



Junos[®] OS for EX Series Ethernet Switches

System Services on EX Series Switches

Release

15.1



Published: 2015-05-15

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos[®] OS for EX Series Ethernet Switches System Services on EX Series Switches
Release 15.1
Copyright © 2015, Juniper Networks, Inc.
All rights reserved.

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.

List of Figures

Part 1	Overview	
Chapter 2	DHCP Overview	7
	Figure 1: DHCP Client/Server Model	8
	Figure 2: DHCP Four-Step Transfer	10

Table 22: show system services service-deployment Output Fields 239

PART 1

Overview

- [Software Overview on page 3](#)
- [DHCP Overview on page 7](#)
- [Public Key Cryptography Overview on page 15](#)
- [Self-Signed Certificates Overview on page 17](#)
- [Protocol Redirect Mechanism Overview on page 19](#)

6. The DHCP relay agent receives the request packet and forwards copies of this packet to each of the two DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ack) packet that contains the client's configuration parameters.
8. The DHCP relay agent receives the ack packet and forwards it to the client.
9. The DHCP client receives the ack packet and stores the configuration information.
10. If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.
11. After establishing the initial lease on the IP address, the DHCP client and the DHCP server use unicast transmission to negotiate lease renewal or release. The DHCP relay agent snoops all of the packets unicast between the client and the server that pass through the relay agent to determine when the lease has expired or been released. This process is referred to as *lease shadowing* or *passive snooping*.

**Related
Documentation**

- [Configuring a DHCP Server on Switches \(CLI Procedure\) on page 32](#)
- [Configuring an Extended DHCP Relay Server on EX Series Switches \(CLI Procedure\) on page 35](#)

PART 2

Configuration

- [Configuration Tasks on page 23](#)
- [Configuration Statements on page 41](#)


```
user@switch# set no-redirects
```

For IPv6 traffic:

```
[edit interfaces interface-name unit logical-unit-number family family]  
user@switch# set no-redirects-ipv6
```

To re-enable the sending of redirect messages on the switch, delete the **no-redirects** statement (for IPv4 traffic) or the **no-redirects-ipv6** statement (for IPv6 traffic) from the configuration.

- Related Documentation**
- [Understanding the Protocol Redirect Mechanism on EX Series Switches on page 19](#)
 - *Junos OS Network Interfaces Library for Routing Devices*


```

boot-server (address | hostname);
default-lease-time (seconds | infinite);
domain-name domain-name;
domain-search {
    domain-suffix;
}
maximum-lease-time (seconds | infinite);
name-server {
    address;
}
next-server address;
option option-index (array type-name [ type-values ] | byte 8-bit-value | flag (false |
off | on | true) | integer signed-32-bit-value | ip-address address |
short signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
unsigned-short 16-bit-value);
pool ip-prefix/prefix-length {
    address-range low address high address;
    boot-file filename;
    boot-server (address | hostname);
    default-lease-time (seconds | infinite);
    domain-name domain-name;
    domain-search {
        domain-suffix;
    }
    exclude-address {
        ipv4-address;
    }
    maximum-lease-time (seconds | infinite);
    name-server {
        address;
    }
    next-server address;
    option option-index (array type-name type-values ] | byte 8-bit-value | flag (false |
off | on | true) | integer signed-32-bit-value | ip-address address |
short signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
unsigned-short 16-bit-value);
    propagate-settings interface-name;
    router {
        address;
    }
    server-identifier identifier;
    sip-server {
        address {
            address;
        }
        name {
            name;
        }
    }
    wins-server {
        address;
    }
}
router {
    address;
}

```

```

server-identifier identifier;
sip-server {
    address {
        address;
    }
    name {
        name;
    }
}
static-binding mac-address {
    boot-file filename;
    boot-server (address | hostname);
    client-identifier (ascii ascii-text | hexadecimal hexadecimal-value);
    domain-name domain-name;
    domain-search {
        domain-suffix;
    }
    fixed-address {
        ipv4-address;
    }
    host-name hostname;
    name-server {
        address;
    }
    next-server address;
    option option-index (array type-name type-values ] | byte 8-bit-value | flag (false |
        off | on | true) | integer signed-32-bit-value | ip-address address |
        short signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
        unsigned-short 16-bit-value);
    router {
        address;
    }
    server-identifier identifier;
    sip-server {
        address {
            address;
        }
        name {
            name;
        }
    }
    wins-server {
        address;
    }
}
traceoptions {
    file <filename> <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    level severity;
    no-remote-trace;
}
wins-server {
    address;
}
}

```



```

        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;
    include-option-82 {
        forcerenew;
        nak;
    }
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}

```



```

        pool pool-name;
    }
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    include-option-82 {
        forcerenew;
        nak;
    }
    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 {

```


- Related Documentation**
- *Extended DHCP Local Server Overview*
 - *DHCPv6 Local Server Overview*

[Switches Overview](#)” on page 11 for more information about the DHCP/BOOTP relay agent.

The remaining statements are explained separately.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) on page 35• Understanding the Extended DHCP Relay Agent for EX Series Switches on page 12

dhcpv6 (DHCP Local Server)

```
Syntax  dhcpv6 {
    access-profile profile-name;
    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 {
        access-profile profile-name;
        authentication {
            ...
        }
        interface interface-name {
            access-profile profile-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 {
        delete-binding-on-renegotiation;
        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;
    delete-binding-on-renegotiation;
    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;
    delete-binding-on-renegotiation;
    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 {

```


dhcpcv6 (DHCP Relay Agent)

```

Syntax  dhcpv6 {
    access-profile profile-name;
    active-server-group server-group-name;
    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;
        }
    }
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    forward-only {
        logical-system <current | default | logical-system-name>;
        routing-instance <current | default | routing-instance-name>;
    }
    forward-only-replies;
    group group-name {
        active-server-group server-group-name;
        authentication {
            ...
        }
        dynamic-profile profile-name {
            ...
        }
        forward-only {
            logical-system <current | default | logical-system-name>;
            routing-instance <current | default | routing-instance-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 {
    ...
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
}
overrides {
    ...
}
relay-agent-interface-id {
    ...
}
relay-agent-remote-id {
    ...
}
relay-option {
    ...
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
    ...
}
overrides {
    allow-snooped-clients;
    delay-authentication;
    delete-binding-on-renegotiation;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    send-release-on-delete;
}
relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
}
relay-agent-remote-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
}
relay-option {
```


- Related Documentation**
- *dhcp-relay*
 - *DHCPv6 Relay Agent Overview*
 - *Using External AAA Authentication Services with DHCP*

domain

Syntax

```
domain {  
  description text-description;  
  interface interface-name {  
    broadcast;  
    description text-description;  
    no-listen;  
    server address <logical-system logical-system-name> <routing-instance  
      routing-instance-name>;  
  }  
  server address <logical-system logical-system-name> <routing-instance  
    routing-instance-name>;  
}
```

Hierarchy Level [edit forwarding-options [helpers](#)]

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

Description Enable DNS request packet forwarding.

The remaining statements are explained separately.

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

- Related Documentation**
- *Configuring DNS and TFTP Packet Forwarding*

drop

Syntax	drop;
Hierarchy Level	[edit forwarding-options dhcp-relay relay-option-60]
Release Information	Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	Drop (discard) DHCP client packets when you use relay option 60 (relay-option-60 is enabled) in DHCP packets to forward client traffic to specific DHCP servers.
Default	Relay Option 60 is disabled.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) on page 35• Understanding the Extended DHCP Relay Agent for EX Series Switches on page 12

group (DHCP Local Server)

```
Syntax  group group-name {
        access-profile profile-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 {
            access-profile profile-name;
            exclude;
            overrides {
                client-discover-match <option60-and-option82 | incoming-interface>;
                delete-binding-on-renegotiation;
                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 {
```


- 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*

group (DHCP Relay Agent)

```
Syntax  group group-name {
        access-profile profile-name;
        active-server-group server-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;
        }
        forward-only {
            logical-system <current | default | logical-system-name>;
            routing-instance <current | default | routing-instance-name>;
        }
        interface interface-name {
            access-profile profile-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;
            }
        }
    }
```


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.

overrides—Override the specified default configuration settings for the interface. The **overrides** statement is described separately.

