite

DHCP lease times:
    Default lease time         1 hour
    Minimum lease time         2 hours
    Maximum lease time         infinite

DHCP options:
    Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
    Name: domain-name, Value: mydomain.tld
    Code: 19, Type: flag, Value: off
    Code: 40, Type: string, Value: domain.tld
    Code: 32, Type: ip-address, Value: 3.3.3.33
```

show system services dhcp pool

Syntax show system services dhcp pool
<detail>
<*subnet-address*>

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server IP address pools.

Options **none**—Display brief information about all IP address pools.

detail—(Optional) Display detailed information.

subnet-address—(Optional) Display information for the specified subnet address.

Required Privilege Level view and system

List of Sample Output
show system services dhcp pool on page 161
show system services dhcp pool subnet-address on page 161
show system services dhcp pool subnet-address detail on page 161

Output Fields Table 9 on page 160 describes the output fields for the **show system services dhcp pool** command. Output fields are listed in the approximate order in which they appear.

Table 9: show system services dhcp pool Output Fields

Field Name	Field Description	Level of Output
Pool name	Subnet on which the IP address pool is defined.	None specified
Low address	Lowest address in the IP address pool.	None specified
High address	Highest address in the IP address pool.	None specified
Excluded addresses	Addresses excluded from the address pool.	None specified
Subnet	(***subnet-address*** option only) Subnet to which the specified address pool belongs.	None specified
Address range	(***subnet-address*** option only) Range of IP addresses in the address pool.	None specified
Addresses assigned	Number of IP addresses in the pool that are assigned to DHCP clients and the total number of IP addresses in the pool.	**detail**
Active	Number of assigned IP addresses in the pool that are active.	**detail**
Excluded	Number of assigned IP addresses in the pool that are excluded.	**detail**
Default lease time	Lease time assigned to clients that do not request a specific lease time.	**detail**

Table 9: show system services dhcp pool Output Fields *(continued)*

Field Name	Field Description	Level of Output
Minimum lease time	Minimum time a client can retain an IP address lease on the server.	**detail**
Maximum lease time	Maximum time a client can retain an IP address lease on the server.	**detail**
DHCP options	User-defined options created for the DHCP server. If no options have been defined, this field is blank.	**detail**

Sample Output

show system services dhcp pool

```
user@host> show system services dhcp pool

Pool name    Low address   High address   Excluded addresses
3.3.3.0/24   3.3.3.2       3.3.3.254      3.3.3.1
```

show system services dhcp pool subnet-address

```
user@host> show system services dhcp pool 3.3.3.0/24

Pool information:
    Subnet                    3.3.3.0/24
    Address range             3.3.3.2 - 3.3.3.254
    Addresses assigned        2/253
```

show system services dhcp pool subnet-address detail

```
user@host> show system services dhcp pool 3.3.3.0/24 detail

Pool information:
    Subnet                    3.3.3.0/24
    Address range             3.3.3.2 - 3.3.3.254
    Addresses assigned        2/253
      Active: 1, Excluded: 1

DHCP lease times:
    Default lease time        1 hour
    Minimum lease time        2 hours
    Maximum lease time        infinite

DHCP options:
    Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
    Name: domain-name, Value: mydomain.tld
    Name: router, Value: { 3.3.3.1 }
    Name: server-identifier, Value: 3.3.3.1
    Code: 19, Type: flag, Value: off
    Code: 40, Type: string, Value: domain.tld
    Code: 32, Type: ip-address, Value: 3.3.3.333.3.3.254 3.3.3.1
```

show system services dhcp statistics

Syntax show system services dhcp statistics

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server statistics.

Options This command has no options.

Required Privilege Level view and system

Related Documentation
- clear system services dhcp statistics on page 152

List of Sample Output show system services dhcp statistics on page 163

Output Fields Table 10 on page 162 describes the output fields for the **show system services dhcp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 10: show system services dhcp statistics Output Fields

Field Name	Field Description
Default lease time	Lease time assigned to clients that do not request a specific lease time.
Minimum lease time	Minimum time a client can retain an IP address lease on the server.
Maximum lease time	Maximum time a client can retain an IP address lease on the server.
Packets dropped	Total number of packets dropped and number of packets dropped because of: • Invalid hardware address • Invalid opcode • Invalid server address • No available address • No interface match • No routing instance match • No valid local addresses • Packet too short • Read error • Send error

Table 10: show system services dhcp statistics Output Fields *(continued)*

Field Name	Field Description
Messages received	Number of the following message types sent from DHCP clients and received by the DHCP server: • BOOTREQUEST • DHCPDECLINE • DHCPDISCOVER • DHCPINFORM • DHCPRELEASE • DHCPREQUEST
Messages sent	Number of the following message types sent from the DHCP server to DHCP clients: • BOOTREPLY • DHCPACK • DHCPOFFER • DHCPNAK

Sample Output

show system services dhcp statistics

```
user@host> show system services dhcp statistics

DHCP lease times:
    Default lease time         1 hour
    Minimum lease time         2 hours
    Maximum lease time         infinite

Packets dropped:
    Total                      0
    Bad hardware address       0
    Bad opcode                 0
    Invalid server address     0
    No available addresses     0
    No interface match         0
    No routing instance match  0
    No valid local address     0
    Packet too short           0
    Read error                 0
    Send error                 0

Messages received:
    BOOTREQUEST                0
    DHCPDECLINE                0
    DHCPDISCOVER               0
    DHCPINFORM                 0
    DHCPRELEASE                0
    DHCPREQUEST                0

