Services Feature Guide for the OCX Series

Release
14.1X53

Modified: 2015-06-17

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

Services Feature Guide for the OCX Series
14.1X53

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

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

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

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

Supported Platforms

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

- OCX1100

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**

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

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

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

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.

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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/cgi-bin/docbugreport/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/

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

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

Opening a Case with JTAC

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

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

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

PART 1

Configuring Port Mirroring

CHAPTER 1

Using Port Mirroring

Understanding Port Mirroring

Port Mirroring Overview

Use port mirroring to send traffic to devices that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on. Port mirroring is needed when you want to perform traffic analysis because a switch normally sends packets only to the port to which the destination device is connected. You probably do not want to send the original packets for analysis before they are forwarded because of the delay that this would cause, so the common alternative is to configure port mirroring to send copies of unicast traffic to another interface and run an analyzer application on a device connected to that interface. .

To configure port mirroring, you configure a port-mirroring instance. You do not specify an input for this instance. Instead, you create a firewall filter that specifies the required traffic and directs it to the instance by including the **port-mirror** action in a **then** term of the filter. The firewall filter must be configured as **family inet**.

Keep performance in mind when configuring port mirroring. Configuring the firewall filter to mirror only the necessary packets reduces the possibility of a performance impact.

Port-Mirroring Terminology

Table 3 on page 4 lists the terms used in the documentation about port mirroring and provides definitions.

Table 3: Port Mirroring Terms and Definitions

Term	Description
Port mirroring instance	A port-mirroring configuration that does not specify an input.. A firewall filter must be used to send traffic to the port mirror. Use the action **port-mirror** action in the firewall filter configuration to send packets to the port mirror.
Output interface (also known as monitor interface)	Access interface to which packet copies are sent and to which a device running an analyzer application is connected. The following limitations apply to an output interface: • Cannot also be a source port. • Cannot be used for switching. • Cannot be an aggregated Ethernet interface (LAG). If the capacity of the output interface is insufficient to handle the traffic from the source ports, overflow packets are dropped.
Output IP address	IP address of the device running an analyzer application. The device can be on a remote network. When you use this feature, the mirrored packets are GRE-encapsulated. The analyzer device must be able to de-encapsulate GRE-encapsulated packets, or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer device. (You can use a network sniffer to de-encapsulate the packets.) • An output IP address cannot be in the same subnetwork as any of the switch's management interfaces. • If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (inet.0 routing table).
Monitoring station	Computer running an analyzer application.
Local port mirroring	Port-mirroring configuration in which the mirrored packets are sent to an interface on the same switch.

Port Mirroring Constraints and Limitations

Port Mirroring Constraints on OCX Series Switches

The following constraints and limitations apply to port mirroring on OCX Series switches:

- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit from the output interface.
- You can create only one port-mirroring session.
- You cannot mirror packets exiting or entering the following ports:
  - Management interfaces
  - Routed VLAN interfaces or IRB interfaces
- An aggregated Ethernet interface cannot be an output interface.

- When packet copies are sent out the output interface, they are not modified for any changes that are normally applied on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.
- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.

Related Documentation

- Configuring Port Mirroring on page 9
- Example: Mirroring Employee Web Traffic with a Firewall Filter on page 5
- *Troubleshooting Port Mirroring*

Example: Mirroring Employee Web Traffic with a Firewall Filter

Requirements

This example uses the following hardware and software components:

- One switch
- Junos 14.1X53-D20

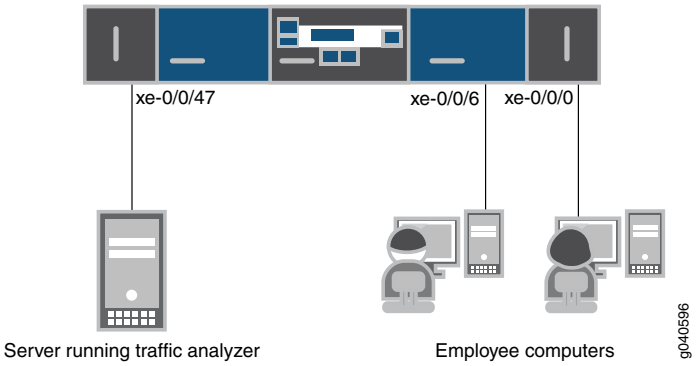
Overview

In this example, **xe-0/0/0** and **xe-0/0/6** serve as connections for employee computers. Interface **xe-0/0/47** is connected to a device running an analyzer application.