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

Related Documentation

- *Extended DHCP Relay Agent Overview*
- *dhcp-relay*
- *Grouping Interfaces with Common DHCP Configurations*
- *Using External AAA Authentication Services with DHCP*

- Related Documentation**
- *dhcp-relay*
 - *Extended DHCP Relay Agent Overview*
 - *Configuring Group-Specific DHCP Relay Options*
 - *Overriding the Default DHCP Relay Configuration Settings*


```
    aex;
    (backup | primary);
    lacp {
        force-up;
    }
}
(auto-negotiation | no-auto-negotiation);
(flow-control | no-flow-control);
ieee-802-3az-eee;
link-mode mode;
(loopback | no-loopback);
speed (auto-negotiation | speed);
}
(gratuitous-arp-reply | no-gratuitous-arp-reply);
hold-time up milliseconds down milliseconds;
media-type;
mtu bytes;
no-gratuitous-arp-request;
traceoptions {
    flag flag;
}
(traps | no-traps);
unit logical-unit-number {
    accounting-profile name;
    bandwidth rate;
    description text;
    disable;
    family family-name {...}
    proxy-arp (restricted | unrestricted);
    (traps | no-traps);
    vlan-id vlan-id-number;
}
vlan-tagging;
}
```

```

interfaces interface-range name {
interface-range   accounting-profile name;
                   description text;
                   disable;
                   ether-options {
                     802.3ad {
                       aex;
                       (backup | primary);
                       lacp {
                         force-up;
                       }
                     }
                     (auto-negotiation | no-auto-negotiation);
                     (flow-control | no-flow-control);
                     ieee-802-3az-eee;
                     link-mode mode;
                     (loopback | no-loopback);
                     speed (auto-negotiation | speed);
                   }
                   (gratuitous-arp-reply | no-gratuitous-arp-reply);
                   hold-time up milliseconds down milliseconds;
                   member interface-name;
                   member-range starting-interface name to ending-interface name;
                   mtu bytes;
                   unit logical-unit-number {
                     accounting-profile name;
                     bandwidth rate;
                     description text;
                     disable;
                     family family-name {...}
                     proxy-arp (restricted | unrestricted);
                     (traps | no-traps);
                     vlan-id vlan-id-number;
                   }
                   vlan-tagging;
                 }

interfaces lo0 lo0 {
                   accounting-profile name;
                   description text;
                   disable;
                   hold-time up milliseconds down milliseconds;
                   traceoptions {
                     flag flag;
                   }
                   (traps | no-traps);
                   unit logical-unit-number {
                     accounting-profile name;
                     bandwidth rate;
                     description text;
                     disable;
                     family family-name {...}
                     (traps | no-traps);
                   }
                 }

```



```
interfaces vme    vme {
    accounting-profile name;
    description text;
    disable;
    (gratuitous-arp-reply | no-gratuitous-arp-reply);
    hold-time up milliseconds down milliseconds;
    mtu bytes;
    no-gratuitous-arp-request;
    traceoptions {
        flag flag;
    }
    (traps | no-traps);
    unit logical-unit-number {
        accounting-profile name;
        bandwidth rate;
        description text;
        disable;
        family family-name {...}
        (traps | no-traps);
        vlan-id vlan-id-number;
    }
    vlan-tagging;
}
```


lease-time

Syntax	lease-time (<i>seconds</i> infinite);
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet dhcp]
Release Information	Statement introduced in Junos OS Release 8.5 for J Series devices. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 9.2 for SRX Series devices. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Request a specific lease time for the IP address. The lease time is the length of time in seconds that a client holds the lease for an IP address assigned by a DHCP server.
Default	If no lease time is requested by client, then the server sends the lease time. The default lease time on a JUNOS OS DHCP server is one day.
Options	seconds —Request a lease time of a specific duration. Range: 60 through 2147483647 seconds infinite —Request that the lease never expire.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring a DHCP Client (CLI Procedure) on page 31 • <i>Example: Configuring the Device as a DHCP Client</i> • interfaces on page 125 • <i>unit</i> • family on page 104

no-listen

Syntax	no-listen;
Hierarchy Level	[edit forwarding-options helpers bootp interface (<i>interface-name</i> <i>interface-group</i>)], [edit forwarding-options helpers domain interface <i>interface-name</i>], [edit forwarding-options helpers tftp interface <i>interface-name</i>]
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 11.3 for QFX Series switches.
Description	Disable recognition of DNS requests or stop packets from being forwarded on a logical interface, a group of logical interfaces, a router, or a switch.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring DNS and TFTP Packet Forwarding</i> • <i>Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents</i>

no-redirects (IPv4 Traffic)

Syntax	no-redirects;
Hierarchy Level	[edit system], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 12.3 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>Stop protocol redirect messages for IPv4 traffic from being sent on the entire switch or on an interface on the router or switch.</p> <p>To disable the sending of protocol redirect messages for the entire router or switch, include the no-redirects statement at the [edit system] hierarchy level.</p> <p>To disable the sending of protocol redirect messages on a specific interface, include the no-redirects statement at the [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>] hierarchy level.</p>
Default	The router or switch sends redirect messages.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Junos OS to Disable Protocol Redirect Messages on the Router or Switch• Understanding the Protocol Redirect Mechanism on EX Series Switches on page 19• Configuring Junos OS to Disable Sending Protocol Redirect Messages on EX Series Switches (CLI Procedure) on page 38• Junos OS Network Interfaces Library for Routing Devices

The remaining statements are explained separately.

The **interface-client-limit** statement is not supported in the **[edit system services dhcp-local-server dhcpv6]** hierarchy level.

The **delegated-pool**, **multi-address-embedded-option-response**, and the **rapid-commit** statements are supported in the **[edit system services dhcp-local-server dhcpv6 ...]** hierarchy level only.

Required Privilege Level	system—To view this statement in the configuration.
	system-control—To add this statement to the configuration.
Related Documentation	• <i>Extended DHCP Local Server Overview</i>
	• <i>Overriding Default DHCP Local Server Configuration Settings</i>
	• <i>Deleting DHCP Local Server and DHCP Relay Override Settings</i>

prefix (Address-Assignment Pools)

