JUNIPER NETWORKS

Junos® OS

DTCP-Initiated Subscriber Secure Policy and Traffic Mirroring Feature Guide

Release
14.1

Published: 2014-04-25

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

Junos® OS DTCP-Initiated Subscriber Secure Policy and Traffic Mirroring Feature Guide
14.1

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:

- MX Series

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

Table 1 on page xiii 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 xiii 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 send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/

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

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Secure Policy Traffic Mirroring in Subscriber Access Networks

Subscriber Secure Policy Overview

Subscriber secure policy enables you to mirror traffic on a per-subscriber basis. You can mirror the content of subscriber traffic as well as monitor events related to the subscriber session that is being mirrored.

Subscriber secure policy mirroring can be based on information provided by either RADIUS or Dynamic Tasking Control Protocol (DTCP), and can mirror both IPv4 and IPv6 traffic. Configuration of subscriber secure policy mirroring is independent of the actual mirroring session—you can configure the mirroring parameters at any time. Also, you can use a single RADIUS or DTCP server to provision mirroring operations on multiple routers in a service provider's network. To provide security, the ability to configure, access, and view the subscriber secure policy components and configuration is restricted to authorized users.

After subscriber secure policy is triggered, both the subscriber incoming and outgoing traffic are mirrored. The original traffic is sent to its intended destination and the mirrored traffic is sent to a mediation device for analysis. The actual mirroring operation is transparent to subscribers whose traffic is being mirrored. A special UDP/IP header is prepended to each mirrored packet sent to the mediation device. The mediation device uses the header to differentiate multiple mirrored streams that arrive from different sources.

Subscriber Secure Policy for Subscribers on VLANs

Interface-based subscriber secure policy is supported on dynamic, authenticated VLAN interfaces and VLAN demux interfaces. When you enable subscriber secure policy for these interfaces, traffic for all configured families (inet, inet6) including Layer 2 and Layer 3 control traffic is mirrored. The mirrored packets include Layer 2 encapsulations.

Traffic Filtering For DTCP-Initiated Subscriber Secure Policy Mirrored Traffic

You can filter mirrored traffic before it is sent to a mediation device. With this feature, service providers can reduce the volume of traffic sent to a mediation device. For some types of traffic, such as IPTV or video on demand, you do not need to mirror the entire content of the traffic because the content may already be known or controlled by the service provider.

Mirroring-Related Event Reporting

Subscriber secure policy also supports the use of SNMPv3 traps to report events related to the mirroring operation to an external device. Types of information sent in traps include identifying information for subscribers, such as username or IP address, and subscriber session events, such as login or logout events or mirroring session activation or deactivation. The traps map to messages defined in the *Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American National Standard for Telecommunications*.

Related Documentation

- *RADIUS-Initiated Subscriber Secure Policy Overview*
- DTCP-Initiated Subscriber Secure Policy Overview on page 5
- Intercept-Related Events Transmitted to the Mediation Device on page 85

Subscriber Secure Policy Licensing Requirements

To enable and use subscriber secure policy, you must install and properly configure the Subscriber Secure Policy license.

Related Documentation

- *Junos OS Feature Licenses*
- *Junos OS Feature License Keys*
- *License Enforcement*

CHAPTER 2

DTCP-Initiated Secure Policy Traffic Mirroring

DTCP-Initiated Subscriber Secure Policy Overview

Dynamic Tasking Control Protocol (DTCP)-initiated mirroring creates secure policies to mirror traffic for the subscriber based on DTCP messages. The attributes in a DTCP ADD message trigger the router to start mirroring traffic and specify the interface on which the mirroring takes place. The mirroring operations can be initiated by DTCP messages as follows:

- Subscriber login—Mirroring starts on the specified interface when the subscriber logs in. The DTCP ADD message must be sent to the router before the subscriber logs in.
- In-session—Mirroring starts for all subscribers that match the trigger supplied in the DTCP ADD message when the router receives a DTCP ADD message.

Related Documentation

- Subscriber Secure Policy Traffic Mirroring Architecture Using DTCP on page 5
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 21

Subscriber Secure Policy Traffic Mirroring Architecture Using DTCP

Figure 1 on page 6 shows the architecture of the DTCP-initiated subscriber secure policy mirroring environment.

Figure 1: DTCP-Initiated Subscriber Secure Policy Architecture

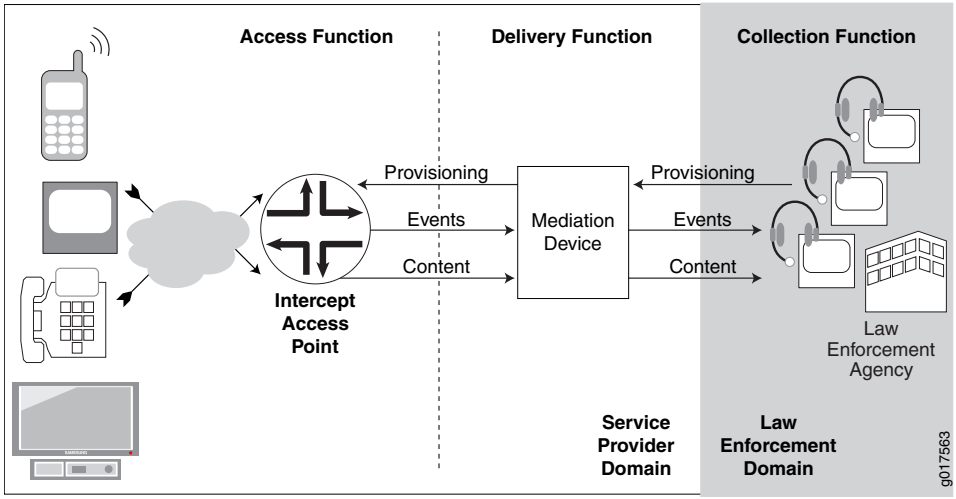


Table 3 on page 6 describes the functions and components of a DTCP-initiated subscriber secure policy traffic mirroring environment.

Table 3: DTCP-Initiated Subscriber Secure Policy Functions and Components

Function or Component	Description
Collection function	The collection function is responsible for collecting intercepted content and identifying information from the delivery function. The collection function is the responsibility of the law-enforcement agency (LEA).
Delivery function	The delivery function delivers information that it receives from the access function to the collection function. The delivery function is performed by the mediation device.
Access function	The access function has access to the intercept target's traffic content and intercept-related events. It is responsible for collecting this information and sending it to the delivery function. The access function is performed by intercept access points (IAPs).
Events	Intercept-related events, such as login or logout events or mirroring session activation or deactivation. The router sends the events to the mediation device in SNMP traps.
LEA	Law enforcement agency. The LEA provides intercept targets to the service provider who provisions the mediation device.

Table 3: DTCP-Initiated Subscriber Secure Policy Functions and Components *(continued)*

Function or Component	Description
Mediation device	The mediation device receives provisioning information from the LEA, and it uses the information to send provisioning information to the IAP (the router). The mediation device also receives intercept-related events and intercepted content from the router, and delivers the events and content to the LEA.
IAP	Intercept access point. In a subscriber access network the Juniper Networks router is the IAP. Using subscriber secure policies, the IAP intercepts traffic to and from the subscriber whose traffic is being mirrored. It encapsulates the intercepted content in a packet header and delivers it to the mediation device, while also sending the traffic to the intended destination. The IAP also sends intercept-related events to the mediation device using SNMP traps.

Related Documentation

- DTCP-Initiated Subscriber Secure Policy Overview on page 5
- DTCP-Initiated Traffic Mirroring Interfaces on page 7
- DTCP-Initiated Traffic Mirroring Process on page 9

DTCP-Initiated Traffic Mirroring Interfaces

Figure 2 on page 7 shows the interfaces involved in DTCP-initiated secure subscriber policy traffic mirroring.

Figure 2: DTCP-Initiated Traffic Mirroring Interfaces

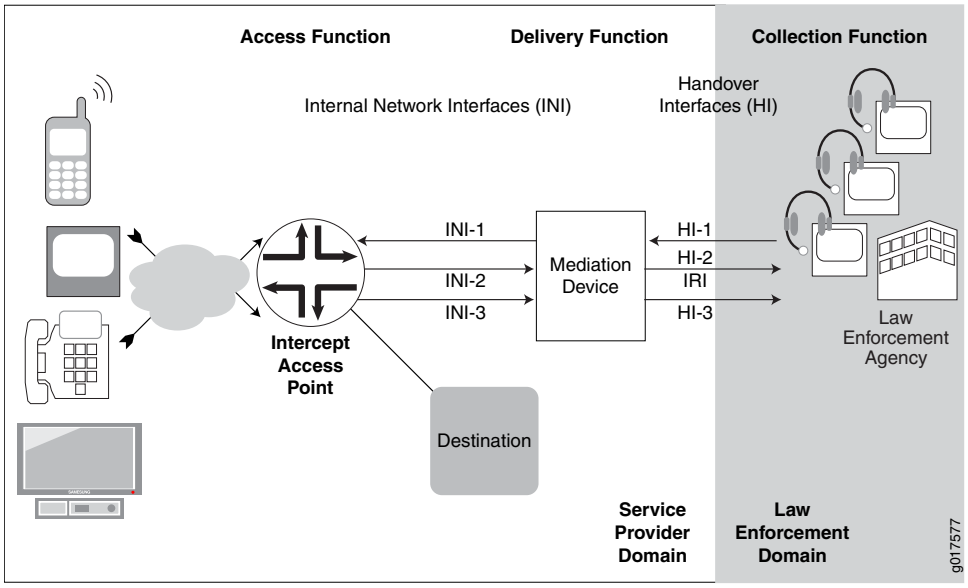


Table 4 on page 8 describes the interfaces involved in DTCP-initiated secure subscriber policy traffic mirroring.

Table 4: DTCP-Initiated Traffic Mirroring Interfaces

Interface	Description
HI-1	Handover Interface 1—Administrative interface between the LEA and the service provider mediation device. The LEA sends provisioning information to the mediation device on this interface.
HI-2	Handover Interface 2—Intercept-related information interface between the LEA and the mediation device that is used to deliver intercept-related events to the LEA. These events can be subscriber session events such as login, logout, and authentication.
HI-3	Handover Interface 3—Intercepted content Interface between the mediation device and LEA that is used to deliver intercepted content to the LEA.
INI-1	Internal network Interface 1—Interface used to send DTCP messages containing intercept provisioning information from the mediation device to the router.
INI-2	Internal network interface 2—Interface used to send intercept-related events from the router to the mediation device. This information is sent in SNMP traps.
INI-3	Internal network interface 3—Interface used to send intercepted content from the router to the mediation device.

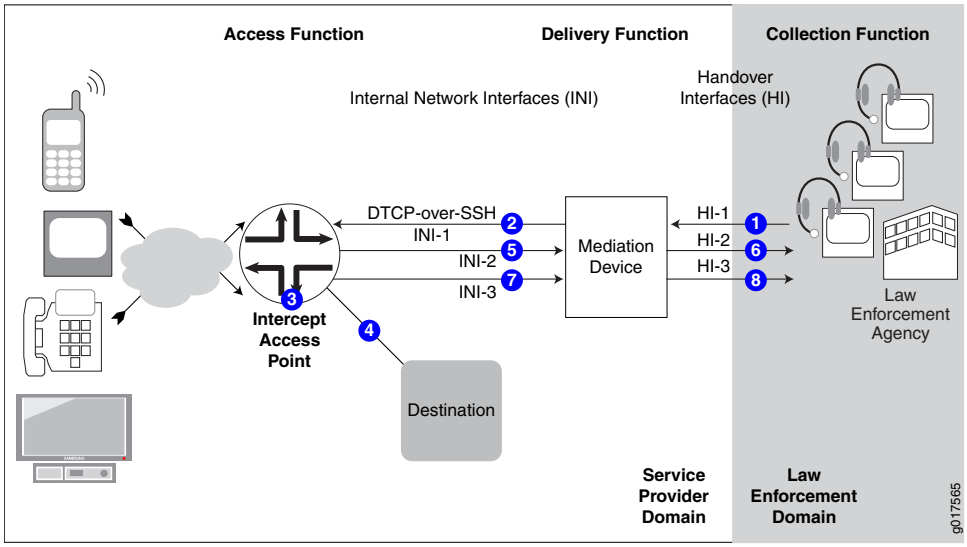
Related Documentation

- Subscriber Secure Policy Traffic Mirroring Architecture Using DTCP on page 5
- DTCP-Initiated Traffic Mirroring Process on page 9

DTCP-Initiated Traffic Mirroring Process

Figure 3 on page 9 shows the process for a DTCP-initiated subscriber mirroring operation.