Rather than mirror all traffic, it is usually desirable to mirror only certain traffic. This is a more-efficient use of your bandwidth and hardware and might be necessary because of constraints on these assets. This example mirrors only traffic sent from employee computers to the Web.

Figure 1 on page 6 shows the network topology for this example.

Figure 1: Network Topology for Local Port Mirroring Example



Configuring

To specify that the only traffic that will be mirrored is traffic sent by employees to the Web, perform the tasks explained in this section. To select this traffic for mirroring, you use a firewall filter to specify this traffic and direct it to a port-mirroring instance.

CLI Quick Configuration

To quickly configure local port mirroring of traffic from employee computers that is destined for the Web, copy the following commands and paste them into a switch terminal window:

```
[edit]
set forwarding-options port-mirroring family inet output interface xe-0/0/47.0 next-hop
192.0.2.100/24
set firewall family inet filter watch-employee term employee-to-corp from destination-address
192.0.2.16/24
set firewall family inet filter watch-employee term employee-to-corp from source-address
192.0.2.16/24
set firewall family inet filter watch-employee term employee-to-corp then accept
set firewall family inet filter watch-employee term employee-to-web from destination-port 80
set firewall family inet filter watch-employee term employee-to-web then port-mirror
set interfaces xe-0/0/0 unit 0 family address 192.0.1.1/24
set interfaces xe-0/0/6 unit 0 family address 192.0.1.2/24
set interfaces xe-0/0/47 unit 0 family address 192.0.1.3/24
set interfaces xe-0/0/0 unit 0 family inet filter input watch-employee
set interfaces xe-0/0/6 unit 0 family inet filter input watch-employee
```

Step-by-Step Procedure

To configure local port mirroring of employee-to-web traffic from the two ports connected to employee computers:

1. Configure a port-mirroring instance, including the output interface and the IP address of the device running the analyzer application as the next hop. (Configure only the output—the input comes from the filter.) You must also specifying that the mirror is for IPv4 traffic (**family inet**).

   ```
   [edit forwarding-options]
   user@switch# set forwarding-options port-mirroring family inet output interface
   xe-0/0/47.0 next-hop 192.0.2.100/28
   ```

2. Configure an IPv4 (**family inet**) firewall filter called **watch-employee** that includes a term to match traffic sent to the Web and send it to the port-mirroring instance. Traffic sent to and arriving from the corporate subnet (destination or source address of **192.0.2.16/24**) does not need to be copied, so first create another term to accept that traffic before it reaches the term that sends Web traffic to the instance:

```
[edit firewall family inet]
er@switch# set filter watch-employee term employee-to-corp from destination-address
192.0.2.16/24
user@switch# set filter watch-employee term employee-to-corp from source-address
192.0.2.16/24
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirror
```

3. Configure addresses for the IPv4 interfaces connected to the employee computers and the analyzer device:

```
[edit interfaces]
user@switch# set xe-0/0/0 unit 0 family inet address 192.0.1.1/24
user@switch# set xe-0/0/6 unit 0 family inet address 192.0.1.2/24
user@switch# set interfaces xe-0/0/47 unit 0 family address 192.0.1.3/24
```

4. Apply the firewall filter to the appropriate interfaces as an ingress filter:

```
[edit interfaces]
user@switch# set xe-0/0/0 unit 0 family inet filter input watch-employee
user@switch# set xe-0/0/6 unit 0 family inet filter input watch-employee
```

Results Check the results of the configuration:

```
[edit]
user@switch# show
forwarding-options {
  port-mirroring {
      employee-web-monitor {
        output {
          ip-address 192.0.2.100.0;
          }
        }
      }
    }
  }
}
...
firewall family inet {
  filter watch-employee {
    term employee-to-corp {
      from {
        destination-address 192.0.2.16/24;
        source-address 192.0.2.16/24;
      }
      then accept {
    }
    term employee-to-web {
      from {
        destination-port 80;
      }
      then port-mirror;
    }
  }
}
...
interfaces {
  xe-0/0/0 {
```

```
      unit 0 {
        family inet {
          filter {
            input watch-employee;
          }
        }
      }
    }
    xe-0/0/6 {
      family inet {
        filter {
          input watch-employee;
        }
      }
    }
  }
```

Verification

Verifying That the Analyzer Has Been Correctly Created

Purpose Verify that the analyzer has been created on the switch with the appropriate input interfaces and appropriate output interface.