Syntax	<code>prefix <i>ipv6-prefix</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet6]
Release Information	Statement introduced in Junos OS Release 10.0. Statement introduced in Junos OS Release 12.3 for EX Series switches.
Description	Specify the IPv6 prefix for the IPv6 address-assignment pool. This statement is mandatory for IPv6 address-assignment pools.
Options	<i>ipv6-prefix</i> —The IPv6 prefix.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Address-Assignment Pools Overview</i>• <i>Configuring Address-Assignment Pools</i>

retransmission-interval

Syntax	<code>retransmission-interval seconds;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet dhcp]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the time between successive retransmissions of the client DHCP request if a DHCP server fails to respond.
Options	seconds —Number of seconds between successive retransmissions. Range: 4 through 64 seconds Default: 4 seconds
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring a DHCP Client (CLI Procedure) on page 31

services (System Services)

```
Syntax  services {
    dhcp { \* DHCP not supported on a DCF
        dhcp_services;
    }
    finger {
        connection-limit limit;
        rate-limit limit;
    }
    ftp {
        authentication-order [authentication-methods];
        connection-limit limit;
        rate-limit limit;
    }
    service-deployment {
        servers address {
            port-number port-number;
        }
        source-address address;
    }
    ssh {
        authentication-order [authentication-methods];
        connection-limit limit;
        protocol-version [v1 v2];
        rate-limit limit;
        root-login (allow | deny | deny-password);
    }
    telnet {
        authentication-order [authentication-methods];
        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*
- *Configuring the Junos OS to Work with SRC Software*

session (Time-out)

Syntax	<pre>session { idle-timeout <i>minutes</i>; session-limit <i>session-limit</i>; }</pre>
Hierarchy Level	[edit system services web-management]
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
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	<p>idle-timeout <i>minutes</i>—Configure the number of minutes a session can be idle before it times out.</p> <p>Range: 1 through 1440</p> <p>Default: 1440</p> <p>session-limit <i>session-limit</i>—Configure the maximum number of simultaneous J-Web user login sessions.</p> <p>Range: 1 through 1024</p> <p>Default: Unlimited</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>J-Web Interface User Guide</i>

sip-server

Syntax	<code>sip-server [address name];</code>
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 in Junos OS Release 10.1 for EX Series switches.
Description	Configure Session Initiation Protocol (SIP) server addresses or names for DHCP servers.
Options	<p>address—IPv4 address of the SIP server. To configure multiple SIP servers, include multiple address options. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).</p> <p>name—Fully qualified domain name of the SIP server. To configure multiple SIP servers, include multiple name options. This domain name must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring a DHCP SIP Server (CLI Procedure) on page 31• Configuring a DHCP Server on Switches (CLI Procedure) on page 32

source-address (SRC Software)

Syntax	<code>source-address source-address;</code>
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	<ul style="list-style-type: none">• Configuring the Junos OS to Work with SRC Software

source-address-giaddr

Syntax	source-address-giaddr;
Hierarchy Level	[edit forwarding-options helpers bootp], [edit forwarding-options helpers bootp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1 for EX Series switches.
Description	<p>Configure the gateway IP address (giaddr) as the source IP address of the switch for relayed DHCP packets when the switch is used as the DHCP relay agent.</p> <p>When this statement is entered in the [edit forwarding-options helpers bootp] hierarchy, the gateway IP address is configured as the source IP address of the switch for relayed DHCP packets exiting all interfaces on the switch.</p> <p>When this statement is entered in the [edit forwarding-options helpers bootp interface <i>interface-name</i>] hierarchy, the gateway IP address is configured as the source IP address of the switch for relayed DHCP packets exiting the specified interface of the switch.</p> <p>In Junos OS Release 10.1 for EX Series switches and later releases, the IP address of the interface that the DHCP packet exits on the switch acting as a DHCP relay agent is used as the source IP address for relayed DHCP packets by default.</p> <p>In Junos OS Releases 9.6 and 10.0 for EX Series switches, the gateway IP address of the switch is always used as the source IP address for relayed DHCP packets when the switch is used as the DHCP relay agent.</p> <p>In Junos OS Releases 9.3 through 9.5 for EX Series switches, the IP address of the interface that the DHCP packet exits on the switch acting as a DHCP relay agent is always used as the source IP address for relayed DHCP packets.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • DHCP/BOOTP Relay for Switches Overview on page 11

ssh

Syntax	<pre>ssh { authentication-order [<i>authentication-methods</i>]; ciphers [<i>cipher-1 cipher-2 cipher-3 ...</i>]; client-alive-count-max <i>seconds</i>; client-alive-interval <i>seconds</i>; connection-limit <i>limit</i>; hostkey-algorithm <<i>algorithm</i> no-<i>algorithm</i>>; key-exchange <<i>algorithm</i>>; macs <<i>algorithm</i>>; max-sessions-per-connection <<i>number</i>>; no-passwords; no-tcp-forwarding; protocol-version [<i>v1 v2</i>]; rate-limit <i>limit</i>; root-login (<i>allow</i> <i>deny</i> <i>deny-password</i>); }</pre>
Hierarchy Level	[edit system services]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>client-alive-interval and client-alive-max-count statements introduced in Junos OS Release 12.2.</p> <p>no-passwords statement introduced in Junos OS Release 13.3.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>
Description	<p>Allow SSH requests from remote systems to the local router or switch.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• <i>Configuring SSH Service for Remote Access to the Router or Switch</i>

static-binding

Syntax	<pre>static-binding <i>mac-address</i> { <i>client-identifier</i> (ascii <i>client-id</i> hexadecimal <i>client-id</i>); fixed-address { <i>address</i>; } host-name <i>client-hostname</i>; }</pre>
Hierarchy Level	<pre>[edit system services <i>dhcp</i>], [edit system services <i>dhcp</i>]</pre>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>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.</p>
Options	<p><i>mac-address</i>—The MAC address of the client. This is a hardware address that uniquely identifies a client on the network.</p> <p><i>fixed-address address</i>—Fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.</p> <p><i>host-name client-hostname</i>—Hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the <i>domain-name</i> statement.</p> <p><i>client-identifier (ascii client-id hexadecimal client-id)</i>—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, <i>Assigned Numbers</i>. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>DHCP Overview</i>

system-generated-certificate

Syntax	system-generated-certificate;
Hierarchy Level	[edit system services web-management https]
Release Information	Command introduced in Junos OS Release 11.1 for EX Series switches.
Description	Configure the automatically generated self-signed certificate for enabling HTTPS services..
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure) on page 36

telnet

Syntax	telnet { authentication-order [<i>authentication-methods</i>]; connection-limit <i>limit</i> ; rate-limit <i>limit</i> ; }
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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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	<ul style="list-style-type: none">• <i>Configuring Telnet Service for Remote Access to a Router or Switch</i>

tftp

Syntax	<pre>tftp { description text-description; interface interface-name { broadcast; description text-description; no-listen; server address <logical-system logical-system-name> <routing-instance routing-instance-name>; } server address <logical-system logical-system-name> <routing-instance routing-instance-name>; }</pre>
Hierarchy Level	[edit forwarding-options helpers]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>Enable TFTP request packet forwarding.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring DNS and TFTP Packet Forwarding</i>

trace (DHCP Relay Agent)

Syntax	trace;
Hierarchy Level	[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4. Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	Enable trace operations for a group of interfaces or for a specific interface within a group. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Tracing Extended DHCP Operations</i>• <i>Tracing Extended DHCP Operations for Specific Interfaces</i>

traceoptions (DNS and TFTP Packet Forwarding)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i>> <size <i>bytes</i>> <world-readable no-world-readable>; flag <i>flag</i>; level <i>level</i>; <no-remote-trace>; } </pre>