Figure 3: DTCP-Initiated Subscriber Secure Policy Model



1—The LEA sends provisioning information for a subscriber whose traffic is to be mirrored over the HI-1 interface to the mediation device.	5—As intercept-related events occur, the IAP sends the events in SNMP traps over the INI-2 interface to the mediation device.
2—The mediation device sends a DTCP ADD message that contains provisioning information over the INI-1 interface to the IAP (the router).	6—The mediation device provides the intercept-related events over the HI-2 interface to the LEA.
3—The IAP creates a subscriber secure policy based on information in the DTCP ADD message. If the IAP receives the DTCP ADD before the subscriber logs in, mirroring begins when the subscriber logs in. If the router receives the DTCP ADD after the subscriber logs in, mirroring begins when the ADD message is received.	7—The IAP sends the mirrored content to the mediation device over the INI-3 interface.
4—The IAP sends the original subscriber traffic to its intended destination.	8—The mediation device sends mirrored content over the HI-3 interface to the LEA.

Related Documentation

- Subscriber Secure Policy Traffic Mirroring Architecture Using DTCP on page 5
- DTCP-Initiated Traffic Mirroring Interfaces on page 7
- DTCP Messages Used for Subscriber Secure Policy on page 10
- DTCP Traffic Mirroring Triggers on page 11

Subscriber Secure Policy Support for IPv4 Multicast Traffic

IP multicast traffic is used for applications such as audio or video streaming, IPTV, video conferencing, or online gaming. Multicast traffic is sent to multiple subscribers who have joined a multicast group.

Secure subscriber policy allows for the mirroring of IPv4 multicast traffic sent to a specific subscriber. If multiple subscribers whose traffic requires mirroring join the same multicast session, the subscriber secure policy feature mirrors each subscriber's traffic and forwards it separately to the mediation device with the proper prepended header.

Mirroring of multicast traffic is supported only for subscribers in the default logical system.

You can enable and disable the mirroring of multicast traffic on a per-chassis basis. You cannot enable or disable it on a per-subscriber basis.

Triggering the Mirroring of IPv4 Multicast Traffic

Multicast traffic being sent towards a subscriber does not contain much of the identifying information used to trigger mirroring of a subscriber's unicast traffic. For example, the multicast packet contains the multicast group address in the destination address of the packet instead of the subscriber's IP address. It also does not contain the user name or MAC address of the subscriber, and does not include information obtained by RADIUS or DHCP. Therefore, methods of identifying multicast traffic that is received by a subscriber are not the same as methods of identifying a subscriber's unicast traffic or multicast traffic that is sent by a subscriber.

To join a multicast group, a subscriber sends an IGMP join request, and it receives a reply. The reply contains the multicast groups to which the subscriber is registered. Triggering the mirroring of multicast traffic is based on the sending of the IGMP join request and the information in the IGMP reply. If the subscriber's unicast traffic is already being mirrored either through DTCP-initiated or RADIUS-initiated traffic mirroring, and the subscriber sends an IGMP join request, mirroring of multicast traffic sent to the subscriber is initiated. The traffic being mirrored is based on the groups contained in the IGMP reply.

Related Documentation

- Enabling Subscriber Secure Policy Mirroring for IPv4 Multicast Traffic on page 29

DTCP Messages Used for Subscriber Secure Policy

You can use DTCP to provision traffic mirroring on the router by sending DTCP messages from the mediation device to the router.

There are three types of DTCP messages:

- ADD—Triggers mirroring of subscriber secure policy sessions. You include an attribute that triggers the router to begin mirroring a subscriber session. You can also include attributes that identify where to send the mirrored session data and how to uniquely identify traffic when simultaneous intercepts are active. The ADD message also provides

instructions to populate fields in the encapsulation header for packets sent to the mediation device.

- LIST—Requests information about sessions that are currently being mirrored. This information is returned in a LIST response.
- DELETE—Removes a subscriber mirroring trigger or can be used to disable all mirroring.

Related Documentation

- DTCP-Initiated Traffic Mirroring Process on page 9
- DTCP Traffic Mirroring Triggers on page 11
- ADD DTCP on page 32
- DELETE DTCP on page 35
- LIST DTCP on page 39

DTCP Traffic Mirroring Triggers

Table 5 on page 11 lists the DTCP attributes that you can use in DTCP ADD messages to trigger traffic mirroring.

Table 5: DTCP Mirroring Triggers for Use in ADD Messages

Attribute Name	DTCP Message Semantic	Description
Account Session ID	X-Act-Sess-Id	Trigger that is based on the text string of the Account Session ID associated with the subscriber session. If the subscriber logs out, the intercept terminates. We recommend that you use other triggers to ensure that all sessions for a subscriber are intercepted.
Calling Station ID	X-Call-Sta-Id	Trigger that is based on the text string of the Calling Station ID associated with the subscriber. If the subscriber is not logged on, the policy is applied at any current or subsequent subscriber log in.
Drop Policy Name	X-Drop-Policy	Trigger that is based on the name of the configured lawful intercept policy.

Table 5: DTCP Mirroring Triggers for Use in ADD Messages *(continued)*

Attribute Name	DTCP Message Semantic	Description
IP Address	X-IP-Addr	Trigger for the IPv4 address that is associated with a subscriber. If you use the IP Address trigger, and the subscriber is not using the default logical system, you must include the Logical System attribute in your DTCP message. If the subscriber is not using the default routing instance, you must include the Routing Instance attribute in your DTCP message.
Interface Identifier	X-Interface-Id	Trigger for subscribers that are configured to use a specific router interface. All subscribers that use the interface have their traffic mirrored. Add this attribute as a text string that identifies the physical interface; for example, **ge-0/0/0.1** or **demux0.107472834**.
NAS Port ID	X-NAS-Port-Id	Trigger that is based on the NAS port ID of the subscriber.
Remote Circuit ID	X-RM-Circuit-Id	For DHCP subscribers, trigger that is used with the Remote Agent ID to specify the DHCP option 82 that is associated with this session to completely specify a trigger. For PPPoE subscribers, agent circuit ID (ACI) in the PPPoE Intermediate Agent (PPPoE IA) tag.
Remote Agent ID	X-RM-Agent-Id	For DHCP subscribers, trigger that is used with the Remote Circuit ID to specify the session or by itself to completely specify the trigger. For PPPoE subscribers, agent remote identifier (ARI) in the PPPoE Intermediate Agent (PPPoE IA) tag.

Table 5: DTCP Mirroring Triggers for Use in ADD Messages *(continued)*

Attribute Name	DTCP Message Semantic	Description
Logical System	X-Logical-System	Trigger attribute that you can use with the IP Address or Subscriber User Name triggers. It is ignored for other triggers. The value **default** is used if no logical system exists for the subscriber.
Routing Instance	X-Router-Instance	Trigger attribute that you can use with the IP Address or Subscriber User Name triggers. It is ignored for other triggers. The value **default** is used if no routing instance exists for the subscriber.
Subscriber User Name	X-UserName	Trigger based on a subscriber username. If you use the Subscriber User Name trigger, and the subscriber is not using the default logical system, you must include the Logical System attribute in your DTCP message. If the subscriber is not using the default routing instance, you must include the Routing Instance attribute in your DTCP message.

Triggering Subscriber Secure Policy for Subscribers on Dynamic Authenticated VLANs

BEST PRACTICE: When you have DHCPv4/DHCPv6 subscribers over VLANs, two sessions are created for each subscriber—one for the Layer 2 VLAN, and one for DHCP. In this case do not use a trigger, such as Remote Circuit ID (ACI), that applies to both the VLAN and the DHCP sessions. If the DHCP and VLAN sessions match the same trigger, the DHCP subscriber login fails and subscriber secure policy is not triggered. You need to select a traffic mirroring trigger that matches only one of these sessions.

Order in Which Trigger Attributes Are Processed

If a subscriber matches more than one of the DTCP mirroring triggers, the router processes mirroring triggers in ADD messages in the following order:

1. Account Session ID
2. Calling Station ID
3. IP Address
4. Interface Identifier
5. NAS Port ID
6. Remote Agent ID
7. Subscriber User Name
8. Drop Policy Name

Related Documentation

- Packet Header for Mirrored Traffic Sent to Mediation Device on page 15
- **ADD DTCP on page 32**
- **DELETE DTCP on page 35**
- **LIST DTCP on page 39**
- Example: Using DTCP Messages to Trigger, Verify, and Disable Traffic Mirroring for Subscribers on page 41

Packet Header for Mirrored Traffic Sent to Mediation Device

When the router sends mirrored traffic to the mediation device, it encapsulates the mirrored payload in a packet header before it sends the mirrored traffic to the mediation device.

Figure 4 on page 15 is the mirrored packet header that the router sends to the mediation device.

Figure 4: Mirrored Packet Header

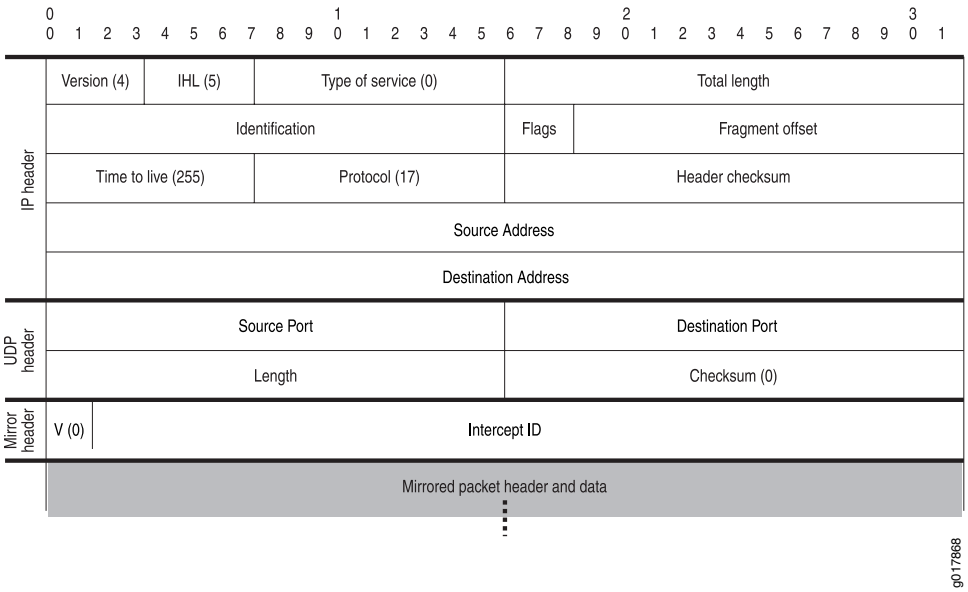


Table 6 on page 15 describes the fields in the packet header of mirrored packets.