Messages sent:
    BOOTREPLY                  0
    DHCPACK                    0
    DHCPOFFER                  0
    DHCPNAK                    0
```

show system services service-deployment

Syntax show system services service-deployment

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Display information about a Session and Resource Control (SRC) client.

Options This command has no options.

Required Privilege Level system
view

List of Sample Output show system services service-deployment on page 165

Output Fields Table 11 on page 165 lists the output fields for the **show system services service-deployment** command. Output fields are listed in the approximate order in which they appear.

Table 11: show system services service-deployment Output Fields

Field Name	Field Description
PDT Keepalive settings	Configured PDT keepalive interval, in seconds.
Keepalives sent	Number of keepalives sent.
Notifications sent	Number of notifications sent.
Last update from peer	Time at which the last update from a peer was received.

Sample Output

show system services service-deployment

```
user@host> show system services service-deployment
Connected to 192.4.4.4 port 10288 since 2004-05-03 11:04:34 PDT Keepalive settings:
 Interval 15 seconds Keepalives sent: 750 Notifications sent: 0 Last update from
 peer: 00:00:06 ago
```

CHAPTER 8

Operational Commands

ssh

Syntax

ssh *host*
<bypass-routing>
<inet | inet6>
<interface *interface-name*>
<logical-system *logical-system-name*>
<routing-instance *routing-instance-name*>
<source *address*>
<v1 | v2>

Syntax (EX Series Switch and the QFX Series)

ssh *host*
<bypass-routing>
<inet | inet6>
<interface *interface-name*>
<routing-instance *routing-instance-name*>
<source *address*>
<v1 | v2>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Use the SSH program to open a connection between a local router or switch and a remote system and execute commands on the remote system. You can issue the **ssh** command from the Junos OS CLI to log in to a remote system or from a remote system to log in to the local router or switch. When executing this command, you include one or more CLI commands by enclosing them in quotation marks and separating the commands with semicolons:

ssh *address* '*cli-command1* ; *cli-command2* '

Options

host—Name or address of the remote system.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

inet | inet6—(Optional) Create an IPv4 or IPv6 connection, respectively.

interface *interface-name*—(Optional) Interface name for the SSH session. (This option does not work when **default-address-selection** is configured at the **[edit system]** hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)

logical-system *logical-system-name*—(Optional) Name of a particular logical system for the SSH attempt.

routing-instance *routing-instance-name*—(Optional) Name of the routing instance for the SSH attempt.

source *address*—(Optional) Source address of the SSH connection.

v1 | v2—(Optional) Use SSH version 1 or 2, respectively, when connecting to a remote host.

Additional Information

To configure an SSH (version 1) key for your user account, include the **authentication ssh-rsa** statement at the **[edit system login user *user-name*]** hierarchy level. To configure an SSH (version 2) key for your user account, include the **authentication dsa-rsa** statement at the **[edit system login user *user-name*]** hierarchy level.

You can limit the number of times a user can attempt to enter a password while logging in through SSH. To specify the number of times a user can attempt to enter a password to log in through SSH, include the **retry-options** statement at the **[edit system login]** hierarchy level. For details, see the .

Required Privilege Level

network

Related Documentation

- *Configuring SSH Host Keys for Secure Copying of Data*

List of Sample Output

ssh on page 169

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

ssh

```
user@switch> ssh cree
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes

Host ?cree' added to the list of known hosts.
boojun@cree's password:
Last login: Sun Jun 21 10:43:42 1998 from junos-router
% ...
```

telnet

Syntax

telnet *host*
<8bit>
<bypass-routing>
<inet | inet6>
<interface *interface-name*>
<logical-system *logical-system-name*>
<no-resolve>
<port *port-number*>
<routing-instance *routing-instance-name*>
<source *source-address*>

Syntax (EX Series Switches)

telnet *host*
<8bit>
<bypass-routing>
<inet | inet6>
<interface *interface-name*>
<no-resolve>
<port *port-number*>
<routing-instance *routing-instance-name*>
<source *source-address*>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Open a telnet session to a remote system. Type Ctrl+] to escape from the telnet session to the telnet command level, and then type **quit** to exit from telnet.

Options

host—Name or address of the remote system.

8bit—(Optional) Use an 8-bit data path.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

inet | inet6—(Optional) Open an IPv4 or IPv6 session, respectively.

interface *interface-name*—(Optional) Interface name for the telnet session. (This option does not work when **default-address-selection** is configured at the **[edit system]** hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)

logical-system *logical-system-name*—(Optional) Name of a particular logical system for the telnet attempt.

no-resolve—(Optional) Do not attempt to determine the hostname that corresponds to the IP address.

port *port-number*—(Optional) Port number or service name on the remote system.

routing-instance ***routing-instance-name***—(Optional) Name of the routing instance for the telnet attempt.

source ***source-address***—(Optional) Source address of the telnet connection.

Additional Information You can limit the number of times a user can attempt to enter a password while logging in through telnet. To specify the number of times a user can attempt to enter a password to log in through telnet, include the **retry-options** statement at the [**edit system login**] hierarchy level. For details, see the *Junos OS Administration Library for Routing Devices*.

Required Privilege Level network

List of Sample Output telnet on page 171

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

telnet

```
user@host> telnet 192.154.1.254
Trying 192.154.169.254...
Connected to level5.company.net.
Escape character is '^]'.
ttypa
login:
```

PART 4

Index

Index

Symbols

A

B

C

D

R

S

T

U

W

X