Hierarchy Level	[edit forwarding-options helpers]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement standardized and match option introduced in Junos OS Release 8.0.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Configure tracing operations for BOOTP, DNS and TFTP packet forwarding.
Default	If you do not include this statement, no tracing operations are performed.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" "). All files are placed in a file named fud in the directory /var/log. If you include the file statement, you must specify a filename.</p> <p>files <i>number</i>—(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.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> • address—Trace address management events • all—Trace all events • bootp—Trace BOOTP or DHCP services events • config—Trace configuration events • domain—Trace DNS service events • ifdb—Trace interface database operations • io—Trace I/O operations • main—Trace main loop events • port—Trace arbitrary protocol events

- **rtsock**—Trace routing socket operations
- **tftp**—Trace TFTP service events
- **trace**—Trace tracing operations
- **ui**—Trace user interface operations
- **util**—Trace miscellaneous utility operations

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing globally or for a specific tracing operation.

no-world-readable—(Optional) Restrict file access to the owner.

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** 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: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB


Range: 0 bytes through 4,294,967,295 KB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Tracing BOOTP, DNS, and TFTP Forwarding Operations</i>

traceoptions

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>>; flag all; flag certificates; flag database; flag general; flag ike; flag parse; flag policy-manager; flag routing-socket; flag timer; level no-remote-trace } </pre>
Hierarchy Level	<p>[edit security], [edit services ipsec-vpn]</p> <p>Trace options can be configured at either the [edit security] or the [edit services ipsec-vpn] hierarchy level, but not at both levels.</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure security trace options.</p> <p>To specify more than one trace option, include multiple flag statements. Trace option output is recorded in the <code>/var/log/kmd</code> file.</p>
<div style="display: flex; align-items: center;">  <p>NOTE: The <code>traceoptions</code> statement is not supported on QFabric systems.</p> </div>	
Options	<p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file (for example, <code>kmd</code>) reaches its maximum size, it is renamed <code>kmd.0</code>, then <code>kmd.1</code>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you must also specify a maximum file size with the size option.</p> <p>Range: 2 through 1000 files</p> <p>Default: 0 files</p> <p>size <i>size</i>—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, <code>kmd</code>) reaches this size, it is renamed, <code>kmd.0</code>, then <code>kmd.1</code> and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>Default: 1024 KB</p>

flag *flag*—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all security events.
- **certificates**—Trace certificate events.
- **database**—Trace database events.
- **general**—Trace general events.
- **ike**—Trace IKE module processing.
- **parse**—Trace configuration processing.
- **policy-manager**—Trace policy manager processing.
- **routing-socket**—Trace routing socket messages.
- **timer**—Trace internal timer events.

level *level*—(Optional) Set traceoptions level.

- **all**—match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

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

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

Related Documentation	• <i>Configuring Tracing Operations for Security Services</i>
------------------------------	---

traceoptions (DHCP Server)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regex</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; } </pre>
Hierarchy Level	[edit system services dhcp]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Define tracing operations for DHCP processes.
Options	<p>file <i>filename</i>—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.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named <i>trace-file</i> reaches its maximum size, it is renamed <i>trace-file.0</i>, then <i>trace-file.1</i>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> • 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: **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	system—To view this statement in the configuration.
	system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Tracing Operations for DHCP Processes</i> • <i>System Management Configuration Statements</i>

update-server

Syntax	update-server;
Hierarchy Level	[edit Interfaces <i>interface-name</i> unit <i>logical-unit-number</i> inet dhcp]
Release Information	Statement introduced in Junos OS Release 8.5 for J Series devices. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 9.2 for SRX Series devices. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Propagate TCP/IP settings learned from an external DHCP server to the DHCP server running on the switch, router, or device.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring a DHCP Client (CLI Procedure) on page 31 • <i>Example: Configuring the Device as a DHCP Client</i> • interfaces on page 125 • <i>unit</i> • family on page 104

use-interface-description

Syntax	<code>use-interface-description (logical device);</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit forwarding-options dhcp-relay relay-option-82 (circuit-id remote-id)],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 (circuit-id remote-id)],</p> <p>[edit logical-systems <i>logical-system-name</i> ... forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit logical-systems <i>logical-system-name</i> ... forwarding-options dhcp-relay ... relay-option-82 (circuit-id remote-id)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ... relay-option-82 (circuit-id remote-id)],</p> <p>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options option-18],</p> <p>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options option-37]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p> <p>Support at the [edit ... relay-agent-remote-id] and [edit ... remote-id] hierarchy levels introduced in Junos OS Release 14.1.</p> <p>Support at the [edit vlans <i>vlan-name</i> dhcp-security dhcpv6-options option-18] and [edit vlans <i>vlan-name</i> dhcp-security dhcpv6-options option-37] hierarchy levels introduced in Junos OS Release 14.1X53-D10 for EX Series switches.</p>
Description	Use the textual interface description instead of the interface identifier in the DHCP base option 82 Agent Circuit ID (suboption 1) or Agent Remote ID (suboption 2) information, or in the DHCPv6 option 18 (Relay Agent Interface ID) or option 37 (Relay Agent Remote ID) information in DHCP packets that the DHCP relay agent sends to a DHCP server.



NOTE: For integrated routing and bridging (IRB) interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID. You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

If you specify that the textual description be used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface description. When you configure the **no-vlan-interface-name** statement, the textual description also includes IRB's description. The textual description is configured using the **description** statement at the [edit interfaces *interface-name*] hierarchy level.



NOTE: The `use-interface-description` statement is mutually exclusive with the `no-vlan-interface-name` and `use-vlan-id` statements.

If you specify the textual interface description, rather than accepting the default syntax, the identification is for packets returned from the server, and only for instances where that identification would be required by the DHCP relay, such as a stateless pass-through.



NOTE: By default, DHCP relay accepts a maximum of 253 ASCII characters. If the textual interface description exceeds 253 characters, DHCP relay drops the packet, which results in the DHCP client failing to bind.

Options **logical**—Use the textual description that is configured for the logical interface.
 device—Use the textual description that is configured for the device interface.

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

Related Documentation

- *Including a Textual Description in DHCP Options*
- *Using DHCP Relay Agent Option 82 Information*
- *Configuring DHCPv6 Relay Agent Options*

use-primary (DHCP Relay Agent)


Syntax	<code>use-primary <i>primary-profile-name</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>],</p> <p>[edit forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Specify the dynamic profile to configure as the primary dynamic profile. The primary dynamic profile is instantiated when the first subscriber logs in. Subsequent subscribers are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber logs out, the next subscriber that logs in is assigned the primary dynamic profile.</p> <p>Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>EX Series switches do not support DHCPv6.</p>
Options	<i>primary-profile-name</i> —Name of the dynamic profile to configure as the primary dynamic profile
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