Table 6: Mirrored Packet Header and Payload Field Descriptions

Field	Value	Length (Bits)
IP Header		
Version	4	4
IHL	5	4
Type of Service	0	8
Total Length	Dynamically computed	16
Identification	Dynamically computed	16
Flags	Dynamically computed	3
Fragment Offset	Dynamically computed	13

Table 6: Mirrored Packet Header and Payload Field Descriptions *(continued)*

Field	Value	Length (Bits)
Time to Live	255	8
Protocol	17	8
Header Checksum	Dynamically computed	16
Source Address	IP address of the router interface that sends mirrored traffic to the mediation device	32
Destination Address	IP address of the mediation device to which mirrored traffic is forwarded. This value is taken from the X-JTap-Cdest-Dest-Address attribute that is sent to the router in the DTCP ADD command.	32
UDP Header		
Source Port	UDP port number on the router from which mirrored traffic is sent to the mediation device	16
Destination Port	UDP port on the mediation device to which mirrored traffic is forwarded. This value is taken from the X-JTap-Cdest-Dest-Port attribute that is sent to the router in the DTCP ADD command.	16
Length	Dynamically computed	16
Checksum	0	16
Mirror Header		
V (mirror header value)	0	2
Intercept ID	Value of the X-MD-Intercept-Id that is sent to the router in the DTCP ADD command.	30

Related Documentation

- DTCP-Initiated Subscriber Secure Policy Overview on page 5
- **ADD DTCP on page 32**
- Example: Using DTCP Messages to Trigger, Verify, and Disable Traffic Mirroring for Subscribers on page 41

Subscriber Secure Policy and L2TP LNS Subscribers

Dynamic Tasking Control Protocol (DTCP)-initiated and RADIUS-initiated per-subscriber traffic mirroring can be applied to Point-to-Point Protocol (PPP) subscribers whose traffic is tunneled with Layer 2 Tunneling Protocol (L2TP). At the L2TP network server (LNS), both subscriber ingress traffic (from the L2TP access concentrator, or LAC, to the LNS) and subscriber egress traffic (from the LNS to the LAC) are mirrored at the inline services (si) interface corresponding to the subscriber. Ingress traffic is mirrored after decapsulation of L2TP, HDLC, and PPP headers. The egress traffic is mirrored before the IP datagram is encapsulated. The mirrored traffic contains only the IP datagram belonging to the subscriber.

Related Documentation

- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*
- *RADIUS Attributes Used for Subscriber Secure Policy*

PART 2

Configuration

CHAPTER 3

Configuration Overview and Guidelines

Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview

Before you configure subscriber secure policy traffic mirroring, note the following:

- Subscriber secure policy mirroring runs on the radius-flow-tap service infrastructure. To configure the subscriber secure policy service, you need the same privileges that are required to configure the radius-flow-tap service.
- The subscriber secure policy feature requires some system resources while mirroring, encrypting, and sending traffic to the mediation device. For example, you might elect to use a 10-Gigabit Ethernet interface for the tunnel and mediation device if you expect the amount of traffic you plan to mirror to approach 1 Gbps of actual user data.

To configure DTCP-initiated subscriber secure policy service:

1. Configure tunnel interfaces that are used to send mirrored content to the mediation device.

   See "Configuring Tunnel Interfaces for Subscriber Secure Policy Mirroring" on page 23.

2. Configure the radius-flow-tap service support for secure subscriber policy. This support includes configuring the tunnels and optional forwarding-class information that the subscriber secure policy service uses to send mirrored traffic to the content destination device.

   See "Configuring Support for Subscriber Secure Policy Mirroring" on page 24.

3. Configure the mediation device as a user on the router. This user account allows the router to receive DTCP messages from the mediation device.

   See "Configuring the Mediation Device as a User on the Router" on page 25.

4. Configure the mediation device to provision traffic mirroring on the router.

   See "Configuring the Mediation Device to Provision Traffic Mirroring" on page 29.

5. Configure a DTCP-over-SSH connection to the mediation device.

   See "Configuring a DTCP-over-SSH Connection to the Mediation Device" on page 26.

6. (Optional) Enable mirroring of IPv4 multicast traffic on the router.

   See "Enabling Subscriber Secure Policy Mirroring for IPv4 Multicast Traffic" on page 29

7. Configure SNMPv3 trap support to report mirroring information to an external device.

   See "Configuring SNMPv3 Traps for Subscriber Secure Policy Mirroring" on page 87.

You can terminate an active subscriber mirroring session at any time.

See "Terminating DTCP-Initiated Subscriber Traffic Mirroring Sessions" on page 89.

Related Documentation

- DTCP-Initiated Subscriber Secure Policy Overview on page 5
- Intercept-Related Events Transmitted to the Mediation Device on page 85

Guidelines for Configuring Subscriber Secure Policy Mirroring

The subscriber secure policy service uses the radius-flow-tap service infrastructure.

When configuring subscriber secure policy mirroring, consider the following guidelines regarding the relationship between subscriber secure policy service and the radius-flow-tap service:

- The radius-flow-tap service **[edit services radius-flow-tap]** and the flow-tap service **[edit services flow-tap]** cannot run simultaneously on the router. Therefore, flow-tap and subscriber secure policy mirroring cannot run simultaneously on the same router.
- You can configure one instance of the radius-flow-tap service on the router. Subscriber secure policy RADIUS-initiated mirroring and DTCP-initiated mirroring use the radius-flow-tap service.
- If you delete the radius-flow-tap service all subscriber secure policy mirroring stops.

Related Documentation

- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 21
- Configuring Support for Subscriber Secure Policy Mirroring on page 24

CHAPTER 4

Configuration Tasks

Configuring Tunnel Interfaces for Subscriber Secure Policy Mirroring

The router, acting as the IAP, uses tunnel interfaces (vt interfaces) to send mirrored traffic to the mediation device. The IAP equally distributes the mirrored traffic across the available tunnel interfaces.

Because the MX Series 3D Universal Edge Routers do not support Tunnel Services PICs, you create a pool tunnel interfaces on MX Series routers at the **[edit chassis]** hierarchy level.

You can configure up to 2048 mirrored subscriber sessions per chassis.

To configure a pool of tunnel interfaces for use by subscriber secure policy mirroring:

1. Access the chassis configuration, and specify the slot number of the DPC, MPC, or MIC.
   - On the MX80 router, the range is 0 through 1.
   - On other MX Series routers, if two System Control Boards (SCBs), are installed, the range is 0 through 11. If three SCBs are installed, the range is 0 through 5 and 7 through 11.

     ```
     [edit chassis]
     user@host# edit fpc 1
     ```
2. Configure the PIC number of the FPC.

- On MX80 routers, if the FPC is 0, the PIC number can only be 0. If the FPC is 1, the PIC range is 0 through 3.
- For all other MX Series routers, the range is 0 through 3.

```
[edit chassis fpc 1]
user@host# edit pic 1
```

3. Specify that the FPC and PIC are to be used for tunnel interfaces.

```
[edit chassis fpc 1 pic 1]
user@host# edit tunnel-services
```

4. Specify the amount of bandwidth to reserve for tunnel traffic on each Packet Forwarding Engine.

   - 1g indicates that 1 Gbps of bandwidth is reserved for tunnel traffic.
   - 10g indicates that 10 Gbps of bandwidth is reserved for tunnel traffic.

   If you specify a bandwidth that is not compatible, tunnel services are not activated. For example, you cannot specify a bandwidth of 1 Gbps for a Packet Forwarding Engine on a 10-Gigabit Ethernet 4-port DPC.

```
[edit chassis fpc 1 pic 1 tunnel-services]
user@host#
user@host# set bandwidth 1g
```

5. Configure the tunnel interfaces, including the family.

   To configure subscriber secure policy mirroring for IPv6 traffic, configure the tunnel interfaces for both the **inet** and **inet6** families.

```
[edit interfaces]
user@host# set vt-1/1/0 unit 0 family inet
user@host# set vt-1/1/0 unit 0 family inet6
```

Related Documentation

- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 21
- Subscriber Secure Policy and L2TP LNS Subscribers on page 17

Configuring Support for Subscriber Secure Policy Mirroring

Subscriber secure policy runs on the radius-flow-tap service. This topic describes the steps to configure radius-flow-tap support for RADIUS-initiated and DTCP-initiated subscriber secure policy mirroring.

To configure the radius-flow-tap service to support subscriber secure policy mirroring:

1. Configure the flow-tap service used for subscriber secure policy mirroring.

```
[edit services]
user@host# edit radius-flow-tap
```

2. Assign the tunnel interfaces that the radius-flow-tap service uses.

```
[edit services radius-flow-tap]
user@host# set interfaces vt-1/1/0.0
```

If a currently used tunnel interface is deleted from the pool of interfaces, the active mirroring sessions are redistributed from the deleted interface to other tunnel interfaces in the pool. Also, when a new tunnel interface is added into the pool, the service adds the new interface to the list of interfaces available for new mirroring sessions or for existing sessions transferred from a failed interface.

3. Specify the source IP address that the radius-flow-tap service uses for mirroring. This address is used in the IP header prepended to mirrored packets that are sent to the content destination device.

   ```
   [edit services radius-flow-tap]
   user@host# set source-ipv4-address ipv4-address
   ```

4. (Optional) Specify the forwarding class that is applied to the mirrored packets sent to the mediation device.

   If you do not specify a forwarding class, mirrored packets inherit the forwarding class from the original packet (which is the forwarding class set by default classification that CoS applies to the packet on the ingress interface).

   ```
   [edit services radius-flow-tap]
   user@host# set forwarding-class class-name
   ```

5. (Optional) Specify the lawful intercept policy that determines what traffic, if any, is not sent to the mediation device.

   You can add or change a lawful intercept policy any time, but a changed policy does not apply to a currently enabled policy. To change a policy, add a policy with a new name, use DTCP DISABLE to turn off the current policy, and use DTCP ENABLE to point to the new policy name.

   ```
   [edit services radius-flow-tap]
   user@host# set policy policy-name
   ```

Related Documentation

- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 21
- Guidelines for Configuring Subscriber Secure Policy Mirroring on page 22

Configuring the Mediation Device as a User on the Router

In order for the router to receive DTCP messages from the mediation device, you need to configure the mediation device as a user on the router. To do so, create a login class that provides flow-tap operation permission and then create a login account that uses the login class.

To configure the mediation device as a user on the router:

1. Create the login class and configure **flow-tap-operation** permissions for the class.

a. Specify that you want to configure login properties.

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

b. Create and name the class.

```
[edit system login]
user@host# edit class class-name
```

c. Configure the **flow-tap-operation** permission for the class.

```
[edit system login class class-name]
user@host# set permissions flow-tap-operation
```

2. Create the user login account for the mediation device.

a. Create the user account.

```
[edit system login]
user@host# edit user username
```

b. Configure the user ID.

```
[edit system login user username]
user@host# set uid uid-value
```

c. Configure the class for the user account.

```
[edit system login user username]
user@host# set class class-name
```

d. Configure the authentication for the user account.

```
[edit system login user username]
user@host# set authentication encrypted-password password
```

Configuring a DTCP-over-SSH Connection to the Mediation Device

DTCP-initiated subscriber secure policy requires a DTCP-over-SSH connection for the flow-tap service. This connection is used to send provisioning information from the mediation device to the router.

To enable the DTCP-over-SSH flow-tap service to support subscriber secure policy mirroring:

1. Access the **flow-tap-dtcp** service.

```
[edit system services]
user@host# edit flow-tap-dtcp
```

2. Enable SSH support for DTCP.

```
[edit system services flow-tap-dtcp]
user@host# set ssh
```

3. (Optional) Configure maximum number of established connections allowed for the DTCP service.

```
[edit system services flow-tap-service ssh]
user@host# set connection-limit limit
```

4. (Optional) Configure the maximum number of connection attempts allowed per minute for DTCP.

```
[edit system services flow-tap-service ssh]
user@host# set rate-limit limit
```

Related Documentation

- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 21

Example: Configuring Traffic That Is Mirrored Using DTCP-Initiated Subscriber Secure Policy

This example shows how to configure traffic that is mirrored using DTCP-initiated subscriber secure policy.

Requirements

- Juniper Networks MX Series routers.
- Junos OS Release 12.3R1 or later.

Overview

This example drops all video on demand TCP traffic from subnet 10.0.0.0/8 to any subscriber on which the policy named vod is enabled.

To configure traffic mirroring using DTCP-initiated subscriber secure policy:

1. Create a policy.
2. Set up the policy to filter IPv4 or IPv6 traffic by source or destination address, or port, protocol, or DSCP value.
3. Apply the policy using the DTCP attribute X-Drop-Policy.
4. Use the X-Drop-Policy with the ADD DTCP command to begin filtering traffic when mirroring is triggered.

NOTE: To begin filtering traffic that is currently being mirrored, use the X-Drop-Policy attribute with the new ENABLE DTCP command. To stop filtering traffic that is currently being mirrored, use the X-Drop-Policy attribute with the new DISABLE DTCP command.