Action You can verify that the port mirror analyzer has been configured as expected using the **show forwarding-options port-mirroring** command.

```
user@switch> show forwarding-options port-mirroring
Instance Name:
  Instance Id: 1
  Input parameters:
    Rate                  : 1
    Run-length            : 0
    Maximum-packet-length : 0
  Output parameters:
    Family              State     Destination          Next-hop
    inet                up      xe-0/0/47.0          192.0.2.100
```

Meaning This output shows that the port-mirroring instance has a ratio of 1 (mirroring every packet, the default setting) and the maximum size of the original packet that was mirrored (**0** indicates the entire packet). If the state of the output interface is down or if the output interface is not configured, the value of state will be **down** and the instance will not be programmed for mirroring.

Related Documentation

- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 9
- Port Mirroring Constraints and Limitations on page 4

Configuring Port Mirroring

You use port mirroring to copy packets and send the copies to a device running an application such as a network analyzer or intrusion detection application so that you can analyze traffic without delaying it. We recommend that you disable port mirroring when you are not using it. To avoid creating a performance issue If you do enable port mirroring, we recommend that you select specific input interfaces instead of using the **all** keyword. You can also limit the amount of mirrored traffic by using a firewall filter.

- Configuring a Port Mirroring Instance on page 9

Configuring a Port Mirroring Instance

To configure port mirroring, you configure a port-mirroring instance and direct traffic to it by using a firewall filter. You do not specify an input for this instance. Instead, you create a firewall filter that specifies the required traffic and directs it to the instance. You also do not specify a name for this instance. (A name is not required because you can create no more than one port mirroring instance.)

To configure port mirroring:

1. Configure an IPv4 (family inet) port-mirroring instance. Configure only the output. For example, enter:

   ```
   [edit forwarding-options]
   user@switch# set port-mirroring family inet output interface interface-name next-hop
   ip-address
   ```

   NOTE: **You cannot configure input to this instance.**

2. Create an IPv4 (family inet) firewall filter using any of the available match conditions.

   - In a **from** term, specify the interfaces that you will apply the filter to—that is, the interfaces for which you want to mirror traffic.

     NOTE: **When specifying the interfaces for which you want to mirror traffic, you must specify the unit. For example, enter from interface xe-/0/0/47.0.**

   - In a **then** term, specify include the action modifier **port-mirror**.

3. Apply the firewall filter to the interfaces:

   ```
   [edit]
   user@switch# set interfaces interface-name unit 0 family inet filter input filter-name
   ```

Related Documentation

- Understanding Port Mirroring on page 3
- Example: Mirroring Employee Web Traffic with a Firewall Filter on page 5
- Port Mirroring Constraints and Limitations on page 4

- *Overview of Firewall Filters*

Port Mirroring Constraints and Limitations

- Port Mirroring Constraints on OCX Series Switches on page 10

Port Mirroring Constraints on OCX Series Switches

The following constraints and limitations apply to port mirroring on OCX Series switches:

- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit from the output interface.
- You can create only one port-mirroring session.
- You cannot mirror packets exiting or entering the following ports:
  - Management interfaces
  - Routed VLAN interfaces or IRB interfaces
- An aggregated Ethernet interface cannot be an output interface.
- When packet copies are sent out the output interface, they are not modified for any changes that are normally applied on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.
- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.

Related Documentation

- Understanding Port Mirroring on page 3
- Example: Mirroring Employee Web Traffic with a Firewall Filter on page 5
- Configuring Port Mirroring on page 9

PART 2

Configuring DHCP and DHCP Relay

CHAPTER 2

Using DHCP and DHCP Relay

DHCP and BOOTP Relay Overview

You can configure a Juniper Networks switch to act as a Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) relay agent. This means that if the switch receives a broadcast DHCP or BOOTP request from a locally attached host (client), it relays the message to a specified DHCP or BOOTP server. You should configure the switch to be a DHCP/BOOTP relay agent if you have locally attached hosts and a distant DHCP or BOOTP server.

You can configure the switch to use 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. For information on configuring this option, see the *source-address-giaddr* configuration statement.

You can also use smart DHCP relay, which enables you to configure alternative IP addresses for the gateway interface so that if the server fails to reply to the requests sent from the primary gateway address, the switch can resend the requests using the alternative gateway addresses. To use this feature, you must configure a Layer 3 interface, Layer 3 subinterface, or IRB interface with multiple IP addresses and configure that interface to be a relay agent.