Related Documentation • *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*

vendor-id

Syntax	vendor-id <i>vendor-id</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet dhcp]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure a vendor class ID for the Dynamic Host Configuration Protocol (DHCP) client.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	• Configuring a DHCP Client (CLI Procedure) on page 31

vendor-option

Syntax	<pre>vendor-option { default-local-server-group <i>local-server-group-name</i> default-relay-server-group <i>server-group-name</i> drop; equals starts-with }</pre>
Hierarchy Level	[edit forwarding-options dhcp-relay relay-option-60]
Release Information	Statement introduced before Junos OS Release 12.1 for EX Series switches. Statement deprecated in Junos OS Release 12.3 for EX Series switches.
Description	Configure the match criteria when you use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers. The extended DHCP relay agent compares the option 60 vendor-specific strings received in DHCP client packets against the match criteria that you specify. If there is a match, you can define certain actions for the associated DHCP client packets.
<div> NOTE: The <code>vendor-option</code> statement has been deprecated and might be removed from future product releases. We recommend that you phase out its use. See option-number.</div>	
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) on page 35• Understanding the Extended DHCP Relay Agent for EX Series Switches on page 12

web-management

Syntax	<pre> web-management { http { interfaces [<i>interface-names</i>]; port <i>port</i>; } https { interfaces [<i>interface-names</i>]; local-certificate <i>name</i>; port <i>port</i>; } } </pre>
Hierarchy Level	[edit system services]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>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.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Management Access for the EX Series Switch (J-Web Procedure)</i> • <i>J-Web Interface User Guide</i> • http on page 117 • https on page 118 • port on page 155

wins-server (System)

Syntax	<code>wins-server { <code>address</code>; }</code>
Hierarchy Level	[edit system services <code>dhcp</code>], [edit system services <code>dhcp</code>], [edit system services <code>dhcp pool</code>], [edit system services <code>dhcp static-binding</code>]
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 <code>\\Marketing</code>). List servers in order of preference.
Options	<code>address</code> —IPv4 address of the NetBIOS Name Server running WINS. To configure multiple servers, include multiple <code>address</code> options.
Required Privilege Level	<code>system</code> —To view this statement in the configuration. <code>system-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><i>DHCP Overview</i>

PART 3

Administration

- [Routine Monitoring on page 201](#)
- [Operational Commands on page 207](#)

CHAPTER 8

Routine Monitoring

- [Monitoring DHCP Services on page 201](#)
- [Verifying and Managing DHCP Relay Configuration for EX Series Switches on page 205](#)

Monitoring DHCP Services

Purpose



NOTE: This topic applies only to the J-Web Application package.

A switch or router can operate as a DHCP server. Use the monitoring functionality to view information about dynamic and static DHCP leases, conflicts, pools, and statistics.

Action

To monitor the DHCP server in the J-Web interface, select **Monitor > Services > DHCP**.

To monitor the DHCP server in the CLI, enter the following CLI commands:

- `show system services dhcp binding`
- `show system services dhcp conflict`
- `show system services dhcp pool`
- `show system services dhcp statistics`
- `show system services dhcp relay-statistics`
- `show system services dhcp global`
- `show system services dhcp client`
- `clear system services dhcp binding`
- `clear system services dhcp conflict`
- `clear system services dhcp statistics`
- `clear dhcp relay-statistics`

On EX4300 switches, to monitor the DHCP server in the CLI, enter the following CLI commands:

- `show dhcp server binding`
- `show dhcp server statistics`
- `show dhcp relay binding`
- `show dhcp relay statistics`
- `clear dhcp server binding`
- `clear dhcp server statistics`
- `clear dhcp relay binding`
- `clear dhcp relay statistics`

Meaning [Table 11 on page 202](#) summarizes the output fields in DHCP displays in the J-Web interface.

Table 11: Summary of DHCP Output Fields

Field	Values	Additional Information
Global tab		
Name	This column displays the following information: <ul style="list-style-type: none">• Boot lease length• Domain Name• Name servers• Server identifier• Domain search• Gateway routers• WINS server• Boot file• Boot server• Default lease time• Minimum lease time• Maximum lease time	
Value	Displays the value for each of the parameters in the Name column.	
Bindings tab		
Allocated Address	List of IP addresses the DHCP server has assigned to clients.	
MAC Address	Corresponding media access control (MAC) address of the client.	
Binding Type	Type of binding assigned to the client: dynamic or static .	DHCP servers can assign a dynamic binding from a pool of IP addresses or a static binding to one or more specific IP addresses.

Table 11: Summary of DHCP Output Fields (*continued*)

Field	Values	Additional Information
Lease Expires	Date and time the lease expires, or never for leases that do not expire.	
Pools tab		
Pool Name	Subnet on which the IP address pool is defined.	
Low Address	Lowest address in the IP address pool.	
High Address	Highest address in the IP address pool.	
Excluded Addresses	Addresses excluded from the address pool.	
Clients tab		
Interface Name	Name of the logical interface.	
Hardware Address	Vendor identification.	
Status	State of the client binding.	
Address Obtained	IP address obtained from the DHCP server.	
Update Server	Indicates whether server update is enabled.	
Lease Obtained	Date and time the lease was obtained.	
Lease Expires	Date and time the lease expires.	
Renew	Reacquires an IP address from the server for the interface. When you click this option, the command sends a discover message if the client state is INIT and a renew request message if the client state is BOUND. For all other states it performs no action.	
Release	Clears other resources received earlier from the server, and reinitializes the client state to INIT for the particular interface.	
Conflicts tab		
Detection Time	Date and time the client detected the conflict.	

Table 11: Summary of DHCP Output Fields (*continued*)

Field	Values	Additional Information
Detection Method	How the conflict was detected.	Only client-detected conflicts are displayed.
Address	IP address where the conflict occurs.	The addresses in the conflicts list remain excluded until you use the clear system services dhcp conflict command to manually clear the list.

DHCP Statistics**Relay Statistics tab**

Packet Counters	Displays the number of packet counters.
Dropped Packet Counters	Graphically displays the number of dropped packet counters.

Statistics tab

Packets dropped	Total number of packets dropped and the number of packets dropped due to a particular condition.
Messages received	Number of BOOTREQUEST, DHCPDECLINE, DHCPDISCOVER, DHCPINFORM, DHCPRELEASE, and DHCPREQUEST messages sent from DHCP clients and received by the DHCP server.
Messages sent	Number of BOOTREPLY, DHCPACK, DHCPOFFER, DHCPNAK, and DHCPFORCERENEW messages sent from the DHCP server to DHCP clients.

[Table 12 on page 204](#) summarizes the output fields in DHCP displays in EX4300 switches in the J-Web interface.

Table 12: Summary of DHCP Output Fields for EX4300 Switches

Field	Values	Additional Information
Binding Information tab		
IP Address	IP address of the DHCP client..	
Session ID	Session ID of the subscriber session.	
Hardware Address	Hardware address of the DHCP client.	
Expires	Number of seconds in which the lease expires.	

Table 12: Summary of DHCP Output Fields for EX4300 Switches (*continued*)

Field	Values	Additional Information
State	State of the address binding table on the extended DHCP local server: <ul style="list-style-type: none"> • BOUND—Client has an active IP address lease. • FORCERENEW—Client has received the FORCERENEW message from the server. • INIT—Initial state. • RELEASE—Client is releasing the IP address lease. • RENEWING—Client is sending a request to renew the IP address lease. • REQUESTING—Client is requesting a DHCP server. • SELECTING—Client is receiving offers from DHCP servers. 	
Interface	Interface on which the request was received.	

Table 13 on page 205 summarizes the output fields in DHCP Statistics Information for EX4300 switches in the J-Web interface.

Table 13: Summary of the DHCP Statistics Information Output for EX4300 switches

Field	Values	Additional Information
Message Counters		
Message Counters	Graphically displays the number of messages sent and received.	
Dropped packet Counters		
MAC Limit	Graphically displays the number of dropped packet counters.	

- Related Documentation**
- [Configuring DHCP Services \(J-Web Procedure\) on page 23](#)
 - [Understanding DHCP Services for Switches on page 7](#)

Verifying and Managing DHCP Relay Configuration for EX Series Switches

Purpose View or clear statistics for extended DHCP relay agent:

- Action**
- To display extended DHCP relay agent statistics:

```
user@switcht> show dhcp relay statistics
```
 - To clear all extended DHCP relay agent statistics:

```
user@switcht> clear dhcp relay statistics
```

- Related Documentation**
- [Configuring an Extended DHCP Relay Server on EX Series Switches \(CLI Procedure\) on page 35](#)
 - [Understanding the Extended DHCP Relay Agent for EX Series Switches on page 12](#)

CHAPTER 9

Operational Commands

- clear dhcp relay statistics
- clear security pki local-certificate
- clear system services dhcp binding
- clear system services dhcp conflict
- clear system services dhcp statistics
- request ipsec switch
- request security certificate enroll (Signed)
- request security certificate enroll (Unsigned)
- request security key-pair
- request security pki generate-key-pair
- request security pki local-certificate generate-self-signed
- show dhcp relay statistics
- show security pki local-certificate
- 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
- ssh
- telnet

clear dhcp relay statistics

Syntax	<code>clear dhcp relay statistics</code> <code><logical-system <i>logical-system-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code>
Syntax	Syntax for EX Series switches: <code>show dhcp relay statistics</code> <code><routing-instance <i>routing-instance-name</i>></code>
Release Information	Command introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 12.1 for EX Series switches. Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.
Description	Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics.
Options	<code>logical-system <i>logical-system-name</i></code> —(On routers only) (Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are cleared for the default logical system. <code>routing-instance <i>routing-instance-name</i></code> —(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show dhcp relay statistics on page 222
List of Sample Output	clear dhcp relay statistics on page 209
Output Fields	Table 14 on page 209 lists the output fields for the <code>clear dhcp relay statistics</code> command.

Table 14: clear dhcp relay statistics Output Fields

Field Name	Field Description
Packets dropped	<p>Number of packets discarded by the extended DHCP relay agent application due to errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</p> <ul style="list-style-type: none"> • Total—Total number of packets discarded by the extended DHCP relay agent application. • Bad hardware address—Number of packets discarded because an invalid hardware address was specified. • Bad opcode—Number of packets discarded because an invalid operation code was specified. • Bad options—Number of packets discarded because invalid options were specified. • Invalid server address—Number of packets discarded because an invalid server address was specified. • Lease Time Violation—Number of packets discarded because of a lease time violation • No available addresses—Number of packets discarded because there were no addresses available for assignment. • No interface match—Number of packets discarded because they did not belong to a configured interface. • No routing instance match—Number of packets discarded because they did not belong to a configured routing instance. • No valid local address—Number of packets discarded because there was no valid local address. • Packet too short—Number of packets discarded because they were too short. • Read error—Number of packets discarded because of a system read error. • Send error—Number of packets that the extended DHCP relay application could not send. • Option 60—Number of packets discarded containing DHCP option 60 vendor-specific information. • Option 82—Number of packets discarded because DHCP option 82 information could not be added.
Messages received	<p>Number of DHCP messages received.</p> <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received • DHCPDECLINE—Number of DHCP PDUs of type DECLINE received • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received • DHCPINFORM—Number of DHCP PDUs of type INFORM received • DHCPRELEASE—Number of DHCP PDUs of type RELEASE received • DHCPREQUEST—Number of DHCP PDUs of type REQUEST received
Messages sent	<p>Number of DHCP messages sent.</p> <ul style="list-style-type: none"> • BOOTREPLY—Number of BOOTP PDUs transmitted • DHCPOFFER—Number of DHCP OFFER PDUs transmitted • DHCPACK—Number of DHCP ACK PDUs transmitted • DHC PNACK—Number of DHCP NACK PDUs transmitted

Sample Output

clear dhcp relay statistics

The following sample output displays the DHCP relay statistics before and after the **clear dhcp relay statistics** command is issued.

```
user@host> show dhcp relay statistics
```

```
Packets dropped:
  Total          1
  Lease Time Violated 1

Messages received:
  BOOTREQUEST    116
  DHCPDECLINE    0
  DHCPDISCOVER   11
  DHCPINFORM     0
  DHCPRELEASE    0
  DHCPREQUEST    105

Messages sent:
  BOOTREPLY      44
  DHCPOFFER      11
  DHCPACK        11
  DHCPNAK        11
```

```
user@host> clear dhcp relay statistics
```


```
user@host> show dhcp relay statistics
```

```
Packets dropped:
  Total          0

Messages received:
  BOOTREQUEST    0
  DHCPDECLINE    0
  DHCPDISCOVER   0
  DHCPINFORM     0
  DHCPRELEASE    0
  DHCPREQUEST    0

Messages sent:
  BOOTREPLY      0
  DHCPOFFER      0
  DHCPACK        0
  DHCPNAK        0
```

clear security pki local-certificate

Syntax	clear security pki local-certificate <all certificate-id <i>certificate-id-name</i> system-generated>
Release Information	Command introduced in Junos OS Release 11.1 for EX Series switches.
Description	Delete local digital certificates, certificate requests, and the corresponding public/private key pairs from the switch.
Options	<p>all—(Optional) Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.</p> <hr/> <div style="display: flex; align-items: center;">  <div> <p>NOTE: This option does not delete the automatically generated self-signed certificate or its public/private key pair.</p> </div> </div> <hr/> <p>certificate-id <i>certificate-id-name</i>—(Optional) Delete the specified local digital certificate and corresponding public and private key pair.</p> <p>system-generated—(Optional) Delete the automatically generated self-signed certificate.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • Deleting Self-Signed Certificates (CLI Procedure) on page 38
List of Sample Output	clear security pki local-certificate all on page 211
Output Fields	This command produces no output.

Sample Output

clear security pki local-certificate all

```
user@switch> clear security pki local-certificate all
```

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	<ul style="list-style-type: none">• show system services dhcp binding on page 228
List of Sample Output	clear system services dhcp binding on page 212
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	<ul style="list-style-type: none"> • show system services dhcp conflict on page 231
List of Sample Output	clear system services dhcp conflict on page 213
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	<ul style="list-style-type: none">• show system services dhcp statistics on page 236
List of Sample Output	clear system services dhcp statistics on page 214
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
```

request ipsec switch


Syntax	<code>request ipsec switch (interface <es-fpc/pic/port> security-associations <sa-name>)</code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(Encryption interface on M Series, PTX Series, and T Series routers and EX Series switches only) Manually switch from the primary to the backup encryption services interface, or switch from the primary to the backup IP Security (IPsec) tunnel.
Options	<code>interface <es-fpc/pic/port></code> —Switch to the backup encryption interface. <code>security-associations <sa-name></code> —Switch to the backup tunnel.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show ipsec redundancy
List of Sample Output	request ipsec switch security-associations on page 215
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request ipsec switch security-associations

```
user@host> request ipsec switch security-associations sa-private
```

request security certificate enroll (Signed)

Syntax	request security certificate enroll filename <i>filename</i> subject <i>subject</i> alternative-subject <i>alternative-subject</i> certification-authority <i>certification-authority</i> encoding (binary pem) key-file <i>key-file</i> domain-name <i>domain-name</i>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Obtain a signed certificate from a certificate authority (CA). The signed certificate validates the CA and the owner of the certificate. The results are saved in a specified file to the <code>/var/etc/ikecert</code> directory.
<div>  <p>NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard. The <code>request security key-pair</code> command is deprecated and not available with Junos in FIPS mode because it generates RSA and DSA keys with sizes of 512 and 1024 bits that are not compliant with the NIST SP 800-131A standard.</p> </div>	
Options	<p>filename <i>filename</i>—File that stores the certificate.</p> <p>subject <i>subject</i>—Distinguished name (dn), which consists of a set of components—for example, an organization (o), an organization unit (ou), a country (c), and a locality (l).</p> <p>alternative-subject <i>alternative-subject</i>—Tunnel source address.</p> <p>certification-authority <i>certification-authority</i>—Name of the certificate authority profile in the configuration.</p> <p>encoding (binary pem)—File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default format is binary.</p> <p>key-file <i>key-file</i>—File containing a local private key.</p> <p>domain-name <i>domain-name</i>—Fully qualified domain name.</p>
Required Privilege Level	maintenance
List of Sample Output	<code>request security certificate enroll filename subject alternative-subject certification-authority key-file domain-name (Signed)</code> on page 217
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security certificate enroll filename subject alternative-subject certification-authority key-file
domain-name (Signed)

```
user@host> request security certificate enroll filename host.crt subject c=uk,o=london  
alternative-subject 10.50.1.4 certification-authority verisign key-file host-1.prv domain-name  
host.juniper.net  
CA name: juniper.net CA file: ca_verisign  
local pub/private key pair: host.prv  
subject: c=uk,o=london domain name: host.juniper.net  
alternative subject: 10.50.1.4  
Encoding: binary  
Certificate enrollment has started. To view the status of your enrollment, check  
the key management process (kmd) log file at /var/log/kmd. <-----
```

request security certificate enroll (Unsigned)