Configuration

Step-by-Step Procedure

To configure filtering mirrored traffic before it is sent to a mediation device:

1. Specify that you want to configure radius-flow-tap.

   ```
   [edit services]
   user@host# edit radius-flow-tap
   ```

2. Specify that you want to configure a video on demand policy.

   ```
   [edit services radius-flow-tap]
   user@host# edit policy vod
   ```

3. Specify inet as the family that you want to use.

   ```
   [edit services radius-flow-tap vod]
   user@host# edit inet
   ```

4. Specify t1 as the term name for the IPv4 drop-policy.

   ```
   [edit services radius-flow-tap vod inet]
   user@host# edit drop-policy t1
   ```

5. Specify the source address for the drop-policy.

   ```
   [edit services radius-flow-tap vod inet drop-policy t1]
   user@host# edit source-address 10.0.0.0/8
   ```

6. Specify the match criteria that you want to use.

   ```
   [edit services radius-flow-tap vod inet drop-policy t1]
   user@host# set protocol tcp
   ```

Results

From configuration mode, confirm your configuration by entering the **show services** command. If the output does not display the intended configuration, repeat the instructions in this example to correct it.

```
[edit services radius-flow-tap policy]
vod {
  inet {
    drop-policy t1 {
      from{
        source-address {
          10.0.0.0/8;
        }
        protocol tcp;
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- Subscriber Secure Policy Overview on page 3
- Configuring Support for Subscriber Secure Policy Mirroring on page 24
- DTCP Traffic Mirroring Triggers on page 11

Configuring the Mediation Device to Provision Traffic Mirroring

To set up the mediation device to provision traffic mirroring on the router, use the following DTCP messages:

- To configure traffic-mirroring triggers, use the ADD DTCP message.
- To remove an existing traffic-mirroring trigger, use the DELETE DTCP message.
- To show existing traffic-mirroring triggers, use the LIST DTCP message.

For an example of how to use the DTCP messages, see "Example: Using DTCP Messages to Trigger, Verify, and Disable Traffic Mirroring for Subscribers" on page 41.

Related Documentation

- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 21

Enabling Subscriber Secure Policy Mirroring for IPv4 Multicast Traffic

This topic describes the steps to enable subscriber secure policy mirroring of IPv4 multicast traffic. You can enable and disable IPv4 multicast intercept on a per chassis basis.

To configure the radius-flow-tap service to support subscriber secure policy mirroring:

1. Configure the flow-tap service used for subscriber secure policy mirroring.

   ```
   [edit services]
   user@host# edit radius-flow-tap
   ```

2. Enable the interception of multicast traffic.

   ```
   [edit services radius-flow-tap]
   user@host# set multicast-interception
   ```

Related Documentation

- Subscriber Secure Policy Support for IPv4 Multicast Traffic on page 10
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 21

CHAPTER 5

DTCP Messages Sent From Mediation Device

ADD DTCP

Syntax

ADD DTCP/0.7
Csource-ID: *user-name*
Cdest-ID: *variable*
Priority: *priority-number*
X-Drop-Policy: *policy-name*
X-JTap-Cdest-Dest-Address: *ipv4-address*
X-JTap-Cdest-Dest-Port: *udp-port*
X-JTap-Cdest-Source-Address: *ipv4-address*
X-JTap-Cdest-Source-Port: *port-number*
X-JTap-Cdest-TTL: *time-to-live*
X-MD-Intercept-Id: *8-byte-id*
Dtcp-trigger: trigger-value
Dtcp-attribute: attribute-value
Flags: *flag*
Seq: *sequence-number*
Authentication-Info: *ssh-authentication-string*

Description

Specify the DTCP attributes used in ADD messages to cause the router to trigger traffic mirroring and provide instructions to populate fields in the encapsulation header for packets sent to the mediation device.

The DTCP ADD message can be sent either before or after subscribers log in through the interface.

The following attributes are added to the packet header of mirrored packets that the router sends to the mediation device. These attributes are required in the DTCP ADD message.

- X-JTap-Cdest-Dest-Address
- X-JTap-Cdest-Dest-Port
- X-MD-Intercept-Id

Options

Csource-ID: *user-name*—Username on the router. This username must be configured as a DTCP user on the router using the **set system login class** or **set system login user** statements.

Cdest-ID: *variable*—ID of the mediation device.

Flags: *flag*—STATIC is the only flag supported.

Priority: *priority-number*—This implementation of DTCP does not use the priority number.

X-Drop-Policy *policy-name*—Name of the policy used to determine which mirrored packets are no longer sent to the mediation device.

X-JTap-Cdest-Dest-Address: *ipv4-address*—Destination IPv4 address of the mediation device to which intercepted packets are sent. You must include this attribute in your ADD messages.. It is used in the header of mirrored traffic that is sent to the mediation device.

X-JTap-Cdest-Dest-Port: ***udp-port***—Destination port of the mediation device to which intercepted packets are sent. You must include this attribute in your ADD messages. It is used in the header of mirrored traffic that is sent to the mediation device.

X-JTap-Cdest-Source-Address: ***ipv4-address***—Source IPv4 address. You must include this attribute in your ADD messages. If the value entered does not match the value configured on the router using the **set services radius-flow-tap source-ipv4-address** ***source-ipv4-address*** statement, it is replaced by configured value.

X-JTap-Cdest-Source-Port: ***port-number***—Source port. You must include this attribute in your ADD messages. If the value entered does not match the value of X-Jtap-Cdest-Dest-Port, it is ignored.

X-JTap-Cdest-TTL: ***time-to-live***—TTL value to be used in the forwarded packet.

X-MD-Intercept-Id ***8-byte-id***—An Id that is used to identify a subscriber. You must include this attribute in your ADD messages. This ID is used in the header of mirrored traffic that is sent to the mediation device to allow the device to track a subscriber. The X-MD-Intercept-ID attribute must consist of 8-bytes, and the first two bits must be 00.

Dtcp-trigger*: *trigger-value—DTCP attribute used to trigger traffic mirroring. "DTCP Traffic Mirroring Triggers" on page 11 lists the DTCP attributes that you can use in DTCP ADD messages to trigger traffic mirroring.

Dtcp-attribute*: *attribute-value—DTCP attribute included in the ADD messages. "DTCP Traffic Mirroring Triggers" on page 11 lists the DTCP attributes that you can use in ADD messages.

Seq: ***sequence-number***—Number added by the mediation device. DTCP messages contain a monotonically increasing sequence number for each successive message.

Authentication-Info: ***ssh-authentication-string***—String used when you are using SSH to connect to the router.

Required Privilege Level

Not applicable.

Related Documentation

- DTCP Traffic Mirroring Triggers on page 11
- DTCP-Initiated Subscriber Secure Policy Overview on page 5
- DELETE DTCP on page 35
- LIST DTCP on page 39

Sample Output

```
ADD DTCP/0.7
Csource-ID: ft-user1
Cdest-ID: cd1
Priority: 2
X-JTap-Cdest-Dest-Address: 10.10.2.50
X-JTap-Cdest-Dest-Port: 7890
```

```
X-JTap-Cdest-Source-Address: 10.10.2.9
X-JTap-Cdest-Source-Port: 12321
X-Interface-Id: ge-0/0/2.1
X-MD-Intercept-Id: 55667788
Flags: STATIC
Seq: 1
Authentication-Info: c16d2d9d1679facf0c4a66683af6114d341e4033

DTCP/0.7 200 OK
SEQ: 7
CRITERIA-ID: 2
TIMESTAMP: 2011-02-13 15:56:49.609
```

DELETE DTCP

Syntax

DELETE DTCP/0.7
Csource-ID: *user-name*
CRITERIA-ID: *criteria-id*
Cdest-ID: *variable*
Flags: *flag*
Seq: *sequence-number*
Authentication-Info:*ssh-authentication-string*

Description

Disable traffic mirroring for a subscriber. Mirroring of the existing subscriber is stopped.

Options

Csource-ID: *user-name*—Username on the router. This name must be configured on the router.

CRITERIA-ID: *criteria-id*—ID that DTCP assigns for the mirrored session when you create a DTCP ADD message. Use this ID in your DELETE messages to disable the intercept for a specific subscriber. To view the ID, use the DTCP LIST message. The CRITERIA-ID and the Cdest-ID are mutually exclusive in DELETE messages.

Cdest-ID: *variable*—ID of the mediation device. Use this ID in your DELETE messages to remove all mirroring sessions associated with a mediation device. The Cdest-ID and the CRITERIA-ID are mutually exclusive in DELETE messages.

Flags: *flag*—STATIC is the only flag supported.

Seq: *sequence-number*—Number added by the mediation device. DTCP messages contain a monotonically increasing sequence number for each successive message.

Authentication-Info: *ssh-authentication-string*—String used when you are using SSH to connect to the router.

Required Privilege Level

Not applicable.

Related Documentation

- DTCP Traffic Mirroring Triggers on page 11
- DTCP-Initiated Subscriber Secure Policy Overview on page 5
- ADD DTCP on page 32
- LIST DTCP on page 39

List of Sample Output

DELETE DTCP on page 36

Sample Output

The following sample shows how to disable mirroring for a specific subscriber by using the CRITERIA-ID.

DELETE DTCP

```
DELETE DTCP/0.7
Csource-ID: dtcp1
CRITERIA-ID: 2
Flags: STATIC
Seq: 10
Authentication-Info: 7e84ae871b12f2da023b038774115bb8d955f17e


DTCP/0.7 200 OK
SEQ: 10
CRITERIA-COUNT: 1
TIMESTAMP: 2011-02-13 16:00:02.802
AUTHENTICATION-INFO: 2834ff32ec07d84753a046cfb552e072cc27d50b
```

DISABLE DTCP

Syntax

DISABLE DTCP/0.7
Csource-ID: *user-name*
Criteria-ID: *variable*
X-Drop-Policy: *variable*
Flags: *flags*

Release Information

Command introduced in Junos OS Release 12.3.

Description

Specify the DTCP ENABLE message to remove a drop policy that exists because of a prior DTCP ADD or DTCP ENABLE command

The DTCP DISABLE message can only be issued on a Criteria-ID that was returned in a response to a previous DTCP ADD. The policy applies to any new subscribers that match the trigger corresponding to the Criteria-ID. Any existing mirroring remains in place, the policy is not be applied to them.

Options

Csource-ID: *user-name*—Username on the router. This username must be configured as a DTCP user on the router using the **set system login class** or **set system login user** statements.

Criteria-ID: *variable*—Identifies the subscriber on which the policy update occurs.

Flags: *flag*—STATIC is the only flag supported.

X-Drop-Policy: *variable*—Name of the policy that determines which mirrored packets are no longer sent to the mediation device.

Required Privilege Level

Not applicable.

Related Documentation

- ENABLE DTCP on page 38

Sample Output

```
DISABLE DTCP/0.7
Csource-ID: ft-user1
Criteria-ID: 1
X-Drop: T1
Flags: STATIC
Seq: 1
Authentication-Info: c16d2d9d1679facf0c4a66683af6114d341e4033

DTCP/0.7 200 OK
SEQ: 7
CRITERIA-ID: 2
TIMESTAMP: 2011-02-13 15:56:49.609
```

ENABLE DTCP

Syntax

ENABLE DTCP/0.7
Csource-ID: *user-name*
Criteria-ID: *variable*
X-Drop-Policy: *variable*
Flags: *flags*

Release Information

Command introduced in Junos OS Release 12.3.

Description

Specify the DTCP attributes used in ENABLE messages to cause the router to trigger a drop policy if one does not already exist from a prior DTCP ADD or DTCP ENABLE command.

The DTCP ENABLE message can only be issued on a Criteria-ID that was returned in a response to a previous DTCP ADD command. The policy applies to any new subscribers who match the trigger corresponding to the Criteria-ID. Any existing mirroring remains in place and the policy is not be applied to them. The DTCP ENABLE command stops only the traffic that is identified by the specified policy from being sent to the mediation device.

Options

Csource-ID: ***user-name***—Username on the router. This username must be configured as a DTCP user on the router using the **set system login class** or **set system login user** statements.

Criteria-ID: ***variable***—Value returned from a prior DTCP ADD that identifies the trigger on which to disable this drop policy.

Flags: ***flag***—STATIC is the only flag supported.

X-Drop-Policy: ***variable***—Name of the policy that determines which mirrored packets are no longer sent to the mediation device.

Required Privilege Level

Not applicable.

Related Documentation

- DISABLE DTCP on page 37

Sample Output