NOTE: **Because DHCP and BOOTP messages are broadcast and are not directed to a specific server, switch, or router, Juniper switches cannot function as both a DHCP server and a DHCP/BOOTP relay agent at the same time. The Junos operating system (Junos OS) generates a commit error if both options are configured at the same time, and the commit operation does not succeed until one of the options is removed.**

Related Documentation

- Configuring DHCP and BOOTP on page 14
- *Configuring DHCP Relay*

Configuring DHCP and BOOTP

You can configure a switch to act as a Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) server or DHCP relay agent. When a switch is a relay agent, if a locally attached host issues a DHCP or BOOTP request as a broadcast message, the switch relays the message to a specified DHCP or BOOTP server. You should configure a switch to be a DHCP and BOOTP relay agent if you have locally attached hosts and a remote DHCP or BOOTP server.

NOTE: This task uses the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Configuring DHCP and BOOTP Relay*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

To configure a switch to be a server, use the dhcp-local-server statement. To configure a switch to be a relay agent, use the dhcp-relay statement.

If you want to enable BOOTP support when the switch is configured to be a DHCP server, enter the following statement:

```
[edit system services dhcp-local-server]
user@switch# set overrides bootp-support
```

If you want to enable BOOTP support when the switch is configured to be a DHCP relay agent, enter the following statement:

```
[edit forwarding-options dhcp-relay]
user@switch# set overrides bootp-support
```

PART 3

Configuration Statements and Operational Commands

CHAPTER 3

Configuration Statements for Port Mirroring

family (Port Mirroring)

Syntax

```
family
  inet
    output {
      ip-address address {
      }
      routing-instance instance-name {
        ip-address address {
      }
    }
```

Hierarchy Level [edit forwarding-options port-mirroring [instance *name*]]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify the type of interface that will be used to forward port mirrored packet to an analyzer device..

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

Related Documentation

- Understanding Port Mirroring on page 3
- Example: Mirroring Employee Web Traffic with a Firewall Filter on page 5
- Configuring Port Mirroring on page 9

inet (Port Mirroring)

Syntax

```
inet {
output {
  ip-addressaddress {
  }
  routing-instance instance-name {
    ip-address address {
  }
}
```

Hierarchy Level [edit forwarding-options port-mirroring [instance *name*] family]

Release Information Statement introduced in Junos OS Release 14.1X53 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify that the output interface will be of type **inet**. Use this statement so that you can send the mirrored packets to the IP address of the device running an analyzer application. The device can be on a remote network. When you use this feature, the mirrored packets are GRE-encapsulated. The analyzer device must be able to de-encapsulate GRE-encapsulated packets, or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer device. (You can use a network sniffer to de-encapsulate the packets.)

NOTE: An output IP address cannot be in the same subnetwork as any of the switch's management interfaces.

NOTE: If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (inet.0 routing table).

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

Related Documentation

- Understanding Port Mirroring on page 3
- Example: Mirroring Employee Web Traffic with a Firewall Filter on page 5
- Configuring Port Mirroring on page 9

ip-address (Port Mirroring)

Syntax ip-address *ip-address*;

Hierarchy Level [edit forwarding-options] analyzer *name* output]
[edit forwarding-options port-mirroring [instance *name*] family ethernet-switching output interface *name*]

Release Information Statement introduced in Junos OS Release 14.1X53 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify the IP address to which traffic should be mirrored (the IP address of the analyzer system). The device can be on a remote network. The analyzer device must be able to de-encapsulate GRE-encapsulated packets, or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer device. (You can use a network sniffer to de-encapsulate the packets.) This statement is not supported on QFabric systems.

NOTE: An output IP address cannot be in the same subnetwork as any of the switch's management interfaces.

NOTE: If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (inet.0 routing table).

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

output

Syntax

```
output {
  interface interface-name;
  ip-address ip-address;
  vlan (vlan-id | vlan-name);
  routing-instance instance-name {
    ip-address address {
}
```

Hierarchy Level

For platforms without ELS:

[edit ethernet-switching-options analyzer *name*]

For platforms with ELS:

[edit forwarding-options analyzer *name*]
[edit forwarding-options port-mirroring [instance *name*] family ethernet-switching]

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Option **output vlan** added in Junos OS Release 12.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the destination for mirrored traffic, either an interface on the switch (for local monitoring) or a VLAN (for remote monitoring).

The statements are explained separately.

Required Privilege Level

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

port-mirroring

Syntax

```
port-mirroring {
  family {
    inet
      output {
        ip-address address {
        }
        routing-instance instance-name {
          ip-address address {
        }
      }
  }
  instance instance-name {
    family
      inet
        output {
          ip-address address {
          }
          routing-instance instance-name {
            ip-address address {
          }
        }
      }
    }
  }
}
```

Hierarchy Level [edit forwarding-options]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Create a port-mirroring configuration.