Syntax	<code>request security certificate enroll filename <i>filename</i> ca-file <i>ca-file</i> ca-name <i>ca-name</i> encoding (binary perm) url <i>url</i></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Obtain a certificate from a certificate authority (CA). The results are saved in a specified file to the <code>/var/etc/ikecert</code> directory.
Options	<p>filename <i>filename</i>—File that stores the public key certificate.</p> <p>ca-file <i>ca-file</i>—Name of the certificate authority profile in the configuration.</p> <p>ca-name <i>ca-name</i>—Name of the certificate authority.</p> <p>encoding (binary pem)—File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default value is binary.</p> <p>url <i>url</i>—Certificate authority URL.</p>
Required Privilege Level	maintenance
List of Sample Output	request security certificate enroll filename ca-file ca-name url (Unsigned) on page 218
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output


request security certificate enroll filename ca-file ca-name url (Unsigned)

```

user@host> request security certificate enroll filename ca_verisign ca-file verisign ca-name
juniper.net urlxyzcompany URL
http://<verisign ca-name xyzcompany url>/cgi-bin/pkiclient.exe CA name: juniper.net
CA file: verisign Encoding: binary
Certificate enrollment has started. To view the status of your enrollment, check
the key management process (kmd) log file at /var/log/kmd. <-----

```

request security key-pair

Syntax	<code>request security key-pair <i>filename</i></code> <code><size <i>key-size</i>></code> <code><type (rsa dsa)></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Generate a public and private key pair for a digital certificate.
<div>  <p>NOTE: The <code>request security-certificates</code> command is deprecated and are not available with Junos in FIPS mode because security certificates are not compliant with the NIST SP 800-131A standard.</p> </div>	
Options	<p><i>filename</i>—Name of a file in which to store the key pair.</p> <p><i>size key-size</i>—(Optional) Key size, in bits. The key size can be 512, 1024, or 2048. The default value is 1024.</p> <p><i>type</i>—(Optional) Algorithm used to encrypt the key:</p> <ul style="list-style-type: none"> • rsa—RSA algorithm. This is the default. • dsa—Digital signature algorithm with Secure Hash Algorithm (SHA).
Required Privilege Level	maintenance
List of Sample Output	request security key-pair on page 219
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security key-pair

```
user@host> request security key-pair security-key-file
```

request security pki generate-key-pair

Syntax	<code>request security pki generate-key-pair certificate-id <i>certificate-id-name</i></code> <code><size (512 1024 2048)></code> <code><type (dsa rsa)></code>
Release Information	Command introduced in Junos OS Release 11.1 for EX Series switches.
Description	Generate a public key infrastructure (PKI) public/private key pair for a local digital certificate.
Options	<p>certificate-id <i>certificate-id-name</i>—Name of the local digital certificate and the public/private key pair.</p> <p>size—(Optional) Key pair size. The key pair size can be 512, 1024, or 2048 bits. If a key pair size is not specified, the default value, 1024 bits, is applied.</p> <p>type—(Optional) The algorithm to be used for encrypting the public/private key pair. The encryption algorithm can be dsa or rsa. If an encryption algorithm is not specified, the default value, rsa, is applied.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 37
List of Sample Output	request security pki generate-key-pair on page 220
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki generate-key-pair

```
user@switch> request security pki generate-key-pair certificate-id billy size 2048
Generated key pair billy, key size 2048 bits
```

request security pki local-certificate generate-self-signed

Syntax	<code>request security pki local-certificate generate-self-signed certificate-id <i>certificate-id-name</i> domain-name <i>domain-name</i> ip-address <i>ip-address</i> email <i>email-address</i> subject <i>subject-distinguished-name</i></code>
Release Information	Command introduced in Junos OS Release 11.1 for EX Series switches.
Description	Manually generate a self-signed certificate for the given distinguished name.
Options	<p>certificate-id <i>certificate-id-name</i>—Name of the local digital certificate and the public/private key pair.</p> <p>domain-name <i>domain-name</i>—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.</p> <p>email <i>email-address</i>—E-mail address of the certificate holder.</p> <p>ip-address <i>ip-address</i>—IP address of the switch.</p> <p>subject <i>subject-distinguished-name</i>—Distinguished name format that contains the common name, department, company name, state, and country:</p> <ul style="list-style-type: none"> • CN—Common name • OU—Organizational unit name • O—Organization name • ST—State • C—Country
Required Privilege Level	<p>maintenance</p> <p>security</p>
Related Documentation	<ul style="list-style-type: none"> • Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 37
List of Sample Output	request security pki local-certificate generate-self-signed on page 221
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki local-certificate generate-self-signed

```
user@switch> request security pki local-certificate generate-self-signed certificate-id self-cert
subject cn=abc domain-name abc.net email jdoe@abc.net
Self-signed certificate generated and loaded successfully
```

show dhcp relay statistics

Syntax	<code>show dhcp relay statistics</code> <code><logical-system <i>logical-system-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code>
Syntax	Syntax for EX Series switches: <code>show dhcp relay statistics</code> <code><routing-instance <i>routing-instance-name</i>></code>
Release Information	Command introduced in Junos OS Release 8.3. Command introduced in Junos OS Release 12.1 for EX Series switches. Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.
Description	Display Dynamic Host Configuration Protocol (DHCP) relay statistics.
Options	<code>logical-system <i>logical-system-name</i></code> —(On routers only) (Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are displayed for the default logical system. <code>routing-instance <i>routing-instance-name</i></code> —(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are displayed for the default routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• clear dhcp relay statistics on page 208
List of Sample Output	show dhcp relay statistics on page 224
Output Fields	Table 15 on page 223 lists the output fields for the <code>show dhcp relay statistics</code> command. Output fields are listed in the approximate order in which they appear.

Table 15: show dhcp relay statistics Output Fields

Field Name	Field Description
Packets dropped	<p>Number of packets discarded by the extended DHCP relay agent application due to errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</p> <ul style="list-style-type: none"> • Total—Total number of packets discarded by the extended DHCP relay agent application. • Bad hardware address—Number of packets discarded because an invalid hardware address was specified. • Bad opcode—Number of packets discarded because an invalid operation code was specified. • Bad options—Number of packets discarded because invalid options were specified. • Invalid server address—Number of packets discarded because an invalid server address was specified. • Lease Time Violation—Number of packets discarded because of a lease time violation • No available addresses—Number of packets discarded because there were no addresses available for assignment. • No interface match—Number of packets discarded because they did not belong to a configured interface. • No routing instance match—Number of packets discarded because they did not belong to a configured routing instance. • No valid local address—Number of packets discarded because there was no valid local address. • Packet too short—Number of packets discarded because they were too short. • Read error—Number of packets discarded because of a system read error. • Send error—Number of packets that the extended DHCP relay application could not send. • Option 60—Number of packets discarded containing DHCP option 60 vendor-specific information. • Option 82—Number of packets discarded because DHCP option 82 information could not be added.
Messages received	<p>Number of DHCP messages received.</p> <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received • DHCPDECLINE—Number of DHCP PDUs of type DECLINE received • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received • DHCPINFORM—Number of DHCP PDUs of type INFORM received • DHCPRELEASE—Number of DHCP PDUs of type RELEASE received • DHCPREQUEST—Number of DHCP PDUs of type REQUEST received
Messages sent	<p>Number of DHCP messages sent.</p> <ul style="list-style-type: none"> • BOOTREPLY—Number of BOOTP PDUs transmitted • DHCPOFFER—Number of DHCP OFFER PDUs transmitted • DHCPACK—Number of DHCP ACK PDUs transmitted • DHCPNACK—Number of DHCP NACK PDUs transmitted • DHCPFORCERENEW—Number of DHCP FORCERENEW PDUs transmitted
External Server Response	State of the external DHCP server responsiveness.
Packets forwarded	<p>Number of packets forwarded.</p> <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTREQUEST protocol data units (PDUs) forwarded • BOOTREPLY—Number of BOOTREPLY protocol data units (PDUs) forwarded

Table 15: show dhcp relay statistics Output Fields (*continued*)

Field Name	Field Description
External Server Response	State of the external DHCP server responsiveness.