```
ENABLE DTCP/0.7
Csource-ID: ft-user1
Criteria-ID: 1
X-Drop: T1
Flags: STATIC
Seq: 1
Authentication-Info: c16d2d9d1679facf0c4a66683af6114d341e4033

DTCP/0.7 200 OK
SEQ: 7
CRITERIA-ID: 2
TIMESTAMP: 2011-02-13 15:56:49.609
```

LIST DTCP

Syntax

LIST DTCP/0.7
Csource-ID: *user-name*
Cdest-ID: *variable*
Flags: BOTH
Seq: *sequence-number*
Authentication-Info:*ssh-authentication-string*

Description

Request information that is returned in a LIST response. The response lists triggers only. It does not return sessions that are being mirrored.

Options

Csource-ID: ***user-name***—Username on the router. This name must be configured on the router.

Cdest-ID: ***variable***—ID of the mediation device.

Flags: ***flag***—BOTH is the only flag supported. This field must be included in the LIST message.

Seq: ***sequence-number***—Number added by the mediation device. DTCP messages contain a monotonically increasing sequence number for each successive message.

Authentication-Info: ***ssh-authentication-string***—String used when you are using SSH to connect to the router.

Required Privilege Level

Not applicable.

Related Documentation

- DTCP Traffic Mirroring Triggers on page 11
- DTCP-Initiated Subscriber Secure Policy Overview on page 5
- ADD DTCP on page 32
- DELETE DTCP on page 35

List of Sample Output

LIST DTCP on page 39

Sample Output

LIST DTCP

```
LIST DTCP/0.7
Csource-ID: dtcp1
Cdest-ID: cd1
Flags: BOTH
Seq: 9
Authentication-Info: f6dd64643021debb167ce2fb2d3c7b6622a87e09

DTCP/0.7 200 OK
SEQ: 9
TIMESTAMP: 2011-02-13 15:57:47.667
CRITERIA-ID: 2
CSOURCE-ID: dtcp1
```

```
CDEST-ID: cd1
CSOURCE-ADDRESS: 10.10.4.224
FLAGS: BOTH
X-JTAP-CDEST-DEST-ADDRESS: 192.0.40.168
X-JTAP-CDEST-DEST-PORT: 65535
X-JTAP-CDEST-SOURCE-ADDRESS: 198.15.0.10
X-JTAP-CDEST-SOURCE-PORT: 50000
X-JTAP-CDEST-TTL: 64
X-INTERFACE-ID: demux0.30010002
X-MD-INTERCEPT-ID: 0x0101010130010002
CRITERIA-NUM: 1
CRITERIA-COUNT: 0

CRITERIA-ID: 3
CSOURCE-ID: dtcp1
CDEST-ID: cd1
CSOURCE-ADDRESS: 10.10.4.224
FLAGS: BOTH
X-JTAP-CDEST-DEST-ADDRESS: 192.0.40.168
X-JTAP-CDEST-DEST-PORT: 65535
X-JTAP-CDEST-SOURCE-ADDRESS: 198.15.0.10
X-JTAP-CDEST-SOURCE-PORT: 50000
X-JTAP-CDEST-TTL: 64
X-INTERFACE-ID: demux0.30010001
X-MD-INTERCEPT-ID: 0x0101010130010001
CRITERIA-NUM: 2
CRITERIA-COUNT: 2
AUTHENTICATION-INFO: 361171ccb24dde6afe8ef66021287f9b8ac16028
```


CHAPTER 6

Examples

Example: Using DTCP Messages to Trigger, Verify, and Disable Traffic Mirroring for Subscribers

This example shows how to create DTCP messages to do the following:

- Trigger traffic mirroring for two subscribers based on interface ID.
- Trigger a drop policy if one does not already exist.
- Remove an existing drop policy.
- Verify that subscriber traffic on the two interfaces is being mirrored.
- Disable traffic mirroring on the two subscriber interfaces.
- Verify that traffic mirroring was stopped on the two subscriber interfaces.

In this example, SSH is being used to communicate with the router.

Creating DTCP ADD Messages to Trigger Traffic Mirroring

This section shows examples of DTCP ADD messages on a mediation device that use the interface ID to trigger traffic mirroring on interfaces demux0.30010002 and demux0.30010001.

```
ADD DTCP/0.7
Csource-ID: dtcp1
Cdest-ID: cd1
Priority: 2
X-JTap-Cdest-Dest-Address: 192.0.40.168
X-JTap-Cdest-Dest-Port: 65535
X-JTap-Cdest-Source-Address: 198.15.0.10
X-JTap-Cdest-Source-Port: 50000
X-JTap-Cdest-TTL: 64
X-Interface-Id: demux0.30010002     /*Used as trigger*/
X-MD-Intercept-Id: 0x0101010130010002
Flags: BOTH
Seq: 7
Authentication-Info: c16d2d9d1679facf0c4a66683af6114d341e4033
```

```
DTCP/0.7 200 OK
SEQ: 7
CRITERIA-ID: 2
TIMESTAMP: 2011-02-13 15:56:49.609
AUTHENTICATION-INFO: 4880de4b8cead98c95813fd9b95e240b107d4693


ADD DTCP/0.7
Csource-ID: dtcp1
Cdest-ID: cd1
Priority: 2
X-JTap-Cdest-Dest-Address: 192.0.40.168
X-JTap-Cdest-Dest-Port: 65535
X-JTap-Cdest-Source-Address: 198.15.0.10
X-JTap-Cdest-Source-Port: 50000
X-JTap-Cdest-TTL: 64
X-Interface-Id: demux0.30010001     /*Used as trigger*/
X-MD-Intercept-Id: 0x0101010130010001
Flags: STATIC
Seq: 8
Authentication-Info: dc3c55481a3810c7dd29fdc1b4681d978ff4e7c4

DTCP/0.7 200 OK
SEQ: 8
CRITERIA-ID: 3
TIMESTAMP: 2011-02-13 15:57:20.640
AUTHENTICATION-INFO: 4b31ef1311647e5ba52d2d5d4237b9e5beaa47b7

ADD DTCP/0.7
Csource-ID: ft-user1
Cdest-ID: cd1
Priority: 2
X-JTap-Cdest-Dest-Address:  1.1.1.2
X-JTap-Cdest-Dest-Port: 7899
X-JTap-Cdest-Source-Address: 2.2.2.9
X-JTap-Cdest-Source-Port: 12321
X-Username: testuser
X-MD-Intercept-Id: 55667789
Flags: STATIC


DTCP/0.7 200 OK
SEQ: 100
CRITERIA-ID: 1
```

Creating DTCP ENABLE Messages to Trigger Traffic Mirroring

This section shows an example of DTCP ENABLE messages on a mediation device that use the interface ID to trigger traffic mirroring on interfaces demux0.30010002 and demux0.30010001.

```
ENABLE DTCP/0.8
Csource-ID: ft-user1
Cdest-ID: cd1
X-Drop-Policy: vod
Flags: STATIC
```

Creating DTCP DISABLE Messages to Trigger Traffic Mirroring

This section shows examples of DTCP DISABLE messages on a mediation device that use the interface ID to trigger traffic mirroring on interfaces demux0.30010002 and demux0.30010001. Whether you used DTCP ADD plus a policy or DTCP ADD and DTCP ENABLE, you can turn the policy off with DTCP DISABLE.

```
DISABLE DTCP/0.8
Csource-ID: ft-user1
Criteria-ID: 1
X-Drop-Policy: vod
Flags: STATIC

DISABLE DTCP/0.8
Csource-ID: ft-user1
Cdest-ID: cd1
X-Drop-Policy: vod
Flags: STATIC
```

Using LIST Messages to Verify That Subscriber Traffic Is Being Mirrored

This section shows examples of a LIST message on the mediation device. The LIST message requests information about the subscribers being mirrored. The information is returned in a LIST response. The response shows that traffic for the two interfaces—demux0.30010002 and demux0.30010001—is being mirrored.

```
LIST DTCP/0.7
Csource-ID: dtcp1
Cdest-ID: cd1
Seq: 9
Authentication-Info: f6dd64643021debb167ce2fb2d3c7b6622a87e09


DTCP/0.7 200 OK
SEQ: 9
TIMESTAMP: 2011-02-13 15:57:47.667
CRITERIA-ID: 2
CSOURCE-ID: dtcp1
CDEST-ID: cd1
CSOURCE-ADDRESS: 10.10.4.224
FLAGS: BOTH
X-JTAP-CDEST-DEST-ADDRESS: 192.0.40.168
X-JTAP-CDEST-DEST-PORT: 65535
X-JTAP-CDEST-SOURCE-ADDRESS: 198.15.0.10
X-JTAP-CDEST-SOURCE-PORT: 50000
X-JTAP-CDEST-TTL: 64
X-INTERFACE-ID: demux0.30010002    /*subscriber interface*/
X-MD-INTERCEPT-ID: 0x0101010130010002
CRITERIA-NUM: 1
CRITERIA-COUNT: 0

CRITERIA-ID: 3
CSOURCE-ID: dtcp1
CDEST-ID: cd1
CSOURCE-ADDRESS: 10.10.4.224
FLAGS: BOTH
X-JTAP-CDEST-DEST-ADDRESS: 192.0.40.168
X-JTAP-CDEST-DEST-PORT: 65535
```

```
X-JTAP-CDEST-SOURCE-ADDRESS: 198.15.0.10
X-JTAP-CDEST-SOURCE-PORT: 50000
X-JTAP-CDEST-TTL: 64
X-INTERFACE-ID: demux0.30010001  /*subscriber interface*/
X-MD-INTERCEPT-ID: 0x0101010130010001
CRITERIA-NUM: 2
CRITERIA-COUNT: 2
AUTHENTICATION-INFO: 361171ccb24dde6afe8ef66021287f9b8ac16028
```

Using DELETE Messages to Remove Traffic Mirroring Triggers

This section shows examples of DELETE messages used to remove traffic mirroring triggers on demux0.30010001 and demux0.30010002. DTCP DELETE can use either Criteria-ID to delete only that criteria or Cdest-ID to delete everything with cdest-ID that you previously created.

```
DELETE DTCP/0.7
Csource-ID: dtcp1
CRITERIA-ID: 2
Flags: STATIC
Seq: 10
Authentication-Info: 7e84ae871b12f2da023b038774115bb8d955f17e


DTCP/0.7 200 OK
SEQ: 10
CRITERIA-COUNT: 1
TIMESTAMP: 2011-02-13 16:00:02.802
AUTHENTICATION-INFO: 2834ff32ec07d84753a046cfb552e072cc27d50b


DELETE DTCP/0.7
Csource-ID: dtcp1
CRITERIA-ID: 3
Flags: STATIC
Seq: 12
Authentication-Info: 7653fd94659a7183a990bdea654a1b97c0895348

DTCP/0.7 200 OK
SEQ: 12
CRITERIA-COUNT: 1
TIMESTAMP: 2011-02-13 16:01:35.895
AUTHENTICATION-INFO: 7cd8171057a327434e1b2d9b35f43b88305f9a74
```

Using Disable Messages to Disable Traffic Mirroring Triggers

This section shows an example of

Using Enable Messages to Enable Traffic Mirroring Triggers

This section shows an example of

Verifying That Traffic Mirroring Was Stopped on the Subscriber Interfaces

This section shows an example of a LIST message used to show that traffic mirroring on demux0.30010001 and demux0.30010002 is disabled.