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

Related Documentation

- Understanding Port Mirroring on page 3
- Example: Mirroring Employee Web Traffic with a Firewall Filter on page 5
- Configuring Port Mirroring on page 9

routing-instance (Port Mirroring)

Syntax routing-instance *instance-name*;

Hierarchy Level [edit forwarding-options] analyzer *name* output]
[edit forwarding-options port-mirroring [instance *name*] family inet output interface *name*]

Release Information Statement introduced in Junos OS Release 12.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure a port mirroring instance. You do not specify an input for this instance. Instead, you, create a firewall filter that specifies the required traffic and directs it to the mirror. This instance type is useful for controlling which types of traffic should be mirrored.

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

CHAPTER 4

Configuration Statements for DHCP and DHCP Relay

dhcp-local-server

Syntax

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

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

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

```
      client-discover-match (option60-and-option82 | incoming-interface);
      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);
    include-option-82 {
      forcerenew;
      nak;
    }
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
  }
  pool-match-order {
    external-authority;
    ip-address-first;
    option-82;
  }
  reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
```

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

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 13.2X51 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

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

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

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

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

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

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

dhcp-relay

Syntax

```
dhcp-relay {
  active-server-group server-group-name;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-name;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  dhcpv6 {
    active-server-group server-group-name;
    authentication {
      password password-string;
      username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-name;
        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;
    }
    group group-name {
      active-server-group server-group-name;
      authentication {
        ...
      }
      dynamic-profile profile-name {
        ...
      }
      interface interface-name {
        exclude;
        liveness-detection {
          failure-action (clear-binding | clear-binding-if-interface-up | log-only);
          method {
```

```
            bfd {
              version (0 | 1 | automatic);
              minimum-interval milliseconds;
              minimum-receive-interval milliseconds;
              multiplier number;
              no-adaptation;
              transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
              }
              detection-time {
                threshold milliseconds;
              }
              session-mode(automatic | multihop | singlehop);
              holddown-interval milliseconds;
            }
          }
        }
        overrides {
          ...
        }
        relay-option {
          ...
        }
        service-profile dynamic-profile-name;
        trace;
        upto upto-interface-name;
      }
      route-suppression:
      service-profile dynamic-profile-name;
      overrides {
        ...
      }
      relay-agent-interface-id {
        ...
      }
      relay-agent-remote-id {
        ...
      }
      relay-option {
        ...
      }
      route-suppression;
      server-response-time seconds;
      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 {
      allow-snooped-clients;
      delay-authentication;
      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);
    }
    server-group {
      server-group-name {
        server-ip-address;
      }
    }
duplicate-clients-in-subnet (incoming-interface | option-82):
dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
}
forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
group group-name {
    active-server-group server-group-name;
    authentication {
      ...
    }
    dynamic-profile profile-name {
      ...
    }
    interface interface-name {
      exclude;
      liveness-detection {
        failure-action (clear-binding | clear-binding-if-interface-up | log-only);
        method {
          bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
```

```
                minimum-receive-interval milliseconds;
                multiplier number;
                no-adaptation;
                transmit-interval {
                  minimum-interval milliseconds;
                  threshold milliseconds;
                }
                detection-time {
                  threshold milliseconds;
                }
                session-mode(automatic | multihop | singlehop);
                holddown-interval milliseconds;
              }
            }
          }
          overrides {
            ...
          }
          service-profile dynamic-profile-name;
          trace;
          upto upto-interface-name;
        }
        overrides {
          ...
        }
        relay-option {
          ...
        }
        relay-option-82 {
          ...
        }
        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 {
```

```
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    client-discover-match (option60-and-option82 | incoming-interface);
    delay-authentication;
    disable-relay;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
    proxy-mode;
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
  }
  relay-option {
    option-number option-number;
    default-action {
      drop;
      forward-only;
      relay-server-group group-name;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
      drop;
      forward-only;
      relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
      drop;
      forward-only;
      local-server-group local-server-group;
      relay-server-group relay-server-group;
    }
  }
  relay-option-82 {
    circuit-id {
      prefix prefix;
      use-interface-description (logical | device);
    }
    remote-id {
      prefix prefix;
      use-interface-description (logical | device);
    }
  }
  server-group {
    server-group-name {
      server-ip-address;
    }
  }
  route-suppression:
  server-response-time seconds;
  service-profile dynamic-profile-name;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 13.2X51 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure extended Dynamic Host Configuration Protocol (DHCP) relay and DHCPv6 relay options on the router or switch and enable the router (or switch) to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.

DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.

The extended DHCP and DHCPv6 relay agent options configured with the **dhcp-relay** and **dhcpv6** statements are incompatible with the DHCP/BOOTP relay agent options configured with the **bootp** statement. As a result, the extended DHCP or DHCPv6 relay agent and the DHCP/BOOTP relay agent cannot both be enabled on the router (or switch) at the same time.

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*
- *DHCPv6 Relay Agent Overview*
- *DHCP Relay Proxy Overview*
- *Using External AAA Authentication Services with DHCP*

CHAPTER 5

Configuration Statements for Encryption

authentication-key-chains

Syntax