Sample Output

show dhcp relay statistics

```

user@host> show dhcp relay statistics
Packets dropped:
    Total                               34
    Bad hardware address                 1
    Bad opcode                           1
    Bad options                          3
    Invalid server address               5
    Lease Time Violation                 1
    No available addresses               1
    No interface match                   2
    No routing instance match            9
    No valid local address                4
    Packet too short                     2
    Read error                           1
    Send error                           1
    Option 60                            1
    Option 82                            2

Messages received:
    BOOTREQUEST                         116
    DHCPDECLINE                          0
    DHCPDISCOVER                         11
    DHCPINFORM                           0
    DHCPRELEASE                          0
    DHCPREQUEST                          105

Messages sent:
    BOOTREPLY                            0
    DHCPOFFER                            2
    DHCPACK                              1
    DHCPNAK                              0
    DHCPFORCERENEW                       0

Packets forwarded:
    Total                                4
    BOOTREQUEST                           2
    BOOTREPLY                             2

External Server Response:
    State                                Responding

```

show security pki local-certificate

Syntax	show security pki local-certificate <brief detail> <certificate-id <i>certificate-id-name</i> > <system-generated>
Release Information	Command introduced in Junos OS Release 11.1 for EX Series switches.
Description	Display information about the local digital certificates and the corresponding public keys installed in the switch.
Options	<p>none—(Same as brief) Display information about all local digital certificates and corresponding public keys.</p> <p>brief detail—(Optional) Display information about local digital certificates and corresponding public keys for the specified level of output.</p> <p>certificate-id <i>certificate-id-name</i>—(Optional) Display information about only the specified the local digital certificate and corresponding public keys.</p> <p>system-generated—(Optional) Display information about the automatically generated self-signed certificate.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 37
List of Sample Output	show security pki local-certificate on page 226 show security pki local-certificate detail on page 227
Output Fields	Table 16 on page 225 lists the output fields for the show security pki local-certificate command. Output fields are listed in the approximate order in which they appear.

Table 16: show security pki local-certificate Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	detail
Serial number	Unique serial number of the digital certificate.	detail
Issued by	Authority that issued the digital certificate.	none brief
Issued to	Device that was issued the digital certificate.	none brief

Table 16: show security pki local-certificate Output Fields (*continued*)

Field Name	Field Description	Level of Output
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: <ul style="list-style-type: none"> • Common name—Name of the authority. • Organization—Organization of origin. • Organizational unit—Department within an organization. • State—State of origin. • Country—Country of origin. 	detail
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: <ul style="list-style-type: none"> • Common name—Name of the authority. • Organization—Organization of origin. • Organizational unit—Department within an organization. • State—State of origin. • Country—Country of origin. 	detail
Alternate subject	Domain name or IP address of the device related to the digital certificate.	detail
Validity	Time period when the digital certificate is valid. Values are: <ul style="list-style-type: none"> • Not before—Start time when the digital certificate becomes valid. • Not after—End time when the digital certificate becomes invalid. 	All levels
Public key algorithm	Encryption algorithm used with the private key, such as rsaEncryption (1024 bits) .	All levels
Public key verification status	Public key verification status: Failed or Passed . The detail output also provides the verification hash.	All levels
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as sha1WithRSAEncryption .	detail
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	detail
Distribution CRL	Distinguished name information and URL for the certificate revocation list (CRL) server.	detail
Use for key	Use of the public key, such as Certificate signing , CRL signing , Digital signature , or Key encipherment .	detail

Sample Output

show security pki local-certificate

```

user@switch> show security pki local-certificate
Certificate identifier: local-entrust2
Issued to: router2.juniper.net, Issued by: juniper

```

```

Validity:
  Not before: 2005 Nov 21st, 23:28:22 GMT
  Not after: 2008 Nov 21st, 23:58:22 GMT
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed

```

show security pki local-certificate detail

```

user@switch> show security pki local-certificate detail
Certificate identifier: local-entrust3
Certificate version: 3
Serial number: 4355 94f9
Issuer:
  Organization: juniper, Country: us
Subject:
  Organization: juniper, Country: us, Common name: switch1.juniper.net
Alternate subject: switch1.juniper.net
Validity:
  Not before: 2005 Nov 21st, 23:33:58 GMT
  Not after: 2008 Nov 22nd, 00:03:58 GMT
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
fb:79:df:d4:a9:03:0f:d3:69:7e:c1:e4:27:35:9c:d9:b1:a2:47:78
d2:6d:f3:e5:f4:68:4f:b3:04:45:88:57:99:82:39:a6:51:9e:5f:42
23:3f:d7:6e:3d:a5:54:a9:b1:2d:6e:90:dd:12:8a:bf:ef:2b:20:50
ba:f0:da:d9:0c:ad:5e:d6:c6:98:3a:ae:3f:90:dd:94:78:c1:ea:2e
7c:f0:2d:d4:79:d4:cd:f0:52:df:5e:72:f2:e7:ae:66:f7:61:f4:bc
72:57:3e:6c:6d:d3:24:58:8b:f4:ef:da:2a:6a:fa:eb:98:f8:34:84
79:54:da:4f:d3:6f:52:1f
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  61:3a:d0:b4:7a:16:9b:39:ba:81:3f:9d:ab:34:e5:c8:be:3b:a1:6d (sha1)
  60:a0:ff:58:05:4a:65:73:9d:74:3a:e1:83:6f:1b:c8 (md5)
Distribution CRL:
  C=us, O=juniper, CN=CRL1
  http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: Digital signature

```

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	<ul style="list-style-type: none"> • clear system services dhcp binding on page 212
List of Sample Output	show system services dhcp binding on page 229 show system services dhcp binding address on page 229 show system services dhcp binding address detail on page 229
Output Fields	Table 17 on page 228 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 17: 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 17: 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	<ul style="list-style-type: none"> • clear system services dhcp conflict on page 213
List of Sample Output	show system services dhcp conflict on page 231
Output Fields	Table 18 on page 231 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 18: 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 233
Output Fields	Table 19 on page 232 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 19: 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 235 show system services dhcp pool subnet-address on page 235 show system services dhcp pool subnet-address detail on page 235
Output Fields	Table 20 on page 234 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 20: 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	(<i>subnet-address</i> option only) Subnet to which the specified address pool belongs.	None specified
Address range	(<i>subnet-address</i> 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 20: 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	<ul style="list-style-type: none"> • clear system services dhcp statistics on page 214
List of Sample Output	show system services dhcp statistics on page 237
Output Fields	Table 21 on page 236 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 21: 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: <ul style="list-style-type: none"> • 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 21: show system services dhcp statistics Output Fields (*continued*)

Field Name	Field Description
Messages received	<p>Number of the following message types sent from DHCP clients and received by the DHCP server:</p> <ul style="list-style-type: none"> • BOOTREQUEST • DHCPDECLINE • DHCPDISCOVER • DHCPINFORM • DHCPRELEASE • DHCPREQUEST
Messages sent	<p>Number of the following message types sent from the DHCP server to DHCP clients:</p> <ul style="list-style-type: none"> • 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. Command introduced in Junos OS Release 14.1X53-D20 for the OCX 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 239
Output Fields	Table 22 on page 239 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 22: 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
```

ssh

List of Syntax [Syntax on page 240](#)
 [Syntax \(EX Series Switch and the QFX Series\) on page 240](#)

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.
 Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

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 241](#)

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

List of Syntax [Syntax on page 242](#)
[Syntax \(EX Series Switches\) on page 242](#)

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 243](#)

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:
```