```
LIST DTCP/0.7
Csource-ID: dtcp1
```

```
Cdest-ID: cd1
Seq: 13
Authentication-Info: 7c9f825427cfeaecebb0d13ea3842af1021c7d26

DTCP/0.7 400 Bad Request
SEQ: 13
AUTHENTICATION-INFO: 5ca2eec65106354fe59c878b4c36b7de3c511acd
```

Related Documentation

- DTCP-Initiated Subscriber Secure Policy Overview on page 5
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 21

CHAPTER 7

Configuration Statements

[edit services radius-flow-tap] Hierarchy Level

```
services {
  radius-flow-tap {
    forwarding-class class-name;
    interfaces interface-name;
    multicast-interception;
    policy  policy-name {
      inet {
        drop-policyrule-name {
          from {
            apply-groups group-name;
            apply-groups-except group-name;
            destination-address address;
            destination-port port-number;
            dscp dscp-value;
            protocol protocol;
            source-address address;
            source-port port-number;
          }
        }
      }
      inet6 {
        drop-policyrule-name {
          from {
            apply-groups group-name;
            apply-groups-except group-name;
            destination-address address;
            destination-port port-number;
            dscp dscp-value;
            protocol protocol;
            source-address address;
            source-port port-number;
          }
        }
      }
    }
    source-ipv4-address ipv4-address;
  )
}
```

Related Documentation
- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

apply-groups (Subscriber Secure Policy)

Syntax apply-groups *group-name*;

Hierarchy Level [edit services radius-flow-tap policy *policy-name* inet drop-policy *rule-name* from],
[edit services radius-flow-tap policy *policy-name* inet6 drop-policy *rule-name* from]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify groups from which to inherit configuration data for the radius-flow-tap policy.

Options ***group-name***— Name of the group that inherits the configuration data.

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

apply-groups-except (Subscriber Secure Policy)

Syntax apply-groups-except *group-name*;

Hierarchy Level [edit services radius-flow-tap policy *policy-name* inet drop-policy *rule-name* from],
[edit services radius-flow-tap policy *policy-name* inet6 drop-policy *rule-name* from]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify groups from which to inherit configuration data for the radius-flow-tap policy.

Options ***group-name***— Name of the group that does not inherit the configuration data.

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

authentication (Login)

Syntax

```
authentication {
  (encrypted-password "password" | plain-text-password);
  load-key-file URL filename;
  ssh-dsa "public-key";
  ssh-ecdsa "public-key";
  ssh-rsa "public-key";
}
```

Hierarchy Level [edit system login user *username*]

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

Description Authentication methods that a user can use to log in to the router or switch. You can assign multiple authentication methods to a single user.

Options

encrypted-password "*password*"—Message Digest 5 (MD5) or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.

You cannot configure a blank password for **encrypted-password** using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

load-key-file *URL filename*—Load previously-generated RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys from a named file at a specified URL location. The file contains one or more SSH keys.

plain-text-password—When using this option, the command-line interface (CLI) prompts you for the password and then encrypts it.

ssh-dsa "*public-key*"—SSH version 2 authentication. Specify the DSA public key. You can specify one or more public keys for each user.

ssh-ecdsa "*public-key*"—SSH version 2 authentication. Specify the ECDSA public key. You can specify one or more public keys for each user.

ssh-rsa "*public-key*"—SSH version 1 and SSH version 2 authentication. Specify the RSA public key. You can specify one or more public keys for each user.

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

Related Documentation

- *Configuring Junos OS User Accounts*
- *root-authentication*

authentication-order

Syntax authentication-order [*authentication-methods*];

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Option **none** introduced in Junos OS Release 11.2.

Description Set the order in which the Junos OS tries different authentication methods when verifying that a client can access the router or switch. For each login attempt, the software tries the authentication methods in order, from first to last.

Default password

Options *authentication-methods*

- **none**—Grants authentication without examining the client credentials. Can be used, for example, when the Diameter function Gx-Plus is employed for notification during subscriber provisioning.
- **password**—Verify the client using the information configured at the **[edit access profile *profile-name* client *client-name*]** hierarchy level.
- **radius**—Verify the client using RADIUS authentication services.

NOTE: For subscriber access management, you must always specify the radius method. Subscriber access management does not support the password option (the default), and authentication fails when no method is specified.

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

Related Documentation

- *Example: Configuring CHAP Authentication with RADIUS*
- *Specifying the Authentication and Accounting Methods for Subscriber Access*
- *Configuring Access Profiles for L2TP or PPP Parameters*

authentication-server

Syntax authentication-server [*ip-address*];

Hierarchy Level [edit access profile *profile-name* radius]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients. The servers in the list are also used as RADIUS dynamic-request servers, from which the router accepts and processes RADIUS disconnect requests, CoA requests, and dynamic service activations and deactivations.

Options ***ip-address***—IPv4 address.

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

Related Documentation

- *Configuring RADIUS Server Parameters for Subscriber Access*

bandwidth (Tunnel Services)

Syntax bandwidth *bandwidth-value*;

Hierarchy Level [edit chassis fpc *slot-number* pic *number* tunnel-services]

Release Information Statement introduced in Junos OS Release 8.2.

Description (MX Series 3D Universal Edge Routers and T4000 Core Routers only) Specify the amount of bandwidth in gigabits per second to reserve for tunnel services.

Options *bandwidth-value*—Define the amount of bandwidth in gigabits per second to reserve for tunnel services. On MX Series routers, the bandwidth values can be **1g**, **10g**, **20g**, or **40g**. On T4000 routers, the bandwidth values are multiples of **10g** up to **100g**.

NOTE: The bandwidth that you specify determines the port number of the tunnel interfaces that are created. When you specify a bandwidth of 1g, the port number is always 10. When you specify any other bandwidth, the port number is always 0.

NOTE: If you specify a bandwidth that is not compatible with the type of DPCs or MPCs and their respective Packet Forwarding Engine, tunnel services are not activated. For example, you cannot specify 1 gigabit per second bandwidth for a Packet Forwarding Engine on a 10-Gigabit Ethernet 4-port DPC.

NOTE: Bandwidth rates of 20 gigabits per second and 40 gigabits per second require use of an MX Series router with the MPC3E and the 100-Gigabit CFP MIC.

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

Related Documentation

- *Example: Configuring Tunnel Interfaces on a Gigabit Ethernet 40-Port DPC*
- *Configuring Tunnel Interfaces on MX Series Routers*
- *Configuring Tunnel Interfaces on T4000 Routers*
- *Example: Configuring Tunnel Interfaces on a 10-Gigabit Ethernet 4-Port DPC*
- *Example: Configuring Tunnel Interfaces on the MPC3E*
- *Configuring Layer 3 Tunnel Services Interfaces on an MX Series Router with a DPC*

- tunnel-services (Chassis) on page 79
- *[edit chassis] Hierarchy Level*

class (Defining Login Classes)

Syntax

```
class class-name {
  allow-commands "regular-expression";
  ( allow-configuration | allow-configuration-regexps) “regular expression 1” “regular
    expression 2”;
  configuration-breadcrumbs;
  deny-commands "regular-expression";
  ( deny-configuration | deny-configuration-regexps ) “regular expression 1” “regular expression
    2 ”;
  idle-timeout minutes;
  login-script filename;
  login-tip;
  permissions [ permissions ];
}
```

Hierarchy Level [edit system login]

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

Description Define a login class.

Options ***class-name***—A name you choose for the login class.

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

- *Defining Junos OS Login Classes*
- user on page 81

class (Assigning a Class to an Individual User)

Syntax class *class-name*;

Hierarchy Level [edit system login user *username*]

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

Description Assign a user to a login class. You must assign each user to a login class.

Options ***class-name***—One of the classes defined at the **[edit system login class]** hierarchy level.

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

Related Documentation

- *Configuring Junos OS User Accounts*

connection-limit

Syntax connection-limit *limit*;

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

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

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

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

Range: 1 through 250

Default: 75

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

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

Related Documentation

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*
- *Configuring DTCP-over-SSH Service for the Flow-Tap Application*
- *Configuring Finger Service for Remote Access to the Router*
- *Configuring FTP Service for Remote Access to the Router or Switch*
- *Configuring SSH Service for Remote Access to the Router or Switch*
- *Configuring Telnet Service for Remote Access to a Router or Switch*

destination-address (Subscriber Secure Policy)

Syntax destination-address *address*;

Hierarchy Level [edit services radius-flow-tap policy *policy-name* inet drop-policy *rule-name* from],
[edit services radius-flow-tap policy *policy-name* inet6 drop-policy *rule-name* from]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify destination IP address or prefix value for radius-flow-tap policy rule mapping.

Options ***address***— IPv4 or IPv6 address for the radius-flow-tap policy.

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

destination-port (Subscriber Secure Policy)

Syntax destination-port *port-number*;

Hierarchy Level [edit services radius-flow-tap policy *policy-name* inet drop-policy *rule-name* from],
[edit services radius-flow-tap policy *policy-name* inet6 drop-policy *rule-name* from]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify the destination IP address for the radius-flow-tap policy.

Options ***port-number***— Number of the IPv4 or IPv6 destination port for the radius-flow-tap policy.

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

drop-policy (Subscriber Secure Policy)

Syntax

```
drop-policy rule-name {
  from {
    apply-groups group-name;
    apply-groups-except group-name;
    destination-address address;
    destination-port port-number;
    dscp dscp-value;
    protocol protocol;
    source-address address;
    source-port port-number;
  }
}
```

Hierarchy Level [edit services radius-flow-tap policy *policy-name* inet| inet6]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify the drop-policy that is applied to mirrored packets sent to a mediation device.

Options *rule*-name—Define the term name.

The remaining statements are explained separately.

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

Related Documentation

- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

dscp (Subscriber Secure Policy)

Syntax dscp *value*;

Hierarchy Level [edit services radius-flow-tap policy *policy-name* inet drop-policy *rule-name* from],
[edit services radius-flow-tap policy *policy-name* inet6 drop-policy *rule-name* from]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify the DSCP value for the radius-flow-tap policy.

Options ***dscp-value***— IPv4 or IPv6 dscp value for the radius-flow-tap policy.

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

Related Documentation

- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

flow-tap-dtcp

Syntax

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

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 8.1.

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

Options

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

Range: 1 through 250

Default: 75

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

Range: 1 through 250

Default: 150

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

Related Documentation

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

forwarding-class (Subscriber Secure Policy)

Syntax forwarding-class *class-name*;

Hierarchy Level [edit services radius-flow-tap]

Release Information Statement introduced in Junos OS Release 9.4.

Description Specify forwarding class that is applied to mirrored packets sent to a mediation device.

Options ***class-name***—Name of the forwarding class.

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

Related Documentation

- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

fpc (MX Series 3D Universal Edge Routers)

Syntax

```
fpc slot-number {
  inline-services {
    flow-table-size {
      ipv4-flow-table-size units;
      ipv4-flow-table-size  units;
    }
  }
  pic number {
    inline-services {
      bandwidth (1g | 10g);
    }
    port-mirror-instance port-mirroring-instance-name-pic-level;
    tunnel-services {
      bandwidth (1g | 10g)
    }
  }
  port-mirror-instance port-mirroring-instance-name-fpc-level;
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 8.2.
Option **port-mirror-instance** introduced in Junos OS Release 9.3.

Description Configure properties for the DPC or MPC and corresponding Packet Forwarding Engines to create tunnel interfaces.

(MX Series Virtual Chassis only) To configure properties for MPCs in a member router in an MX Series Virtual Chassis configuration, you must specify the router's Virtual Chassis member number *before* the **fpc** statement. Specify the member number in the form **member *member-id***, where ***member-id*** is 0 or 1. If you do not specify the member number before the **fpc** statement, the commit operation fails and the software displays an error message indicating that the **fpc** statement must include the member number for routers in Virtual Chassis mode.

Options

fpc *slot-number*—Specify the slot number of the DPC.

Range: 0 through 11

pic *number*—Specify the number of the Packet Forwarding Engine. Each DPC includes four Packet Forwarding Engines.

Range: 0 through 4

port-mirror-instance *port-mirroring-instance-name-fpc-level*—Associate a port-mirroring instance with the DPC and its corresponding PICs. The port-mirroring instance is configured under the **[edit forwarding-options port-mirroring]** hierarchy level.

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 Port-Mirroring Instances on MX Series 3D Universal Edge Routers*
- *Enabling Inline Service Interfaces*

from (Subscriber Secure Policy)

Syntax

```
from {
  apply-groups group-name;
  apply-groups-except group-name;
  destination-address address;
  destination-port port-number;
  dscp dscp-value;
  protocol protocol;
  source-address address;
  source-port port-number;
}
```

Hierarchy Level
[edit services radius-flow-tappolicy *policy-name* inet| inet6]

Release Information
Statement introduced in Junos OS Release 12.3.

Description
Define the match criteria for the drop-policy rule.

The remaining statements are explained separately.