```
authentication-key-chains {
  key-chain key-chain-name {
    description text-string;
    key key {
      algorithm (md5 | hmac-sha-1);
      options (basic | isis-enhanced);
      secret secret-data;
      start-time yyyy-mm-dd.hh:mm:ss;
    }
    tolerance seconds;
  }
}
```

Hierarchy Level [edit security]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure authentication key updates for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol. When the **authentication-key-chains** statement is configured at the **[edit security]** hierarchy level, and is associated with the BGP, LDP, or IS-IS protocols at the **[edit protocols]** hierarchy level or with the BFD protocol using the **bfd-liveness-detection** statement, authentication key updates can occur without interrupting routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

ca-name

Syntax ca-name *ca-identity*;

Hierarchy Level [edit security certificates certification-authority]

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 (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the certificate authority (CA) identity to use in the certificate request.

Options ***ca-identity***—CA identity to use in the certificate request.

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

Related Documentation
- *Configuring Digital Certificates for an ES PIC*

cache-size

Syntax cache-size *bytes*;

Hierarchy Level [edit security certificates]

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 (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the cache size for digital certificates.

Options ***bytes***—Cache size for digital certificates.

Range: 64 through 4,294,967,295

Default: 2 megabytes (MB)

NOTE: We recommend that you limit your cache size to 4 MB.

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

Related Documentation

- *Configuring Digital Certificates for an ES PIC*

cache-timeout-negative

Syntax cache-timeout-negative *seconds*;

Hierarchy Level [edit security certificates]

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 (Encryption interface on M Series and T Series routers and EX Series switches only) Configure a negative cache for digital certificates.

Options ***seconds***—Negative time to cache digital certificates, in seconds.

Range: 10 through 4,294,967,295

Default: 20

CAUTION: **Configuring a large negative cache value can lead to a denial-of-service attack.**

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

Related Documentation

- *Configuring Digital Certificates for an ES PIC*

certificates

Syntax

```
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority ca-profile-name {
    ca-name ca-identity;
    crl file-name;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
  }
  enrollment-retry attempts;
  local certificate-name {
    certificate-key-string;
    load-key-file URL filename;
  }
  maximum-certificates number;
  path-length certificate-path-length;
}
```

Hierarchy Level [edit security]

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

(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificates for IPsec.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring Digital Certificates for an ES PIC*

certification-authority

Syntax

```
certification-authority ca-profile-name {
  ca-name ca-identity;
  crl file-name;
  encoding (binary | pem);
  enrollment-url url-name;
  file certificate-filename;
  ldap-url url-name;
}
```

Hierarchy Level [edit security certificates]

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 (Encryption interface on M Series and T Series routers and EX Series switches only) Configure a certificate authority profile name.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring Digital Certificates for an ES PIC*

crl (Encryption Interface)

Syntax crl *file-name*;

Hierarchy Level [edit security certificates]

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 (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.

Options ***file-name***—Specify the file from which to read the CRL.

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

Related Documentation
- *Configuring Digital Certificates for an ES PIC*

encoding

Syntax encoding (binary | pem);

Hierarchy Level [edit security ike policy *ike-peer-address*],
[edit security certificates certification-authority *ca-profile-name*]

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 (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file format used for the **local-certificate** and **local-key-pair** statements.

Options **binary**—Binary file format.

pem—Privacy-enhanced mail (PEM), an ASCII base 64 encoded format.

Default: **binary**

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

Related Documentation
- *Configuring Digital Certificates for an ES PIC*
- *Configuring an IKE Policy for Digital Certificates for an ES PIC*

enrollment-retry

Syntax enrollment-retry *attempts*;

Hierarchy Level [edit security certificates]

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 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify how many times a router or switch can resend a digital certificate request.

Options ***attempts***—Number of enrollment retries.

Range: 0 through 100

Default: 0

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

Related Documentation
- *Configuring Digital Certificates for an ES PIC*

enrollment-url

Syntax enrollment-url *url-name*;

Hierarchy Level [edit security certificates certification-authority *ca-profile-name*]

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 (Encryption interface on M Series and T Series routers and EX Series switches only) Specify where your router or switch sends Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests (certificate authority URL).

Options *url-name*—Certificate authority URL.

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

Related Documentation
- *Configuring Digital Certificates for an ES PIC*

file

Syntax file *certificate-filename*;

Hierarchy Level [edit security certificates certification-authority *ca-profile-name*]

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 (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file from which to read the digital certificate.

Options *certificate-filename*—File from which to read the digital certificate.

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

Related Documentation

- *Configuring Digital Certificates for an ES PIC*

key (Authentication Keychain)

Syntax

```
key key {
    algorithm (md5 | hmac-sha-1);
    options (basic | isis-enhanced);
    secret secret-data;
    start-time yyyy-mm-dd.hh:mm:ss;
}
```

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name*]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure the authentication element.

Options

key—Each key within a keychain is identified by a unique integer value.

Range: 0 through 63

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

key-chain (Security)

Syntax

```
keychain key-chain-name {
  description text-string;
  key key {
    algorithm (md5 | hmac-sha-1);
    options (basic | isis-enhanced);
    secret secret-data;
    start-time yyyy-mm-dd.hh:mm:ss;
  }
  tolerance seconds;
}
```

Hierarchy Level [edit security authentication-key-chains]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Create the key-chain configuration for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol.

Options

key-chain-name—Authentication keychain name. It can be up to 126 characters. Characters can include any ASCII strings. If you include spaces, enclose all characters in quotation marks (“ ”).

Required Privilege Level

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

Related Documentation

- authentication-key-chains on page 36
- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

ldap-url

Syntax <ldap-url *url-name*>;

Hierarchy Level [edit security certificates certification-authority *ca-profile-name*]

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 (Encryption interface on M Series and T Series routers and EX Series switches only) (Optional) Specify the Lightweight Directory Access Protocol (LDAP) URL for digital certificates.

Options ***url-name***—Name of the LDAP URL.

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

Related Documentation
- *Configuring Digital Certificates for an ES PIC*

local

Syntax

```
local certificate-name {
    certificate-key-string;
    load-key-file URL filename;
}
```

Hierarchy Level [edit security certificates]

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 Import a paired X.509 private key and authentication certificate, to enable Junos XML protocol client applications to establish Secure Sockets Layer (SSL) connections to the router or switch.

NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard.

Options

certificate-namecertificate-key-string—String of alphanumeric characters that constitute the private key and certificate.

certificate-name—Name that uniquely identifies the certificate.

load-key-file *URL filename*—File that contains the private key and certificate. It can be one of two types of values:

- Pathname of a file on the local disk (assuming you have already used another method to copy the certificate file to the router's or switch's local disk)
- URL to the certificate file location (for instance, on the computer where the Junos XML protocol client application runs)

Required Privilege Level

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

Related Documentation

- *Importing SSL Certificates for Junos XML Protocol Support*

maximum-certificates

Syntax maximum-certificates *number*;

Hierarchy Level [edit security certificates]

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 (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the maximum number of peer digital certificates to be cached.

Options ***number***—Maximum number of peer digital certificates to be cached.

Range: 64 through 4,294,967,295 peer certificates

Default: 1024 peer certificates

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

Related Documentation
- *Configuring Digital Certificates for an ES PIC*

path-length

Syntax path-length *certificate-path-length*;

Hierarchy Level [edit security certificates]

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 (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificate path length.

Options ***certificate-path-length***—Digital certificate path length.

Range: 2 through 15 certificates

Default: 15 certificates

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

Related Documentation
- *Configuring Digital Certificates for an ES PIC*

secret

Syntax secret *secret-data*;

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify a password in encrypted text or plain text format. The secret password always appears in encrypted format.

Options ***secret-data***—Password to use; it can include spaces if the character string is enclosed in quotation marks.

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

Related Documentation

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

security

Syntax