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

interfaces (Subscriber Secure Policy)

Syntax interfaces *interface-name*;

Hierarchy Level [edit services radius-flow-tap]

Release Information Statement introduced in Junos OS Release 9.4.

Description Specify tunnel interfaces that are used to send mirrored packets to a mediation device.

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

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

inet (Subscriber Secure Policy)

Syntax

```
inet {
  drop-policy rule-name {
    from {
      apply-groups group-name;
      apply-groups-except group-name;
      destination-address address;
      destination-port port-number;
      dscp dscp-value;
      protocol protocol;
      source-address address;
      source-port port-number;
    }
  }
}
```

Hierarchy Level [edit services radius-flow-tap policy *policy-name*]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify the inet family for the policy that is applied to mirrored packets sent to a mediation device.

The remaining statements are explained separately.

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

inet6 (Subscriber Secure Policy)

Syntax

```
inet6 {
  drop-policy rule-name {
    from {
      apply-groups group-name;
      apply-groups-except group-name;
      destination-address address;
      destination-port port-number;
      dscp dscp-value;
      protocol protocol;
      source-address address;
      source-port port-number;
    }
  }
}
```

Hierarchy Level [edit services radius-flow-tap policy *policy-name*]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify the inet6 family for the policy that is applied to mirrored packets sent to a mediation device.

The remaining statements are explained separately.

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

Related Documentation

- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

login

Syntax

```
login {
  announcement text;
  class class-name {
    allow-commands "regular-expression";
    allow-configuration-regexps "regular expression 1" "regular expression 2";
    configuration-breadcrumbs;
    deny-commands "regular-expression";
    ( deny-configuration | deny-configuration-regexps ) “regular expression 1” “regular
      expression 2 ”;
    idle-timeout minutes;
    login-script filename;
    login-tip;
    permissions [ permissions ];
  }
  message text;
  password {
    change-type (set-transitions | character-set);
    format (md5 | sha1 | des);
    maximum-length length;
    minimum-changes number;
    minimum-length length;
  }
  retry-options {
    backoff-threshold number;
    backoff-factor seconds;
    minimum-time seconds;
    tries-before-disconnect number;
  }
  user username {
    full-name complete-name;
    uid uid-value;
    class class-name;
    authentication authentication;
    (encrypted-password "password" | plain-text-password);
    ssh-rsa "public-key";
    ssh-dsa "public-key";
  }
}
```

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 user access to the router or switch.

NOTE: 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
- *Defining Junos OS Login Classes*

multicast-interception (Subscriber Secure Policy)

Syntax
multicast-interception;

Hierarchy Level
[edit services radius-flow-tap]

Release Information
Statement introduced in Junos OS Release 11.4.

Description
Enables subscriber secure policy to mirror IPv4 multicast traffic sent to subscribers. It enables the mirroring of multicast traffic for all subscribers on the chassis.

Mirroring of multicast traffic is supported only for subscribers in the default logical system.

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- Subscriber Secure Policy Support for IPv4 Multicast Traffic on page 10
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 21

permissions

Syntax
permissions [*permissions*];

Hierarchy Level
[edit system login class]

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 login access privileges to be provided on the router or switch.

Options
permissions—Privilege type. For a list of permission flag types, see *Understanding Junos OS Access Privilege Levels*.

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

Related Documentation
- *Configuring Access Privilege Levels*
- user on page 81

policy (Subscriber Secure Policy)

Syntax

```
policy policy-name {
  inet {
    drop-policy rule-name {
      from {
        apply-groups group-name;
        apply-groups-except group-name;
        destination-address address;
        destination-port port-number;
        dscp dscp-value;
        protocol protocol;
        source-address address;
        source-port port-number;
      }
    }
  }
  inet6 {
    drop-policy rule-name {
      from {
        apply-groups group-name;
        apply-groups-except group-name;
        destination-address address;
        destination-port port-number;
        dscp dscp-value;
        protocol protocol;
        source-address address;
        source-port port-number;
      }
    }
  }
}
```

Hierarchy Level [edit services radius-flow-tap]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify the policy that is applied to mirrored packets sent to a mediation device.

Options *policy-name*—Name of the policy from which to drop traffic.

The remaining statements are explained separately.

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

Related Documentation

- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

profile (Access)

Syntax

```
profile profile-name {
  accounting {
    address-change-immediate-update
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    ancp-speed-change-immediate-update;
    coa-immediate-update;
    coa-no-override service-class-attribute;
    duplication;
    duplication-vrf {
      access-profile-name profile-name;
      vrf-name vrf-name;
    }
    immediate-update;
    order [ accounting-method ];
    send-acct-status-on-config-change;
    statistics (time | volume-time);
    update-interval minutes;
    wait-for-acct-on-ack;
    }
  authentication-order [ authentication-methods ];
  client client-name {
    chap-secret chap-secret;
    group-profile profile-name;
    ike {
      allowed-proxy-pair {
        remote remote-proxy-address local local-proxy-address;
      }
      pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
      ike-policy policy-name;
      interface-id string-value;
    }
    l2tp {
      aaa-access-profile profile-name;
      interface-id interface-id;
      lcp-renegotiation;
      local-chap;
      maximum-sessions-per-tunnel number;
      multilink {
        drop-timeout milliseconds;
        fragment-threshold bytes;
      }
      ppp-authentication (chap | pap);
      ppp-profile profile-name;
      shared-secret shared-secret;
    }
    pap-password pap-password;
    ppp {
      cell-overhead;
      encapsulation-overhead bytes;
      framed-ip-address ip-address;
      framed-pool framed-pool;
```

```
        idle-timeout seconds;
        interface-id interface-id;
        keepalive seconds;
        primary-dns primary-dns;
        primary-wins primary-wins;
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
    }
    user-group-profile profile-name;
}
domain-name-server;
domain-name-server-inet;
domain-name-server-inet6;
preauthentication-order preauthentication-method;
provisioning-order (gx-plus | jsrc);
radius {
    accounting-server [ ip-address ];
    attributes {
        exclude {
            ...
        }
        ignore {
            framed-ip-netmask;
            input-filter;
            logical-system:routing-instance;
            output-filter;
        }
    }
    authentication-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        calling-station-id-delimiter delimiter-character;
        calling-station-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
        }
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        coa-dynamic-variable-validation;
        ethernet-port-type-virtual;
        interface-description-format {
            exclude-adapter;
            exclude-sub-interface;
        }
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            ae-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
            atm {
```

```
            adapter-width width;
            port-width width:
            slot-width width;
            vci-width width:
            vpi-width width;
          }
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
          agent-circuit-id;
          agent-remote-id;
          interface-description;
          nas-identifier;
        }
        nas-port-type {
          ethernet {
            port-type;
          }
        }
        revert-interval interval;
        vlan-nas-port-stacked-format;
      }
      preauthentication-server ip-address;
    }
    radius-server server-address {
      accounting-port port-number;
      accounting-retry number;
      accounting-timeout seconds;
      port port-number;
      retry attempts;
      routing-instance routing-instance-name;
      secret password;
      max-outstanding-requests value;
      source-address source-address;
      timeout seconds;
    }
    service {
      accounting-order (activation-protocol | radius);
    }
    session-options {
      client-group [ group-names ];
      client-idle-timeout minutes;
      client-session-timeoutminutes;
    }
  }
```

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure PPP CHAP, or a profile and its subscriber access, L2TP, or PPP properties.

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

For CHAP, the name serves as the mapping between peer identifiers and CHAP secret keys. This entity is queried for the secret key whenever a CHAP challenge or response is received.

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 PPP Authentication Protocol*
- *Configuring Access Profiles for L2TP or PPP Parameters*
- *Configuring L2TP Properties for a Client-Specific Profile*
- *Configuring an L2TP LNS with Inline Service Interfaces*
- *Configuring PPP Properties for a Client-Specific Profile*
- *Configuring Service Accounting with JSRC*
- *AAA Service Framework Overview*
- *show network-access aaa statistics*
- *clear network-access aaa statistics*

protocol (Subscriber Secure Policy)

Syntax protocol *protocol*;

Hierarchy Level [edit services radius-flow-tap policy *policy-name* inet drop-policy *rule-name* from],
[edit services radius-flow-tap policy *policy-name* inet6 drop-policy *rule-name* from]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify the match IP protocol type for the radius-flow-tap policy.

Options ***protocol***—Protocol for the IPv4 or IPv6 address for the radius-flow-tap policy.

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

Related Documentation

- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

radius (Access Profile)

Syntax

```
radius {
    accounting-server [ ip-address ];
    attributes {
        exclude
            ...
        }
        ignore {
            framed-ip-netmask;
            input-filter;
            logical-system-routing-instance;
            output-filter;
        }
    }
    authentication-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        calling-station-id-delimiter delimiter-character;
        calling-station-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
        }
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        coa-dynamic-variable-validation;
        ethernet-port-type-virtual;
        interface-description-format {
            exclude-adapter;
            exclude-sub-interface;
        }
        ip-address-change-notify message;
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            ae-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
            atm {
                adapter-width width;
                port-width width:
                slot-width width;
                vci-width width:
                vpi-width width;
            }
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
            agent-circuit-id;
```

```
        agent-remote-id;
        interface-description;
        nas-identifier;
      }
      nas-port-type {
        ethernet {
          port-type;
        }
      }
      revert-interval interval;
      vlan-nas-port-stacked-format;
    }
    preauthentication-server ip-address;
}
```

Hierarchy Level [edit access profile *profile-name*]

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

Description Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.

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 RADIUS Server Parameters for Subscriber Access*
- *RADIUS Server Options for Subscriber Access*

radius-flow-tap

Syntax

```
radius-flow-tap {
  forwarding-class class-name;
  interfaces interface-name;
  multicast-interception;
  policy  policy-name {
    inet {
      drop-policyrule-name {
        from {
          apply-groups group-name;
          apply-groups-except group-name;
          destination-address address;
          destination-port port-number;
          dscp dscp-value;
          protocol protocol;
          source-address address;
          source-port port-number;
        }
      }
    }
    inet6 {
      drop-policy rule-name {
        from {
          apply-groups group-name;
          apply-groups-except group-name;
          destination-address address;
          destination-port port-number;
          dscp dscp-value;
          protocol protocol;
          source-address address;
          source-port port-number;
        }
      }
    }
  }
  source-ipv4-address ipv4-address;
)
```

Hierarchy Level [edit services]

Release Information Statement introduced in Junos OS Release 9.4.

Description Assign parameters that are used with subscriber secure policy mirroring.

The remaining statements are explained separately.

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

Related Documentation

- Subscriber Secure Policy Overview on page 3
- Configuring Support for Subscriber Secure Policy Mirroring on page 24

radius-server

Syntax

```
radius-server server-address {
  accounting-port port-number;
  accounting-retry number;
  accounting-timeout seconds;
  port port-number;
  retry attempts;
  routing-instance routing-instance-name;
  secret password;
  max-outstanding-requests value;
  source-address source-address;
  timeout seconds;
}
```

Hierarchy Level

[edit access],
[edit access profile *profile-name*]

Release Information

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

Description

Configure RADIUS for subscriber access management, L2TP, or PPP.

To configure multiple RADIUS servers, include multiple **radius-server** statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Options

server-address—Address of the RADIUS authentication server.

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 RADIUS Authentication for L2TP*
- *Configuring the PPP Authentication Protocol*
- *Configuring RADIUS Authentication*
- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)*
- *show network-access aaa statistics*
- *clear network-access aaa statistics*

rate-limit

Syntax rate-limit *limit*;

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

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

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

Default 150 connections

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

Range: 1 through 250

Default: 150

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

Related Documentation

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

source-address (Subscriber Secure Policy)

Syntax source-address *address*;

Hierarchy Level [edit services radius-flow-tap policy *policy-name* inet drop-policy *rule-name* from],
[edit services radius-flow-tap policy *policy-name* inet6 drop-policy *rule-name* from]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify source IP address or prefix value from which to inherit configuration data for radius-flow-tap policy rule mapping.

Options ***address***— IPv4 or IPv6 address for the radius-flow-tap policy.

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

source-ipv4-address

Syntax source-ipv4-address *ipv4-address*;

Hierarchy Level [edit services radius-flow-tap]

Release Information Statement introduced in Junos OS Release 9.4.