```
security {
  authentication-key-chains {
    key-chain key-chain-name {
      key key {
        secret secret-data;
        start-time yyyy-mm-dd.hh:mm:ss;
      }
    }
  certificates {
    cache-size bytes;
    cache-timeout-negative seconds;
    certification-authority ca-profile-name {
      ca-name ca-identity;
      crl file-name;
      encoding (binary | pem);
      enrollment-url url-name;
      file certificate-filename;
      ldap-url url-name;
    }
    enrollment-retry attempts;
    local certificate-filename {
      certificate-key-string;
      load-key-file key-file-name;
    }
    maximum-certificates number;
    path-length certificate-path-length;
  }
  ssh-known-hosts {
    host {
      fetch-from-server host-name;
      load-key-file file-name;
    }
  }
  traceoptions {
    file filename <files number> <size size>;
    flag flag;
    level level;
    no-remote-trace
  }
}
```

Hierarchy Level [edit]

Release Information 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 Configure security services. Most of the configuration statements do not have default values. If you do not specify an identifier for a statement that does not have a default value, you cannot commit the configuration.

Required Privilege Level

Related Documentation

ssh-known-hosts

Syntax

```
ssh-known-hosts {
  host host-name {
    fetch-from-server host-name;
    load-key-file file-name;
  }
}
```

Hierarchy Level [edit security ssh-known-hosts]

Release Information 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 Configure SSH support for known hosts and for administering SSH host key updates.

Options **host *host-name***—Hostname of the SSH known host entry. This option has the following suboptions:

- **fetch-from-server *host-name***—Retrieve SSH public host key information from a specified server.
- **load-key-file *filename***—Import SSH host key information from the **/var/tmp/ssh-known-hosts** file.

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

Related Documentation

- *Understanding Security Features on the QFabric System*
- *Configuring SSH Host Keys for Secure Copying of Data*

start-time (Authentication Key Transmission)

Syntax start-time (now | *yyyy-mm-dd.hh:mm:ss*);

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify a start time for key transmission. You do not need to specify an end time for the key. If a new key is present with a new start time, the keychain rolls over to the new one. The start time must be unique within the keychain.

Options **now**—Start time as the current year, month, day, hour, minute, and second.

***day*days**—Start time as the specified number of days after the current day. For example, if the current day is the 12th and you configure **start-time 2day**, the start time will be on the 14th, exactly two days after the configuration is entered.

***hour*hours**—Start time as the specified number of hours after the current hour. For example, if the current hour is 9:00 and you configure **start-time 3hour**, the start time will be in 12:00, exactly three hours after the configuration is entered.

***minute*minutes**—Start time as the specified number of minutes after the current minute. For example, if the current minute is 27 minutes after the hour and you configure **start-time 5min**, the start time will be in 32 minutes after the hour, exactly five minutes after the configuration is entered.

***month*months**—Start time as the specified number of months after the current month. For example, if the current month is March and you configure **start-time 4month**, the start time will be in July, exactly four months after the configuration is entered.

***second*seconds**—Start time as the specified number of seconds after the current second. For example, if the current second is 10:20:40 and you configure **start-time 10seconds**, the start time will be 10:20:50, exactly 10 seconds after the configuration is entered.

***year*years**—Start time as the specified number of years after the current year. For example, if the current year is 2011 and you configure **start-time 1year**, the start time will be in 2012, exactly one year after the configuration is entered.

yyyy–mm-dd.hh:mm:ss—Start time in UTC (Coordinated Universal Time). The start time must be unique within the keychain.

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

Related Documentation

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

traceoptions

Syntax

```
traceoptions {
  file filename <files number> <size size>;
  flag all;
  flag certificates;
  flag database;
  flag general;
  flag ike;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
  level
  no-remote-trace
}
```

Hierarchy Level

[edit security],
[edit services ipsec-vpn]

Trace options can be configured at either the **[edit security]** or the **[edit services ipsec-vpn]** hierarchy level, but not at both levels.

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

Configure security trace options.

To specify more than one trace option, include multiple **flag** statements. Trace option output is recorded in the **/var/log/kmd** file.

NOTE: The **traceoptions**statement is not supported on QFabric systems.

Options

files ***number***—(Optional) Maximum number of trace files. When a trace file (for example, **kmd**) reaches its maximum size, it is renamed **kmd.0**, then **kmd.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the **size** option.

Range: 2 through 1000 files

Default: 0 files

size ***size***—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, **kmd**) reaches this size, it is renamed, **kmd.0**, then **kmd.1** and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Default: 1024 KB

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 Level

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

Related Documentation

- *Configuring Tracing Operations for Security Services*