Description Specify the source IP address used in the IP header that is prepended to mirrored packets sent to a mediation device.

Options ***ipv4-address***—IPv4 address.

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

source-port (Subscriber Secure Policy)

Syntax source-port *port-number*;

Hierarchy Level [edit services radius-flow-tap policy *policy-name* inet drop-policy *rule-name* from],
[edit services radius-flow-tap policy *policy-name* inet6 drop-policy *rule-name* from]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify the match source port for the radius-flow-tap policy.

Options ***port-number***— Number of the IPv4 or IPv6 source port for the radius-flow-tap policy.

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

Related Documentation

- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*

ssh

Syntax

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

Hierarchy Level [edit system services]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
client-alive-interval and **client-alive-max-count** statements introduced in Junos OS Release 12.2.
no-passwords statement introduced in Junos OS Release 13.3.

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

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring SSH Service for Remote Access to the Router or Switch*

tunnel-services (Chassis)

Syntax

```
tunnel-services {
  bandwidth (1g | 10g | 20g | 40g);
  tunnel-only;
}
```

Hierarchy Level [edit chassis fpc *slot-number* pic *number*]

Release Information Statement introduced in Junos OS Release 8.2.

Description For MX Series 3D Universal Edge Routers, configure the amount of bandwidth for tunnel services.

For M7i, M10i, M120, M320, T Series and TX Matrix routers with IQ2 PICs and IQ2E PICs, configure support for per unit scheduling for GRE tunnels. You can specify the IQ2 and IQ2E PICs to work exclusively in tunnel mode or as a regular PIC. The default setting uses IQ2 and IQ2E PICs as a regular PIC. If you do not configure the **tunnel-only** option, the IQ2 and IQ2 PICs operate as regular PICs. For M7i, M10i, M120, M320, T Series and TX Matrix routers with IQ2 PICs and IQ2E PICs, you can use the **tunnel-only** option to specify that an IQ2 or IQ2E PIC work in tunnel mode only.

NOTE: Bandwidth rates of 20 gigabits per second and 40 gigabits per second require use of an MX Series router with the 100-Gigabit Ethernet Modular Port Concentrator (MPC) and the 100-Gigabit CFP MIC.

Options **tunnel–only** (Optional)—For M7i, M10i, M120, M320, T Series and TX Matrix routers with IQ2 PICs and IQ2E PICs, specify that an IQ2 or IQ2E PIC work in tunnel mode only.

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

- *Example: Configuring Tunnel Interfaces on a Gigabit Ethernet 40-Port DPC*
- *Example: Configuring Tunnel Interfaces on a 10-Gigabit Ethernet 4-Port DPC*
- *Example: Configuring Tunnel Interfaces on the MPC3E*
- bandwidth (Tunnel Services) on page 53
- *[edit chassis] Hierarchy Level*
- *Configuring Layer 3 Tunnel Services Interfaces on an MX Series Router with a DPC*

uid

Syntax uid *uid-value*;

Hierarchy Level [edit system login user]

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

Description Numeric identifier associated with the user account name, either assigned by an administrator or assigned automatically when you commit the user configuration. It is used by applications that request numeric identifiers, such as some RADIUS queries or secure applications such as flow-tap monitoring.

Options ***uid-value***—Number associated with the login account. This value must be unique on the router or switch.

Range: 100 through 64000

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

Related Documentation

- *Configuring Junos OS User Accounts*

user (Access)

Syntax

```
user username {
  authentication {
  class class-name;
  (encrypted-password "password" | plain-text-password);
  full-name complete-name;
  load-key-file URL filename;
  ssh-dsa “public-key” <from hostname>;
  ssh-rsa “public-key” <from hostname>;
  uid uid-value;
  }
}
```

Hierarchy Level [edit system login]

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

Description Configure access permission for individual users.

Options 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 Junos OS User Accounts*
- class on page 55

PART 3

Administration

CHAPTER 8

Reporting Intercept Related Information for Subscriber Secure Policy

Intercept-Related Events Transmitted to the Mediation Device

You can use SNMPv3 traps to report intercept-related events to the mediation device. These events include identifying information for subscribers, such as username or IP address, and subscriber session events, such as login or logout events or mirroring session activation or deactivation. The router sends the events to the mediation device in SNMP traps. Using SNMPv3 provides secure traps that are visible only to authorized individuals on the intended secure mediation device. The traps help support compliance with the Communications Assistance for Law Enforcement Act (CALEA), which defines electronic surveillance guidelines for telecommunications companies.

The supported SNMPv3 traps map to messages defined by the *Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American Nation Standard For Telecommunications*. "SNMP Traps for Subscriber Secure Policy LAES Compliance" on page 85 describes the supported SNMPv3 traps and their related LAES messages.

Related Documentation

- Subscriber Secure Policy Overview on page 3
- *Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview*
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 21
- SNMP Traps for Subscriber Secure Policy LAES Compliance on page 85
- Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring on page 91

SNMP Traps for Subscriber Secure Policy LAES Compliance

Table 7 on page 86 describes the SNMPv3 traps that subscriber secure policy mirroring uses to provide information that maps to messages defined in the *Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American National Standard for Telecommunications*. These messages enable subscriber secure policy to comply with

the *Communications Assistance for Law Enforcement Act* (CALEA). The Juniper Packet Mirroring MIB, **jnx-js-packet-mirror.mib**, provides the SNMP trap.

Table 7: Subscriber Secure Policy SNMPv3 Traps for LAES Messages

SNMPv3 Trap	LAES Message	Description
jnxPacketMirrorLiSubscriberLoggedIn	• **access-attempt** (implied) • **access-session-accept** • **packet-data-session-start**	A subscriber, who is identified to have a mirrored service that is activated at login, has successfully logged in.
jnxPacketMirrorSessionLiSubscriberLogInFailed	• **access-attempt** (implied) • **access-failed** (all termination reasons except authentication-reject) • **access-reject** (termination reason is authentication-reject)	A subscriber, who is identified to have a mirrored service that is activated at login, has failed to log in.
jnxPacketMirrorInterfaceLiSubscriberLoggedOut	• **access-session-end** • **packet-data-session-end**	A subscriber, who had an active mirrored service, has logged out.
jnxPacketMirrorInterfaceLiServiceActivated	• **packet-data-session-already-established**	A mirrored session has been activated.
jnxPacketMirrorSessionLiServiceActivationFailed	–	A mirrored session for a subscriber has failed.
jnxPacketMirrorSessionLiServiceDeactivated	–	A mirrored session for an established subscriber has been deactivated.
jnxPacketMirrorMirroringFailure	–	A mirrored service request failed due to an invalid value in the request. Note: This trap is not related to LAES messages.
jnxPacketMirrorTriggerType	–	The type of trigger that caused the mirroring session to be activated.
jnxPacketMirrorCallingStationIdentifier	–	The calling station ID of the subscriber whose traffic is currently being mirrored.
jnxPacketMirrorNasIdentifier	–	The NAS ID of the session in which traffic is being mirrored.
jnxPacketMirrorTargetIPv6Address	–	The IPv6 address of the subscriber interface that is being mirrored.

Related Documentation

- Intercept-Related Events Transmitted to the Mediation Device on page 85
- Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring on page 91

Configuring SNMPv3 Traps for Subscriber Secure Policy Mirroring

This topic provides an overview of the SNMPv3 configuration process as it pertains to subscriber secure policy. For more information, see *Example: Configuring SNMPv3*.

To configure SNMPv3 trap support for subscriber secure policy and to send the trap information to the mediation device:

1. Configure the MIB view.

   See *Configuring MIB Views*.

2. Configure the trap notification and trap notification filter. See the following topics:
   - *Configuring the SNMPv3 Trap Notification*
   - *Configuring the Trap Notification Filter*
3. Configure the target device. The target device is the mediation device that receives the trap information.

   See *Configuring SNMPv3 Traps on a Device Running Junos OS*.

4. Configure the SNMPv3 user, authentication method and password, and privacy method and password. See the following topics:
   - *Creating SNMPv3 Users*
   - *Configuring the SNMPv3 Authentication Type*
   - *Configuring the Encryption Type*
5. Configure user access privileges to management information.

   See *Defining Access Privileges for an SNMP Group*.

Related Documentation

- Intercept-Related Events Transmitted to the Mediation Device on page 85
- SNMP Traps for Subscriber Secure Policy LAES Compliance on page 85
- Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring on page 91
- *SNMPv3 Overview*

CHAPTER 9

Terminating Subscriber Secure Policy Traffic Mirroring Sessions

Terminating DTCP-Initiated Subscriber Traffic Mirroring Sessions

You can terminate DTCP-initiated traffic mirroring sessions by the following action:

- DTCP DELETE message receipt—Terminated upon receipt of a DTCP DELETE message. The DTCP administrator configures the DELETE message to include the same mirroring attributes that are used in the ADD message to initiate mirroring.

Related Documentation

- DELETE DTCP on page 35
- DTCP Messages Used for Subscriber Secure Policy on page 10

CHAPTER 10

Example

Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring

This example shows an SNMP configuration that provides SNMPv3 trap support.

Configure the SNMPv3 trap support at the **[edit snmp]** hierarchy level.

```
[edit snmp]
v3 {
    usm {
        local-engine {
            user mediation-device1 { ## Name of the mediation device
                authentication-md5 {
                    authentication-key "yourAuthentictaionKey"; ## SECRET-DATA
                }
                privacy-des {
                    privacy-key "YourPrivacyKey"; ## SECRET-DATA
                }
            }
        }
    }
    target-address london-1 {
        address 172.19.87.240; ## Address of the mediation device receiving the traps
        port 162;
        tag-list mediation-8;
        target-parameters tp1;
    }
    target-parameters tpi {
        parameters {
            message-processing-model v3;
            security-model usm;
            security-level authentication;
            security-name mediation-device1; ## Name of the mediation device
        }
        notify-filter nf1;
    }
    notify n1 {
        type trap;
        tag mediation-8;
    }
```

```
    notify-filter nf1 {
      oid .1 include;
    }
  }
  view system {
    oid 1.3.6.1.2.1.1 include;
  }
  view all {
    oid .1 include;
  }
```

Related Documentation

- Subscriber Secure Policy Overview on page 3
- Configuring SNMPv3 Traps for Subscriber Secure Policy Mirroring on page 87
- *SNMPv3 Overview*

PART 4

Troubleshooting

CHAPTER 11

Acquiring Troubleshooting Information

Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

Problem When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

Solution To collect standard troubleshooting information:

- Redirect the command output to a file.

  user@host> **request support information | save rsi-1**

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.

```
[edit]
set system syslog archive size 100m files 25
set system auto-configuration traceoptions file filename
set system auto-configuration traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions level all
set protocols ppp-service traceoptions flag all
set protocols ppp traceoptions file filename size 100m files 25
set protocols ppp traceoptions level all
set protocols ppp traceoptions flag all
set protocols ppp monitor-session all
set interfaces pp0 traceoptions flag all
set demux traceoptions file filename size 100m files 25
set demux traceoptions level all
set demux traceoptions flag all
set system processes dhcp-service traceoptions file filename
set system processes dhcp-service traceoptions file size 100m
set system processes dhcp-service traceoptions file files 25
set system processes dhcp-service traceoptions flag all
set class-of-service traceoptions file filename
set class-of-service traceoptions file size 100m
set class-of-service traceoptions flag all
set class-of-service traceoptions file files 25
set routing-options traceoptions file filename
set routing-options traceoptions file size 100m
set routing-options traceoptions flag all
set routing-options traceoptions file files 25
set interfaces traceoptions file filename
set interfaces traceoptions file size 100m
set interfaces traceoptions flag all
set interfaces traceoptions file files 25
set system processes general-authentication-service traceoptions file filename
set system processes general-authentication-service traceoptions file size 100m
set system processes general-authentication-service traceoptions flag all
set system processes general-authentication-service traceoptions file files 25
```

2. Copy the relevant statements into a text file and modify the log filenames as you want.
3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.

NOTE: The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.

BEST PRACTICE: Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

Related Documentation

- *Compressing Troubleshooting Logs from /var/logs to Send to Juniper Technical Support*

PART 5

Index

Index